ACS/Part III R210

Current applications and research in computer security

Dr Robert N. M. Watson, Professor Ross Anderson,
Dr Frank Stajano, Dr Steven Murdoch

+ several guest conveners

18 January 2013

NB: this version contains corrections to e-mail addresses that were incorrect in an earlier version

Welcome (back)!

- Computer security
- *Seminar-style* research readings courses
  - R209 Michaelmas term
    - History, discourse, methodology, and themes
  - R210 Lent term
    - Active research topics of local interest
- Ambitious scope, limited time

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%)

Less focus than in R210

More focus than in R210

Changes from R209

- Content: focus on active research
- Continuing uncertainty on room assignment
- Essay format adjustments for R210
- E-mail addresses changes:

  acs-2013-r210-essays@cl.cam.ac.uk
  acs-2013-r210-slides@cl.cam.ac.uk

R210 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 **future research directions** (1-2 para)
  4. Literature review (1-2 para)
  5. Class discussion questions (4 is a good number)
- All papers must include references
- Revised word limit: **1,750** words; aim for 1,500 or lower

Change from R209: all topics are contemporary, so we will shift essay section focus to new ideas

Change from R209: many of you were writing longer essays — wanted to confirm this is OK. However, pithy is good.

UNIVERSITY OF CAMBRIDGE

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

Submission

- Submit on paper to the graduate education office
- Please also e-mail copies to acs-2013-r210@cl.cam.ac.uk
- Must be received by **noon** on the **Wednesday** before we meet
- Marks will usually be returned via the graduate education office the following week
- Bring discussion questions to class

Change from R209: essays due on Wednesdays not Tuesdays

Student presentations

- 8 sessions, 3 talks/session, 15 minutes each
  - You will present 2-3 times this term
  - Scores are normalised
- We have provided a schedule for the first five sessions; others to follow in the next week
  - If you like, you can exchange slots…
  - … but both students must agree, and let us know **in writing at least two days in advance**
  - E-mail acs-2013-r210-slides@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 **future research directions**
  - ➡ Prepare for adversarial Q&A - defend the work
- Don't just follow paper outline
- Presentations without pictures (like this one) are uninspiring!

Change from R209: shift focus forward: what might be done to extend research in this area?

Notes on slides

- All presentations from our notebooks
- Slides must be in PDF form
  - Sorry, no fancy animations; builds OK
- Submit slides **by e-mail** no later than **10:00am** on the day of presentation
  - Use acs-2013-r210-slides@cl.cam.ac.uk not our personal e-mail addresses
- Late submission of slides will be **heavily penalised**
- Most often in the order listed in the syllabus

Question last term:

Do we expect all talks to use slides?

Yes.

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!

Course e-mail

- We are e-mailing your CRSid with presentation assignments, schedule and room updates, clarifications, etc.
- 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/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

R210 weekly meetings

Date	Topic	Leader
18 Jan	Covert and anonymous communications	SJM
25 Jan	Tampering with hardware	SPS
1 Feb	Bootstrapping security relationships	FMS
8 Feb	Behavioural economics of privacy	SDP
15 Feb	Mobile system security	ARB, LMRS
22 Feb	TBC* Possible topics: Internet infrastructure security, API	-
1 Mar	TBC* security, payment systems, clean-slate host security,	-
8 Mar	TBC* malware reverse engineering, social networks	-

* Paper selection to be confirmed

Introductions

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?