Today’s Class

1. Module introduction
2. Paper: Protection of Information in Computer Systems
4. Discussion: security motivations and methodology
Welcome!

• *Seminar-style* research readings module
• R209: Principles and Foundations (Michaelmas)
  – History, discourse, methodology, and themes
  – Topics include local systems, crypto/protocols, human factors, and economics
• R210: Current Research and Applications (Lent)
  – Guest conveners lead sessions on current research topics (usually current or past lab researchers)
  – E.g., censorship resistance, tamper-proof hardware...
• Ambitious scope, limited time
Prerequisites

Goal: transition from ‘factual’ understanding to 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 and discourse
  – Appreciate (+critique) research as published
  – Consider contemporary implications
  – Contrast with original research context
  – Discuss future research directions

• Student-led discussion is critical 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
Typical class structure

- 3x 15-20-minute student presentations (do not run shorter/longer!)
- 3x 10-15-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)
  – R210: Eight total (hit ground running)

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

• *Synthesis writing* reports, organizes, interprets works of others
  – *Not an original research paper!*
  – More a formulaic series of short answers than an actual essay

• Your essays will have the following sections 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)
  5. Proposed discussion questions (4 bullet points)

• All essays **must** include a bibliography
• NB: word limit (1,500) enforced; see the website for details
Notes on essay marking

• 10 divided equally across each of five sections

- 0 failed to submit
- 1-4 seriously lacking
- 5-6 poor or (minimally) adequate
- 7-8 good
- 9-10 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 12:00 on the Friday before we meet *
• Submit on paper to the graduate education office
• E-mail as PDF to: cl-acs-r209-essays@lists.cam.ac.uk

• Bring discussion questions to class and be prepared to ask (and answer) them

• Marks/comments returned via the graduate education office; we usually e-mail them as well
• We attempt to return essays to you within two weeks, but sometimes this is not possible

* Except for the first essay, which is due next Monday at 12:00 to give you a full week.
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
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 12:00 on the Monday to cl-acs-r209-slides@lists.cam.ac.uk
  – Also submit on paper to graduate education office
  – Failure to prepare or submit will be heavily penalized due to disruption it will cause

• Usually presented in roughly 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?
  – Are they 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 robert.watson@cl.cam.ac.uk

• Recurring guests (e.g., PhD students, RAs) will be asked to present 1-2 times during the term
  – E-mail me to talk about which papers
Module Website

- Reading list, marking criteria, etc. found here: https://www.cl.cam.ac.uk/teaching/1617/R209/

- Beginnings of next term’s website here: https://www.cl.cam.ac.uk/teaching/1617/R210/

- Look at the ‘Materials’, ‘Assessment’ pages

- Model, including presentations/essays/etc, remain the same for R210
How to Reach Us

robert.watson@cl.cam.ac.uk
ross.anderson@cl.cam.ac.uk
daniel.thomas@cl.cam.ac.uk

Essays: cl-acs-r209-essays@lists.cam.ac.uk
Slides: cl-acs-r209-slides@lists.cam.ac.uk
# R209 Weekly Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Convener(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Oct</td>
<td>Origins and Foundation of Computer Security</td>
<td>Watson, Anderson, Beresford</td>
</tr>
<tr>
<td>17 Oct</td>
<td>Adversarial Reasoning</td>
<td>Anderson</td>
</tr>
<tr>
<td>24 Oct</td>
<td>Access Control</td>
<td>Watson</td>
</tr>
<tr>
<td>31 Oct</td>
<td>Capability Systems</td>
<td>Watson</td>
</tr>
<tr>
<td>7 Nov</td>
<td>Security Economics</td>
<td>Anderson</td>
</tr>
<tr>
<td>14 Nov</td>
<td>Passwords</td>
<td>Stajano (guest convener)</td>
</tr>
<tr>
<td>21 Nov</td>
<td>Cryptographic Protocols</td>
<td>Anderson</td>
</tr>
<tr>
<td>28 Nov</td>
<td>Correctness vs. Mitigation</td>
<td>Thomas</td>
</tr>
</tbody>
</table>
R210 Weekly Meetings
(last year’s, but a good predictor)

<table>
<thead>
<tr>
<th>Session</th>
<th>Topic</th>
<th>Convener</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Covert and Anonymous Communications</td>
<td>Murdoch</td>
</tr>
<tr>
<td>2</td>
<td>Bootstrapping Security Relationships</td>
<td>Stajano</td>
</tr>
<tr>
<td>3</td>
<td>Mobile-System Security</td>
<td>Beresford</td>
</tr>
<tr>
<td>4</td>
<td>Censorship Resistance</td>
<td>Khattak</td>
</tr>
<tr>
<td>5</td>
<td>Psychology and Security</td>
<td>Anderson</td>
</tr>
<tr>
<td>6</td>
<td>Banking Security</td>
<td>Anderson</td>
</tr>
<tr>
<td>7</td>
<td>Vulnerability Management</td>
<td>Leverett</td>
</tr>
<tr>
<td>8</td>
<td>Hardware Security and Tamper Resistance</td>
<td>Skorobogatov</td>
</tr>
</tbody>
</table>
QUESTIONS
INTRODUCTIONS
WHAT IS SECURITY?
TODAY’S READINGS