ACS/Part III R209

Computer Security: Principles and Foundations

Professor Ross J. Anderson
Professor Alastair Beresford
Dr Robert N. M. Watson
Dr Alice Hutchings

16 January 2020
Introductions

• Name, background
• Interest in security
• What you hope to learn, or better understand, at the end of this module
Today’s Class

1. Module introduction
2. Presentation and discussion: *A Note on the Confinement Problem*
3. Video and discussion: *Chip and PIN is broken*
4. Presentation and discussion: *Experimental Security Analysis of a Modern Automobile*
5. Brief summary of next week: Access Control
Welcome!

• Seminar-style research readings module
• **R254: Cybercrime** (Michaelmas)
  – Interdisciplinary perspective
  – Focus on key debates, research and policy
  – What cybercrime is, how it is regulated, policed, detected, and prevented
• **R209: Computer Security: Principles and Foundations** (Lent)
  – History, discourse, methodology, and themes
  – Topics include adversarial reasoning, access control, usability, inference control, ...
• Ambitious scope, limited time
Prerequisites

**Goal**: Transition from *factual* understanding to *research engagement* with core debates, intellectual history, methodology, and evolution of the field

- Undergraduate degree in computer science
  - Or similar education/experience
  - Basic background in computer security
  - Also beneficial: OS, networking, programming languages...

- Some topics familiar, but cast as *research* not *fact*
- Other topics will not [yet] be widely taught
Brushing up on computer security


Seminar-style teaching (1)

• Preparation for research and development
  – Trace intellectual history
  – Study evolving vocabulary, discourse, and methodology
  – Discuss and learn from methodological and narrative aspects of the research
  – Appreciate (+critique) research as published
  – Consider contemporary implications; contrast with original research context
  – Discuss future research directions

• Student-led presentation and discussion is central to this format
Seminar-style teaching (2)

Each week you will:

1. Critically read three original papers/reports

2. Submit synthesis essays across all readings
   or
2. Present and lead discussion on a specific reading

3. Participate in classroom discussion of the readings

(Guest PhD students, postdocs in the class will present papers but not submit essays)
Typical class structure

- 3x 15–to–20-minute student presentations (do not run shorter/longer!)
- 3x 15–to–20-minute student-led discussions
- Discussions are cumulative: pull ideas forward as we look at later papers
Assessment

• One presentation or essay a week
  – R209: Seven total (none today)

• Marking
  – 10 marks per assessed essay or presentation
  – **Lowest mark** each term will be dropped (usually the first)
  – Remaining scores scaled to a total out of 100

• Department heavily penalizes late submissions
  – Instructors cannot grant extensions
  – Contact the graduate education office as **early as possible**
WEEKLY ESSAY
Synthesis Essays

- **Synthesis writing** reports, organizes, and interprets the works of others
  - Not an original research paper!
  - More a series of short answers than an actual essay
- Your essays **will** have the following section headings:

1. Summaries of readings (1-2 para/reading)
2. Three key themes spanning papers (1 para/theme)
3. Ideas in our contemporary context (2 para)
4. Brief literature review (2 para)

- All essays **must** include a bibliography
- Word limit (1,250) enforced (excl. bibliography)
- See Assessment page on module website
Notes on essay marking

• 10 divided equally across four sections plus 2 marks for overall delivery (quality of writing, ...):

  0   failed to submit
  1-4  seriously lacking
  5-6  poor or (minimally) adequate
  7-8  good
  9-10 strong or exceptional

• First essay will likely have a lower mark than you hope
• If so, it will probably be dropped as the lowest
Essay Submission

• Deadline 16:00 on the Tuesday before we meet
• **Submit via Moodle**
• Bring discussion questions to class and be prepared to ask (and answer) them
• Marks/comments returned via Moodle
• We attempt to return essays to you within two weeks, but sometimes this is not possible
Weekly Presentations

• 7 sessions, 3 talks/session, **15-20 minutes each**
  – You will present at least once per term
  – No essay due for classes where you present
  – Do not run much shorter or longer than 17 minutes!
  – 10 marks per presentation; similar criteria to essays

• Initial presentation schedule has been e-mailed
  – If you like, you can exchange presentation slots...
  – Both students must agree; let us know in advance
## R209 Weekly Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Paper</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 Jan</td>
<td>Access Control</td>
<td>Bell &amp; LaPadula (1975)</td>
<td>tll39</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wagner &amp; Tribble (2002)</td>
<td>ttb29</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Watson (2013)</td>
<td>jga33</td>
</tr>
<tr>
<td>30 Jan</td>
<td>Usable Security</td>
<td>Whitten &amp; Tygar (2014)</td>
<td>psb34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Herley (2014)</td>
<td>ytc36</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acar et al. (2016)</td>
<td>nm712</td>
</tr>
<tr>
<td>6 Feb</td>
<td>Inference Control</td>
<td>Adams &amp; Wortmann (1989)</td>
<td>bjc63</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dwork et al. (2006)</td>
<td>mda46</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Narayanan &amp; Shmatikov (2007)</td>
<td>mgp35</td>
</tr>
<tr>
<td>13 Feb</td>
<td>Correctness v. Mitigation</td>
<td>Klein et al. (2009)</td>
<td>lsw37</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bessey et al. (2010)</td>
<td>sps62</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Davis et al. (2019)</td>
<td>rmn30</td>
</tr>
<tr>
<td>20 Feb</td>
<td>Adversarial Reasoning II</td>
<td>Razavi et al. (2016)</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bond et al. (2014)</td>
<td>dh623</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kocher et al. (2019)</td>
<td>vv301</td>
</tr>
<tr>
<td></td>
<td></td>
<td>van Eeten et al. (2010)</td>
<td>htb25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vasek &amp; Moore (2015)</td>
<td>jga33</td>
</tr>
<tr>
<td>5 Mar</td>
<td>Passwords</td>
<td>Morris &amp; Thompson (1979)</td>
<td>doaa2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adams &amp; Sasse (1999)</td>
<td>az369</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bonneau et al. (2012)</td>
<td>mgp35</td>
</tr>
</tbody>
</table>

*** If you would like to volunteer for a second speaking slot, rather than submitting an essay for that week, please email alice.hutchings@cl.cam.ac.uk
Presentation Structure

• Prepare a teaching- or research-style presentation
  → What motivated the work?
  → What are the key ideas?
  → How were scientific ideas evaluated?
  → Critique the argument/evaluation
  → Compare to related research – especially other readings
  → Consider current-day research and applications
  → Prepare for adversarial Q&A – defend the work

• Don’t just follow paper outline
• Slides without pictures (e.g., this one) are uninspiring!
Your Slides

• You will present with slides
  – All presentations will be on our computer
  – Slides will be in **PDF format** – no fancy animations

• Submit slides by e-mail no later than 16:00 on the Wednesday via Moodle
  – Failure to prepare or submit will be heavily penalized due to disruption it will cause

• Usually presented roughly in syllabus order
Class Discussion

• Roughly half of each two-hour class is set aside for discussion
  – Bring discussion questions to class and be prepared to ask (and answer) them

• No explicit marks for participation...
  – ... but presenter is rewarded for interesting discussion, so mutual benefit to participating!
READING
About the Readings

• Original research papers or early surveys
  – Highly cited and/or first appearance of key ideas

• Questions to consider (in advance)
  – Why have the authors done this work?
  – Has it aged well? Are the ideas used today?
  – How would we attack the system they propose?
  – What methodology do the papers use: Science? Engineering? Mathematics? How does this affect the style, evaluation, etc.?
  – Why did we pick this paper and not another?
  – Is there a retrospective piece?
How to Read (a Lot)

• Read strategically
  – Plan ahead for the time it takes to read and digest papers
  – Skim in the first pass to decide what is important
  – Take notes in moderation
  – With practice, you will get much faster at reading papers
• As you read, highlight ideas that answer key questions:
  – Framing/motivation of the paper
  – Key ideas that influenced the paper / related work
  – Key contributions of the paper – and their implications
  – Evaluation approach, limitations
  – Common themes and ideas across the papers
• See Keshav’s “How to Read a Paper”, CCR 2007
ADMIN THINGS
Module E-mail and ‘Hangers On’

• We will e-mail reading and schedule updates, clarifications, room changes, etc. there!
  – We will use your CRSid (via a class mailing list)
  – If you are not registered, but are sitting in, please e-mail alice.hutchings@cl.cam.ac.uk

• Recurring guests (e.g., PhD students, RAs) will be asked to present 1-2 times during the term
Module Website

• Reading list, marking criteria, etc. found here: https://www.cl.cam.ac.uk/teaching/1920/R209/

• Look at the ‘Materials’, ‘Assessment’ pages
# R209 Weekly Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Convener(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 Jan</td>
<td>Adversarial Reasoning</td>
<td>Anderson, Beresford, Watson, Hutchings</td>
</tr>
<tr>
<td>23 Jan</td>
<td>Access Control</td>
<td>Watson</td>
</tr>
<tr>
<td>30 Jan</td>
<td>Usable Security</td>
<td>Hutchings</td>
</tr>
<tr>
<td>6 Feb</td>
<td>Inference Control</td>
<td>Anderson</td>
</tr>
<tr>
<td>13 Feb</td>
<td>Correctness v. Mitigation</td>
<td>Beresford</td>
</tr>
<tr>
<td>20 Feb</td>
<td>Adversarial Reasoning II</td>
<td>Beresford</td>
</tr>
<tr>
<td>27 Feb</td>
<td>Security Economics</td>
<td>Anderson</td>
</tr>
<tr>
<td>5 Mar</td>
<td>Passwords</td>
<td>Hutchings</td>
</tr>
</tbody>
</table>
How to Reach Us

ross.anderson@cl.cam.ac.uk
alastair.beresford@cl.cam.ac.uk
robert.watson@cl.cam.ac.uk
alice.hutchings@cl.cam.ac.uk
Security Group Seminars & Meetings

• Seminars every Tuesday at 2pm in LT2
  – Coming up: ‘Challenges in the Decentralised Web: The Mastodon Case’ by Gareth Tyson, Queen Mary University of London

• Security group meetings every Friday at 4pm in FW11
QUESTIONS
TODAY’S READINGS