ACS/Part III R209 Computer Security: Principles and Foundations

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

14 October 2014

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

- Undergraduate computer-science degree
  - Or similar education/experience
  - Ideally included operating systems, networking, computer security
- Some topics will be familiar, but recast as research rather than ‘truth’
- Other topics will not yet be widely taught

Goal: transition from ‘factual’ understanding to engagement with core debates, intellectual history, methodology, evolution of the field

Brushing up on computer security

Anderson, R. J., Security Engineering (second edition), Wiley, 2008.

Gollmann, D., Computer Security, Wiley, 2010.

McKusick, M. K., Neville-Neil, G. N., and Watson, R. N. M. Design and Implementation of the FreeBSD Operating System (second edition): Chapter 5 – Security, Pearson, 2014.

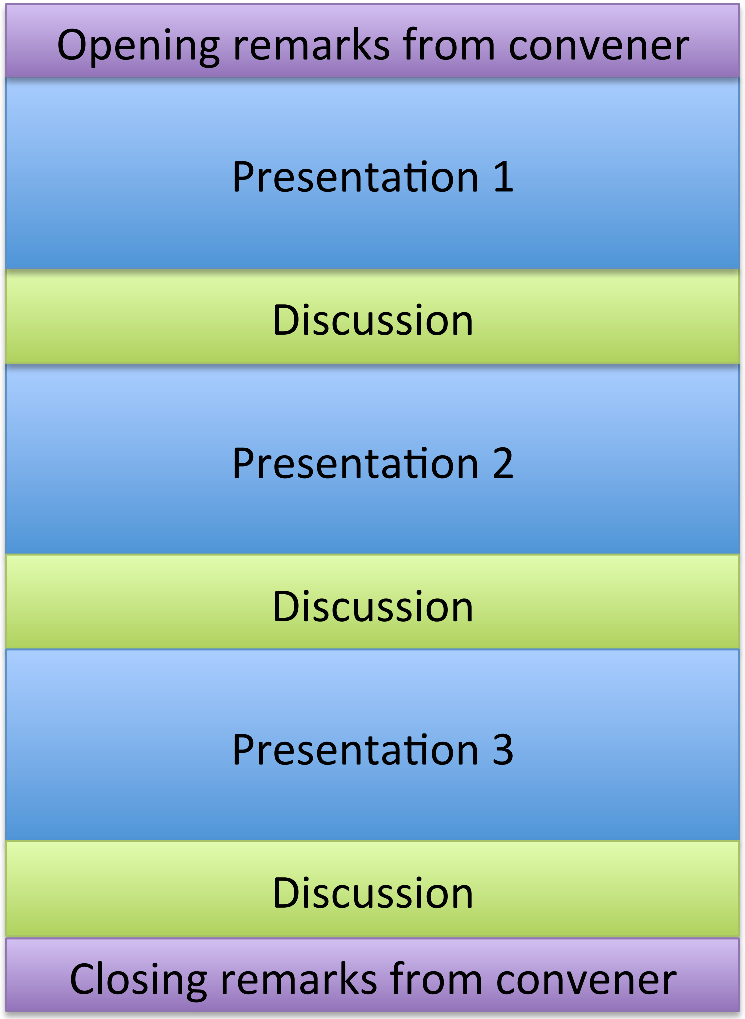
Seminar-style teaching (1)

- Preparation for research and development
  - Trace intellectual history
  - Study evolving vocabulary and discourse
  - Appreciate (and critique) original 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:
  - Critically read three original papers/reports
  - Submit synthesis essays across all readings
    or
  - Present and lead discussion on a specific reading
  - Participate in classroom discussion of the readings

Typical class structure



Opening remarks from convener

Presentation 1

Discussion

Presentation 2

Discussion

Presentation 3

Discussion

Closing remarks from convener

- 15–20-minute student presentations
- 5–10-minute student-led discussions
- All R209/R210 sessions except the first one

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 each term will be dropped
  - R209: typically the first essay; consider this a 'practice run'
- Remaining scores scaled to a percent
- Department aggressively penalizes late submissions
  - Instructors cannot grant extensions
  - If you are ill or have a conflict (e.g., a deadline in another module), contact the graduate education office **as soon as possible** to negotiate deadlines

WEEKLY ESSAY

Synthesis Essays

- *Synthesis writing* reports, organizes, and interprets the work of others - **not an original research paper**
- We specify a highly formulaic essay; no explicit thesis required:

  1. Summaries of readings (1-2 para/reading)
  2. Discussion of three key themes (1 para/theme)
  3. Consider ideas in contemporary (today's) context (1-2 para)
  4. Literature review (2 para)
  5. Class discussion questions (4 bullet points)

- We recommend using explicit section headings
- All essays must include a bibliography
- If this is an unfamiliar style, Google 'synthesis essay'

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

- Your first essay will likely have a lower mark than you hope, but will likely be dropped as the lowest of the term
- Do worry – but not too much; experience suggests your next essay will be dramatically better as you become used to the writing style and our expectations

Essay Submission

- Submit on paper to the graduate education office
- E-mail as PDF to: acs-2014-r209-essays@cl.cam.ac.uk
- Deadline 12:00 on the Monday before we meet
- Marks and comments will be 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
- We hope to return the first batch of essays more quickly to help guide later essay writing
- Bring discussion questions to class and be prepared to ask (and answer) them

Weekly Presentations

- 7 sessions, 3 talks/session, 15 minutes each
  - You will present at least once per term
  - No essay due for meeting 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 presentation slots…
  - … but both students must agree; let us know in advance
- E-mail robert.watson@cl.cam.ac.uk
- We are seeking 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 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

- You will present with slides
- All presentations will be from a computer we provide
- Slides must be in PDF format - no fancy animations; builds OK
- Submit slides by e-mail no later than 12:00 on the Monday before the presentation to acs-2014-r209-slides@cl.cam.ac.uk
- Also submit on paper to graduate education office
- Late submission will be heavily penalized due to disruption it will cause to other students
- Usually presented within class 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 raise 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 surveys
- Highly cited and/or first appearance of key ideas
- 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)

- As you read, take notes/highlight ideas that answer questions for your essay:
  - Framing/motivation of the paper
  - Key ideas that influenced the paper
  - Key contributions of the paper – and their implications
  - Evaluation approach, limitations
  - Common ideas across the papers
- In some cases, you may need to skim due to volume
- You will get faster at reading; papers written more recently will [often] be more accessible
- See Keshav's "How to Read a Paper", CCR 2007

ADMIN THINGS

Module E-mail

- We will be e-mailing you using your CRSid
- We will send reading and schedule updates, clarifications, room changes, etc. there!
- 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 once during the term

Module Website

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

  http://www.cl.cam.ac.uk/teaching/1415/R209/

- Beginnings of next term's website here:

  http://www.cl.cam.ac.uk/teaching/1415/R210/

- 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

alastair.beresford@cl.cam.ac.uk

acs-2014-r209-essays@cl.cam.ac.uk

acs-2014-r209-slides@cl.cam.ac.uk

R209 Weekly Meetings

Date	Topic	Convener(s)
14 Oct	Origins of computer security	Watson, Anderson
21 Oct	Access control	Watson
28 Oct	Capability systems	Watson
4 Nov	Passwords	Stajano
11 Nov	Cryptographic protocols	Anderson
18 Nov	Programming-language security and information flow control	Beresford
25 Nov	Correctness vs. mitigation	Watson
2 Dec	Security economics	Anderson

R210 Weekly Meetings
(last year's, but a good predictor)

Session	Topic	Convener
1	Covert and anonymous communications	Murdoch
2	Bootstrapping security protocols	Stajano
3	Mobile-system security	Beresford
4	Censorship resistance	Murdoch
5	Psychology and security	Anderson
6	Banking security	Bond
7	Social-network security	J. Anderson
8	Hardware security	Skorobogatov

SOME KEY THEMES

A Few Key Themes

- Methodologies and tools
- ‘Making and breaking’
- Assurance arguments and verification
- Integrity, confidentiality, and availability
- Certification
- Pure and applied cryptography
- Protocols, security APIs, and boundaries
- Prevention vs. mitigation
- Policy representation and development
- Security and program representation
- Local vs. distributed systems
- Nation-state actors
- Humans and computers as part of larger systems
- Compliance budgets
- Economic framing for security
- Designing for change

QUESTIONS

INTRODUCTIONS

TODAY’S READINGS

Saltzer and Schroeder, 1973-1975

PROTECTION OF INFORMATION IN COMPUTER SYSTEMS

Protection of Information in Computer Systems (Saltzer and Schroeder)

- Survey paper covering state-of-the-art of local security in 1975
- One of the most cited papers in computer security
  - Security vs. privacy; confidentiality, integrity, availability
  - Systems with varying levels of protection model
  - Discretionary vs. mandatory protection; object labeling
  - Principle of least privilege, separation of privilege, economy of mechanism, human factors, work factor, audit trails
  - Isolation/protection as a foundation for compartmentalization
  - Authorization; Capabilities vs. Access Control Lists (ACLs)
  - Dynamic enforcement including protected subsystems (encapsulation)
  - The challenges of revocation
  - Authentication and the psychology of security,
- Future research directions and challenges; e.g., verification
- What topics are not raised? How has our framing has changed?

Lampson, 1973

A NOTE ON THE CONFINEMENT PROBLEM

A Note on the Confinement Problem (Lampson 1973)

- Also heavily cited for a critical contribution to the field
- One phrase: *covert channel*
  - Not unlike the *halting problem*: a fundamental limitation
  - Source of suffering for 10-20 years of research
  - Tradeoff between resource investment and effective isolation
  - Can you find them? Measure them? Prevent them?
  - Does this idea come up in PICS?
  - Can the technologies in PICS solve this problem?
- Suddenly relevant again
  - Anonymity technologies
  - Anti-censorship technologies
- Compare/contrast: *covert channel* and *side channel*?

Diffie and Hellman, 1976

NEW DIRECTIONS IN CRYPTOGRAPHY

Needham and Schroeder, 1978

USING ENCRYPTION FOR AUTHENTICATION IN LARGE NETWORKS OF COMPUTERS