Researching wickedness

Doing a PhD in the Security Group

Markus Kuhn

University of Cambridge
Computer Laboratory

18 November 2014

Security Group origins

- Originated in 1970s: Roger Needham, David Wheeler
- Early landmark work on password security, OS security, Needham–Schroeder protocol, CAP computer
- 1990s: protocols, BAN logic, cryptography, information hiding, compromising emanations, tamper resistance
- 2000s: banking systems, security economics, hardware security, positioning-system security, embedded systems, anonymity systems, OS security for mobile devices, hybrid capability systems, digital forensics, social-network security

Security group today

- Ross Anderson, Markus Kuhn, Frank Stajano, Robert Watson
- 12 postdocs
- 10 PhD students
- Courses in Part IB, Part II, MPhil
- Hardware-tamper and signal-security lab
- Collaborations with NetOS, Comp-Arch, Theory, DTG

UNIVERSITY OF CAMBRIDGE

Computer Security Research at Cambridge

The University of Cambridge is home to some of the world's leading computer security researchers, with a long history of key contributions to the field. Cambridge's early interests in security include the identification of large primes (Wheeler 1949), one-way password encryption (Needham 1962), the capability-system security model (Wilkes, Needham, Walker 1970–1977), the Needham-Schroeder Protocol (1978), and the Burrows-Abadi-Needham logic (1989). We continue to make core contributions in the field – cryptographic protocol design, processor and operating system security, anonymity research, hardware security, and malware analysis. We also perform foundational cross-disciplinary work in security economics, cybercrime measurement, censorship resistance, security psychology, human factors, and domestic and international policy.

Faculty staff supervising PhD students within the Security Group are:


Ross Anderson


Markus Kuhn


Frank Stajano


Robert Watson

Their webpages describe their research interests. Facilities and ongoing projects available for PhD students include:

- ATMs and banking devices
- eCrime data
- Tamper Lab: hardware reverse engineering, side-channel and fault injection attacks
- Software-defined radio test and measurement equipment for electro-magnetic eavesdropping research
- Pico: password-free online authentication device
- CHERI processor: hardware-assisted sandboxing with capabilities
- Android application development and Device Analyzer data

The Security Group currently has eleven full-time post-doctoral researchers, spanning many disciplines, from compiler construction and electronics to psychology and criminology. This provides expertise in the usability of security devices, the psychology of deception, and cyber crime. We also work with other groups within the department, bringing a security perspective to their projects. The group's website and blog summarise recent research, provide musings on security, and advertise jobs and studentships:

http://www.lightbluetouchpaper.org/
http://www.cl.cam.ac.uk/research/security/


Security Group, 2014

Active security and privacy research areas

- Anonymous communication
- API and protocol security
- Application compartmentalisation techniques
- Authentication and biometric identification systems
- Banking and payment system security
- Censorship resistance
- Capability systems
- Compromising emanations
- Cryptology
- Digital forensics
- Distributed system and cloud computing security
- Economics of cybercrime
- Economics of information security
- Formal methods
- Hardware security
- Location and positioning systems
- Malware analysis
- Medical information security
- Mobile and embedded system security
- Operating system security
- Passwords
- Privacy and freedom issues
- Programming language security
- Psychology of deception
- SCADA and the security of industrial control systems
- Security and human behaviour
- Security protocols
- Social networking and privacy
- Steganography
- Tampering with tamper-resistant devices
- Temporal security properties

PhD in Computer Science

The PhD in Computer Science mentors students in award-winning research and methodology. Research students in the security group frequently publish security-related research at top conferences. Current research students, and their topics, include:

- Sheharbano Khattak: *Measuring censorship, censorship circumvention/resistance technologies* (Murdoch)
- Ilias Marinos: *Program analysis and transform for security* (Watson)
- Christian O'Connell: *Eavesdropping, compromising emanations, hardware security* (Kuhn)
- Kumar Sharad: *Mobile payments, privacy* (Murdoch)
- Laurent Simon: *Mobile payment, mobile security* (Anderson)
- Daniel Thomas: *Mobile security, cryptography, cloud storage, secure updates* (Beresford)
- Rubin Xu: *Android security and malware analysis* (Anderson)
- Dongting Yu: *BGP security* (Anderson)
- Bjoern Zeeb: *Operating-system security, network stacks* (Moore/Watson)

Recently completed security-related PhDs include:

- Jonathan Anderson: *Privacy engineering in social networks* (Stajano)
- Joseph Bonneau: *Guessing human-chosen secrets* (Anderson)
- Omar-Salim Choudary: *Efficient multivariate statistical techniques for extracting secrets from electronic devices* (Kuhn)
- Shailendra Fuloria: *Robust security for the electricity network* (Anderson)
- Kim Hyoungshick: *Complex network analysis for secure and robust communications* (Anderson)
- Wei Ming Khoo: *Decompilation as search* (Anderson)
- Andrew Lewis: *Reconstructing compressed photo and video data* (Kuhn)
- Theo Markettos: *Active electromagnetic attacks on secure hardware* (Moore)
- Jean Martina: *Verification of security protocols based on multicase communication* (Paulson)
- John Miller: *Distributed virtual environment scalability and security* (Crowcroft)
- Robert Watson: *New approaches to operating system security extensibility* (Anderson)

Prof Ross Anderson

Current main research interests:

- Economics and psychology of security
  - measuring cybercrime
  - the psychology of deception
- Payment systems
  - failures of EMV (chip-and-pin) systems
  - mobile device security
- Security protocols
- Security and policy
  - surveillance and privacy
  - risk and liability

Prof Ross Anderson – PhD students

- Rubin Xu: Android security and malware analysis (current)
- Dongting Yu: BGP security (current)
- Joseph Bonneau: Guessing human-chosen secrets
- Shailendra Fuloria: Robust security for the electricty network
- Wei Ming Khoo: Decompilation as search
- Hyoungshick Kim: Complex network analysis for secure and robust communications
- Shishir Nagaraja: Robust covert network topologies
- Tyler Moore: Cooperative attack and defense in distributed networks
- Andy Ozment: Vulnerability discovery and software security

Dr Markus Kuhn

Current main research interests:

- Signal-processing aspects of security
  - compromising emanations
  - side channels, covert channels
  - forensic signal analysis
  - audio/video coding systems (recompression, recovery)
- Hardware security
  - tamper resistance
  - programmable logic security
  - physical uncloneable functions
- Physical-layer communication security
  - distance-bounding protocols
  - positioning-system and sat-nav security
  - jamming and spoofing resistance
  - RFID
- Web security, NoXML/NoSQL databases, ...

Dr Markus Kuhn – PhD students

- Christian O'Connell: Model-based assessment of compromising emanations (ongoing)
- Omar Choudary: Efficient multivariate statistical techniques for extracting secrets from electronic devices
- Andrew Lewis: Reconstructing compressed audio and video data
- Saar Drimer: Security for volatile FPGAs
- Gerhard Hancke: Security of proximity identification systems
- Steven Murdoch: Covert channel vulnerabilities in anonymity systems
- Piotr Zieliński: Minimizing latency of agreement protocols

Dr Frank Stajano

Mission: making the digital society fair and secure for regular humans

Pico: no more passwords!

- European Research Council starter grant
- 5 RAs, 6 project students so far
- Will you join for a PhD?

Other research interests: privacy, human factors, ubicomp

- **Deterrence of deception** (with Ross Anderson et al)
- Resurrecting Duckling (own PhD)

Dr Frank Stajano – PhD students

- Jonathan Anderson: Privacy engineering for social networks
- Ford-Long Wong: Protocols and technologies for security in pervasive computing
- Alastair Beresford: Location privacy

Dr Robert N.M. Watson

OS security; capability systems;
application compartmentalization;
software tracing, analysis, transformation;
hardware-software interface;
high-performance networking / storage

Funding from DARPA, Google, EU, EPSRC,
others; studentships available

Also involved in NetOS, Computer Architecture, Theory groups.

Dr Robert N.M. Watson (cont'd)

- MAC Framework: OS access-control extensibility used in FreeBSD, Apple iOS, Apple Mac OS X, Juniper Junos
- Capsicum: Practical capabilities for UNIX
- CHERI: Capability hardware enhanced RISC instructions
- SOAAP: Security-oriented analysis of application programs
- TESLA: Temporally enhanced system logic assertions
- OS network-stack and storage-stack tracing and optimisation

Dr Robert Watson – PhD students

- Illias Marinos: Program analysis and transform for security (ongoing)
- Bjoern Zeep: Operating-system security / setwork stacks (ongoing)

Dr Richard Clayton

post-doctoral researcher

Current main research interests:

- Cybercrime
  - spam
  - phishing
- ISP policies and practices
- Internet resiliency

Current research areas

UNIVERSITY OF CAMBRIDGE

Economics and psychology of security

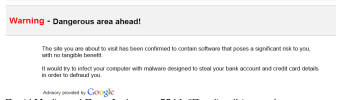
The psychology of deception

David Modic, Sophie van der Zee, Ross Anderson

We perform experiments on a range of topics in security usability, risk communication and deception online. For example, we have been working with an industrial funder on browser security warnings, which we see so often that we have mostly learned to ignore them. How can we make browser warnings fewer but better? We experimented with a range of warnings and found that many favourite 'nudges', such as appeals to authority and social compliance, do not work well. Even putting cartoon faces on browser warnings to activate social cognition doesn't give a significant improvement. What does work is making warnings more concrete. Telling users that a website will try to install a trojan that will steal their bank credentials gets much better compliance than a vague warning that "this site may harm your computer".

We have developed a psychometric tool measuring people's susceptibility to persuasion. Our new scale (StP-II) combines established factors such as need for cognition, sensation seeking, susceptibility to advertising, attitudes towards risky choices and so on. We are currently testing StP-II extensively to understand the causes of scam compliance. Once we understand better which people are likely to fall for which scams, we can start thinking about what can be done by way of education, training or even automated scam detection.

We have a large project on the deterrence of deception in socio-technical systems with researchers at Portsmouth, Newcastle and UCL. In 2008 we founded the Workshop on Security and Human Behaviour, which brings psychologists together with security engineers.



David Modic and Ross Anderson, 2014. "Reading this may harm your computer: The psychology of malware warnings" . *Computers in Human Behaviour, 41*, 71-79.

Understanding and disrupting the economics of cybercrime

Richard Clayton, Alice Hutchings, Ross Anderson

We study cybercrime by combining established concepts and approaches from many different scientific domains, including computer science, economics and criminology. We aim to understand a wide range of online crime and develop innovative ways to detecting offenders and reduce their impact. Recent work has included:

- Measurement of the "phishing" ecosystem (the theft of credentials using fake web pages)
- Identifying the extent to which criminals use privacy and proxy systems to conceal their identities when registering domain names
- Examining what use is made of the domain names once used by banks when they shut down or merge with another institution
- Understanding how online Ponzi schemes operate and estimating the criminal income
- Analysing the online stolen data economy: the supply of hardware and software to steal data; the sale of stolen data, the provision of services to turn data into money -- and then identifying points for intervention
- Creating the Cambridge Computer Crime Database, which records computer crime events where the offender has been arrested, charged and/or prosecuted in the UK
- Surveying offenders who provide denial of service attacks for a fee, in order to identify pathways into offending, and estimate the benefits received

Tyler Moore, Richard Clayton and Ross Anderson, 2009. "The economics of online crime". *Journal of Economic Perspectives, 23*(3), 3-20.

Pico

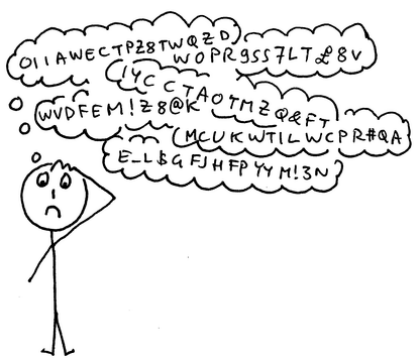
Pico: no more passwords!

Frank Stajano, Quentin Stafford-Fraser, Graeme Jenkinson, Max Spencer, Chris Warrington, Jeunese Payne

Users are told by security people that their passwords must be unguessable, must contain mixed-case letters, numbers and symbols, must not be written down, must all be different and must also be changed every couple of months. The intersection of all these constraints is the empty set. It's objectively impossible to follow all these directives at once – an unfair deal for users. As the number of online accounts per person keeps growing, passwords are not sustainable as a user authentication scheme.

Pico was designed so that you would not have to memorise secrets. It is a hardware token that can handle thousands of accounts. Besides usability, it also addresses many security problems: resisting brute-forcing, eavesdropping, phishing, keylogging etc. Pico unlocks in the presence of its owner by recognising miniature gadgets embedded in wearable items such as clothes and jewellery (Picosiblings). The user never has to type a PIN to unlock the Pico.

A competitive European Research Council grant worth over £1M funds the research team that is currently prototyping, validating and refining the design of Pico and will eventually produce a reference implementation, which will not be encumbered by patents or licensing fees.



Frank Stajano, "Pico: no more passwords!". Security Protocols Workshop 2011, LNCS 7114, Springer 2011.

UNIVERSITY OF CAMBRIDGE

Hardware security

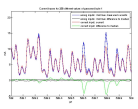
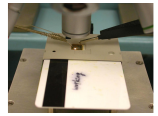
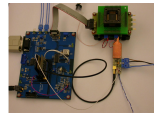
Hardware tamper resistance

Sergei Skorobogatov, Markus G. Kuhn

Protection against physical attacks has become an essential part of many modern system designs. These days we have a continuous battle between manufacturers who invent new security solutions learning from previous mistakes, and a hacker community that is constantly trying to break protection in various devices. The importance of security is dictated by the amount of valuable and sensitive information stored on the chip. This could be cryptographic keys, secret data, company secrets, intellectual property, electronic money or banking smartcards.

Our group have invented semi-invasive attacks (optical fault injection) which have forced the industry to rethink protection mechanisms in smartcards and amend Common Criteria requirements. As with invasive attacks (microprobing, chip modification), they require opening the chip in order to get access to its surface without destroying it or creating contacts to internal wires. Those attacks are as easy to implement as inexpensive non-invasive attacks (power analysis, glitching).

In collaboration with Quo Vadis Labs we developed a new side-channel analysis technique. This breakthrough approach means it is now possible to extract encryption keys from devices and systems up to a million times faster than state-of-the-art power analysis techniques, e.g. DPA. Our recent research is focused on Hardware Assurance – testing of silicon chips for backdoors and trojans. Because of the speed at which analysis can be performed, it becomes possible to identify hidden backdoors and trojans in silicon chips – a task that is not feasible with current DPA methods.

Banking and payment system security

Ross Anderson, Mike Bond, Omar Choudary, Steven J. Murdoch, Laurent Simon

Known in the UK as "Chip and PIN", EMV (Europay, MasterCard, Visa) is the dominant standard for smart-card payments worldwide. Introduced to reduce card fraud, EMV is used throughout Europe; it is being introduced in the US, Canada and South America. EMVCo estimates that over a billion EMV payment cards are in circulation. EMV makes card transactions more secure by adding a chip to cards to make them harder to counterfeit and requiring customers to enter a PIN to authorize payment. While initially reducing fraud, criminals adapted to the change, resulting in increased losses.

Research at Cambridge has discovered numerous vulnerabilities in the deployed Chip and PIN system, including the ability for criminals to trick terminals into accepting an incorrect PIN for a stolen card, failures in the tamper resistance measures present in widely deployed Chip and PIN terminals, and ways for corrupt bank employees circumvent protections against insider attacks to discover customer PINs. We have developed methods to resolve these vulnerabilities and work with industry to have these improvements deployed. Smart Architects Ltd sell auditing equipment, developed at Cambridge, to detect these vulnerabilities. Methods for securing online banking against man-in-the-middle malware, developed at Cambridge, have been commercialised by spin-out company Cronto Ltd, since acquired by VASCO, and are in use at several banks.

Signal analysis

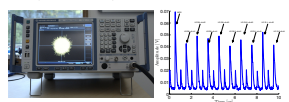
Compromising emanations and side channels

Markus G. Kuhn, Omar Choudary, Christian O'Connell

Computers unintentionally emit information about the data they process on various parasitic analog side channels, such as high-frequency current fluctuations on power-supply lines, electromagnetic fields, as well as audible, ultrasonics and light emissions. These signals can be picked up nearby and decoded by well-equipped eavesdroppers, and used to circumvent cryptographic and access-control security mechanisms. We investigated the nature of compromising emanations of analog and digital computer displays, as well as television sets, and developed software techniques to manipulate these. We work on civilian emission-security standards, including one for voting machines by the Dutch government.

We optimized template attacks on security microcontrollers, a powerful statistical signal-processing technique to extract data from instruction-specific information leakage. The attacker first builds a high-dimensional multivariate model of both the information leakage and noise while observing the processing of known data, and then uses that model to perform maximum-likelihood estimation of unknown processed data in products involving the same type of processor.

We provide advice to manufacturers of TEMPEST equipment for government applications that require protection against electromagnetic eavesdropping. We preparing new digital signal-processing techniques to improve industrial emission-security measurement processes.

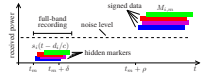


Omar Choudary, Markus G. Kuhn: Efficient Template Attacks. CARDIS 2013.
Markus G. Kuhn: Compromising emanations of LCD TV sets. IEEE Trans. on Electromagnetic Compatibility, Vol. 55, No. 3, June 2013.

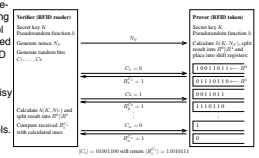
Location security: cryptography at the speed of light

Markus G. Kuhn

Global navigation satellite systems still lack signal-integrity protection for mass-market applications. A particular challenge is the need to protect not only the integrity of broadcast data, but also the nanosecond-accurate relative arrival times of signals from different satellites, from which receivers determine their position. We have proposed several new types of signal-authentication and spoofing detection techniques. A steganographic transmission scheme with delayed release of spreading keys provides the same asymmetric security that made digital signatures so useful: the ability to verify a signal does not lead to the ability to spoof it. This is of particular importance in civilian mass-market applications where the holder of the receiver may want to manipulate its reading: road toll, pay-as-you-drive car insurance, or offender-tagging. In addition, we have also proposed heuristics that help GPS receivers detected spoofed signals.



Distance-bounding protocols ascertain both the identity of a communications partner and also their location. They securely answer questions such as "is this smartcard really within 1 metre of the reader?", by incorporating a rapid exchange of single challenge-response bits, where the speed of light is the main part of the round-trip time. We proposed the first distance-bounding protocol optimized for RFID applications with noisy wide-band channels.



Forensic signal analysis

Markus G. Kuhn, Andrew B. Lewis

Widespread use of digital cameras, compression, high-capacity storage, and advanced tools (video editors, SDR, etc.) pose new challenges to forensic investigators, who need techniques to confirm claimed origins and processing histories of signal evidence, and recover data without the cooperation of the hardware owner or designer.

In collaboration with the Metropolitan Police, we designed a sophisticated tool for recovering compressed video data from fragmented storage where file-system metadata is unavailable. Manufacturers are unwilling to release documentation for proprietary file-systems, block allocation, and Flash wear-leveling algorithms, leaving investigators with a random puzzle of 4KB memory blocks to be assembled back into a video stream (H.264, etc.), a task that our new high-performance parser can handle for gigabytes of data.

Our *exact JPEG recompressor* uses iterative interval arithmetic to invert a JPEG decompressor, recreating the original compressed bitstream. It can help to identify/exclude particular decoders as a source, but also has applications in evaluating copy -protection schemes.

Andrew B. Lewis, Markus G. Kuhn, "Exact JPEG recompression". Proc. SPIE 7543, Visual Information Processing and Communication, 75430V, January 2010.
Andrew B. Lewis, "Reconstructing compressed photo and video data". Computer Laboratory Technical report UCAM-CL-TR-813, February 2012.

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

http://www.lightbluetouchpaper.org/