Welcome!

- “Seminar-style” research readings courses
- R209: Principles and Foundations (Michaelmas)
  - History, discourse, methodology, and themes
- R210: Current research + applications (Lent)
  - Guest conveners lead sessions on specific current research topics (usually lab staff)
- Ambitious scope, limited time
Prerequisites

• Undergraduate degree or a strong grounding in computer science
• At least one past course in operating systems, networking, and/or security
• Some topics will be familiar from taught material at the undergraduate level…
• … but grounded in their original research contexts and presentations

Brushing up on computer security

Seminar-style course

• Preparation for research and development in the field
  • Study vocabulary and discourse; trace intellectual history
  • Appreciate (and critique) original research as published
  • Consider current-day implications; contrast with original context
  • Discuss future research directions
• Each week you will:
  • Critically read three(ish) original research papers or reports
  • Submit synthesis essays across all readings or present and lead discussion on a specific reading
  • Particulate in class discussion of the readings

Assessment

• One presentation or essay a week
  • R209: Seven total (none today)
  • R210: Eight total (hit ground running)
• Each assessment is out of ten marks
• Lowest mark dropped; remaining scores scaled to a percent
• Department aggressively penalises late submissions
  • Instructors cannot grant extensions
  • If you are ill or unavailable, contact the graduate education office as soon as possible to negotiate deadlines
Weekly essays

Synthesis essay

- Synthesis writing reports, organises, and interprets readings
- Synthesis essays are not original research papers
- Suggested outline covers five areas:
  1. Summaries of readings (1-2 para/reading)
  2. Discussion of a 2-3 key themes spanning readings (2-4 para)
  3. Consideration of ideas in current context (1-2 para)
  4. Literature review (1-2 para)
  5. Class discussion questions (4 is a good number)
- All essays must include a bibliography
- If this is new to you, Google “synthesis essay”
Essay marking notes

- 10 points divided evenly across five aspects:
  - 0 - failed to submit
  - 1-4 - seriously lacking
  - 5-6 - adequate
  - 7-8 - good
  - 9-10 - exceptional

Essay submission

- Submit on paper to the graduate education office
- Must be received by **noon** on the Thursday before we meet (except this week: noon Friday is OK)
- Please **also** e-mail an electronic copy, in PDF format, to **acs-2013-r209-essays@cl.cam.ac.uk**
- Marks will be returned via the graduate education office; we usually e-mail them as well
- Bring discussion questions to class
Weekly presentations

Student presentations

- 7 sessions, 3 talks/session, 15 minutes each
- You will present at least once per term
- No essay due for class where you present
- Up to 10 marks per presentation; similar criteria to essays
- Presentation schedule has been e-mailed out
- If you like, you can exchange slots…
- … but both students must agree, and let us know in advance
- E-mail robert.watson@cl.cam.ac.uk, CCing other student
- As term passes, we will seek volunteers for remaining slots
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 our other readings
  - Consider current-day research and applications
  - Prepare for adversarial Q&A - defend the work

- Don’t just follow paper outline
- Presentations without pictures (like this one) are uninspiring!

Your slides

- For avoidance of doubt: you will present with slides
- All presentations will be from our notebooks
- Slides must be in PDF format - no fancy animations; builds OK
- Submit slides by e-mail no later than 10:00 on the day of presentation to acs-2013-r209-slides@cl.cam.ac.uk
- Also submit on paper to graduate education office
- Late submission will be heavily penalised due to disruption it will cause to other students
- Usually presented within class in roughly syllabus order
Class discussions

- Roughly half of each two-hour meetings set aside for discussion
- Bring discussion questions to class and be prepared to discuss them
- No explicit marks for participation…
- … but presenter is rewarded for interesting discussion, so mutual benefit to participating!

Other admin things
Course e-mail

- From now on, we will be e-mailing you using your Cambridge CRSid
- We will be sending reading and schedule updates, clarifications, etc. there!
- If you are not registered, but are sitting in, please e-mail robert.watson@cl.cam.ac.uk so that I can add you to the mailing list
- Recurring guests will usually be asked to present once during the term

Course web site

- Reading list, marking criteria, etc. found here: http://www.cl.cam.ac.uk/teaching/1314/R209/
- Beginnings of next term’s website here: http://www.cl.cam.ac.uk/teaching/1314/R210/
How to reach us

robert.watson@cl.cam.ac.uk
ross.anderson@cl.cam.ac.uk
frank.stajano@cl.cam.ac.uk
steven.murdoch@cl.cam.ac.uk

acs-2013-r209-essays@cl.cam.ac.uk
acs-2013-r209-slides@cl.cam.ac.uk

R209 weekly meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 Oct</td>
<td>Origins of computer security*</td>
<td>RNMW, RJA</td>
</tr>
<tr>
<td>21 Oct</td>
<td>The economics of security</td>
<td>RJA</td>
</tr>
<tr>
<td>28 Oct</td>
<td>Cryptographic protocols: possibilities and limitations</td>
<td>RJA</td>
</tr>
<tr>
<td>4 Nov</td>
<td>Passwords: technology, human factors, and what goes wrong</td>
<td>FMS</td>
</tr>
<tr>
<td>11 Nov</td>
<td>Access control and adversarial reasoning</td>
<td>RNMW</td>
</tr>
<tr>
<td>18 Nov</td>
<td>Hardware and software capability systems</td>
<td>RNMW</td>
</tr>
<tr>
<td>25 Nov</td>
<td>Programming language and information-flow security</td>
<td>RNMW</td>
</tr>
<tr>
<td>2 Dec</td>
<td>Correctness vs. mitigation</td>
<td>RNMW</td>
</tr>
</tbody>
</table>

*First session is a bit unusual because no student presentations/essays
Last year’s R210 topics
(may differ somewhat this year, but should be similar)

<table>
<thead>
<tr>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covert and anonymous communications</td>
</tr>
<tr>
<td>Tampering with hardware</td>
</tr>
<tr>
<td>Bootstrapping security relationships</td>
</tr>
<tr>
<td>Behavioural economics of privacy</td>
</tr>
<tr>
<td>Social network security</td>
</tr>
<tr>
<td>API security</td>
</tr>
<tr>
<td>Mobile system security</td>
</tr>
<tr>
<td>Psychology and security</td>
</tr>
</tbody>
</table>

Introductions
Some thoughts on computer security

A few key themes

- Methodologies and tools
- “Making and breaking”
- Assurance arguments and verification
- Certification
- Pure and applied cryptography
- Protocols, security APIs, and boundaries
- Prevention vs. mitigation
- Policy representation, but also policy development
- Tensions between security and representation
- Adversarial vs. probabilistic views of bugs
- Local vs. distributed system behaviour
- National state-level actors
- Humans and computers as parts of larger systems
Questions?

Protection of Information in Computer Systems
Saltzer and Schroeder, 1973-1975
A Note on the Confinement Problem
Lampson, 1973

New Directions in Cryptography
Diffie and Hellman, 1976
Using Encryption for Authentication in Large Networks of Computers
Needham and Schroeder, 1978