ACS/Part III R209

Principles and foundations of computer security

Dr Robert N. M. Watson
Professor Ross Anderson
Dr Frank Stajano

4 October 2012
Welcome!

- Computer security
- “Seminar-style” research readings courses
  - R209 Michaelmas term
    - History, discourse, methodology, and themes
  - R210 Lent term
    - Current research topics
- Ambitious scope, limited time
Prerequisites

• Undergraduate degree or a strong grounding in computer science
• Ideally at least one past course in operating systems, networks, or security
• This course is about gaining research-level insight into a field you have already studied
• R210 next term digs into current research topics in computer security in greater detail
Brushing up on computer security


Seminar-style courses?

• Preparation for research in the field
  • Study vocabulary and discourse
  • Trace and discuss intellectual history
  • Consider contemporary implications
  • Identify future research directions

• Each week you will …
  • … read 3-4 critical research papers per week
  • … submit synthesis essays (80%)
  • … participate in student-led presentation and discussion (20%)
Weekly essays
Synthesis essay

- *Synthesis writing* reports, organises, and interprets readings
- *Synthesis essays are not* original research papers
- Typical outline might be:
  1. Summary of papers (1-2 para/paper)
  2. Discussion of key themes (2-4 para)
  3. Consideration of contemporary context (1-2 para)
  4. Literature review (1-2 para)
  5. Class discussion questions (4 is a good number)
- All papers must include *references*
- If this is new to you, Google “synthesis essay”
Essay marking notes

- 10 points each for 7 essays, scaled to 80% of total course mark
- Marks are divided evenly across these five essay aspects; totals…
  - 0 - not submitted (or remarkably bad!)
  - 1-4 - seriously lacking
  - 5-6 - adequate
  - 7-8 - good
  - 9-10 - exceptional
- 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
Essay submission

• Submit on paper to the graduate education office
• Must be received by noon on the Tuesday before we meet
• Marks will usually be returned via the graduate education office the following week
• Please also e-mail an electronic copy, in PDF format, to acs-2012-r209-essays@cl.cam.ac.uk.
• Bring discussion questions to class
Weekly presentations
Student presentations

- 7 sessions, 3 talks/session, 15 minutes each
  - You will present (roughly) twice this term
  - This means a few of you may do three talks
  - Scores are normalised
- We provide an initial talk schedule by e-mail shortly
  - If you like, you can exchange slots…
  - … but both students must agree, and let us know in writing at least one week in advance
  - E-mail robert.watson@cl.cam.ac.uk, CCing other student
Presentation structure

- Introduction, motivation, methodology, (possible) evaluation, related work, and contemporary implications
- Prepare a teaching- or research-style presentation
  - Teach the key ideas
  - Present the good and the bad
  - Trace related research
  - Consider contemporary 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!
Notes on slides

• All presentations from our notebooks
• Slides must be in PDF format
  • Sorry, no fancy animations; builds OK
• Submit slides by e-mail no later than 10:00am on the day to acs-2012-r209-slides@cl.cam.ac.uk.
• Late submission will be heavily penalised
• Most often presented in the syllabus order
Class discussions

- Nearly half of our 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
Course web site

- Reading list, marking criteria, etc. found here:

  http://www.cl.cam.ac.uk/teaching/1213/R209/
How to reach us

robert.watson@cl.cam.ac.uk
ross.anderson@cl.cam.ac.uk
frank.stajano@cl.cam.ac.uk
acs-2012-r209-essays@cl.cam.ac.uk
acs-2012-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>4 Oct</td>
<td>Origins and foundations of computer security</td>
<td>RNMW</td>
</tr>
<tr>
<td>11 Oct</td>
<td>Access control systems</td>
<td>RNMW</td>
</tr>
<tr>
<td>18 Oct</td>
<td>Hardware and software capability systems</td>
<td>RNMW</td>
</tr>
<tr>
<td>25 Oct</td>
<td>Programming language and information flow security</td>
<td>RNMW</td>
</tr>
<tr>
<td>1 Nov</td>
<td>The economics of security</td>
<td>RJA</td>
</tr>
<tr>
<td>8 Nov</td>
<td>Passwords: technology, human factors, and what goes wrong</td>
<td>FMS</td>
</tr>
<tr>
<td>15 Nov</td>
<td>Cryptographic protocols: possibilities and limitations</td>
<td>RJA</td>
</tr>
<tr>
<td>22 Nov</td>
<td>Correctness vs. mitigation*</td>
<td>RNMW</td>
</tr>
</tbody>
</table>

* Paper selection to be confirmed
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