

ACS/Part III R209

Computer Security: Principles and Foundations

Professor Ross J. Anderson

Dr Robert N. M. Watson

Dr Alice Hutchings

10 October 2022

Introductions

- Name, background
- Interest in security
- What you hope to learn, or better understand, at the end of this module

Today's Class

1. Module introduction
2. Presentation and discussion: ***Reflections on Trusting Trust***
3. Video and discussion: ***Chip and PIN is broken***
4. Presentation and discussion: ***Experimental Security Analysis of a Modern Automobile***
5. Brief summary of next week: Usable security

Welcome!

- *Seminar-style* research readings module
- **R209: Computer Security: Principles and Foundations** (Michaelmas)
 - History, discourse, methodology, and themes
 - Topics include adversarial reasoning, access control, usability, inference control, ...
- **R254: Cybercrime** (Lent)
 - Interdisciplinary perspective
 - Focus on key debates, research and policy
 - What cybercrime is, how it is regulated, policed, detected, and prevented
- Ambitious scope, limited time

Prerequisites

Goal: Transition from **simplistic factual** understanding to **research 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

Anderson, R. J., **Security Engineering** (3rd edition), Wiley, 2020.

Gollmann, D., **Computer Security** (3rd edition), Wiley, 2010.

McKusick, M. K., Neville-Neil, G. N., and Watson, R. N. M., **Design and Implementation of the FreeBSD Operating System** (2nd edition): *Chapter 5 – Security*, Pearson, 2014.

Seminar-style teaching

- Preparation for research and development
 - Trace intellectual history
 - Study evolving vocabulary, discourse, and methodology
 - Discuss, learn from, and challenge methodological and narrative aspects of the research
 - Appreciate (+critique) research as published -- and various styles of academic analysis and presentation
 - Consider contemporary implications; contrast with original research context
 - Discuss future research directions
- 6x sessions: Student-led presentation + discussion
- 1x session: Small-group discussions of the essays
- In-person, with remote attendance via Zoom possible for anyone isolating. No recordings.

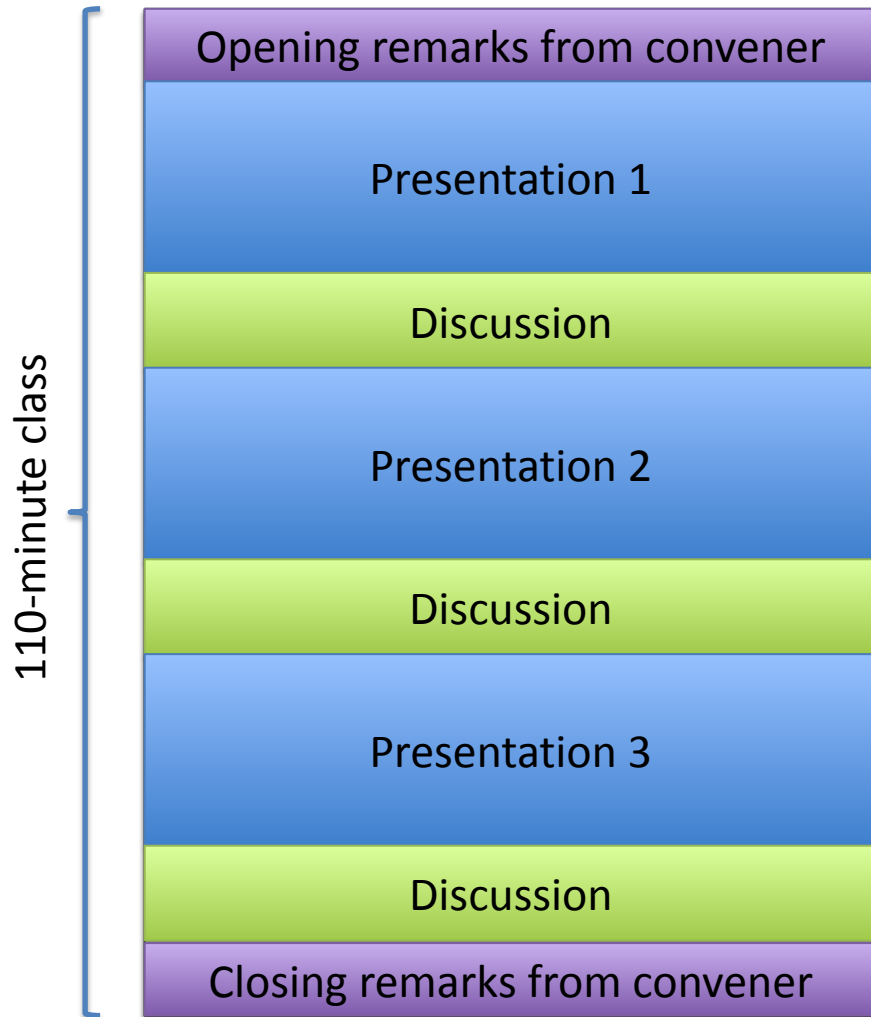
Presentation weeks (6x)

Each presentation week you will:

1. Critically read three original papers/reports
2. Submit synthesis essays across all readings (unless presenting)
- or -
2. Present and lead discussion on a specific reading
3. Participate in classroom discussion of the readings

(Guest PhD students, postdocs in the class will present papers but not submit essays)

Class structure (presentation weeks)



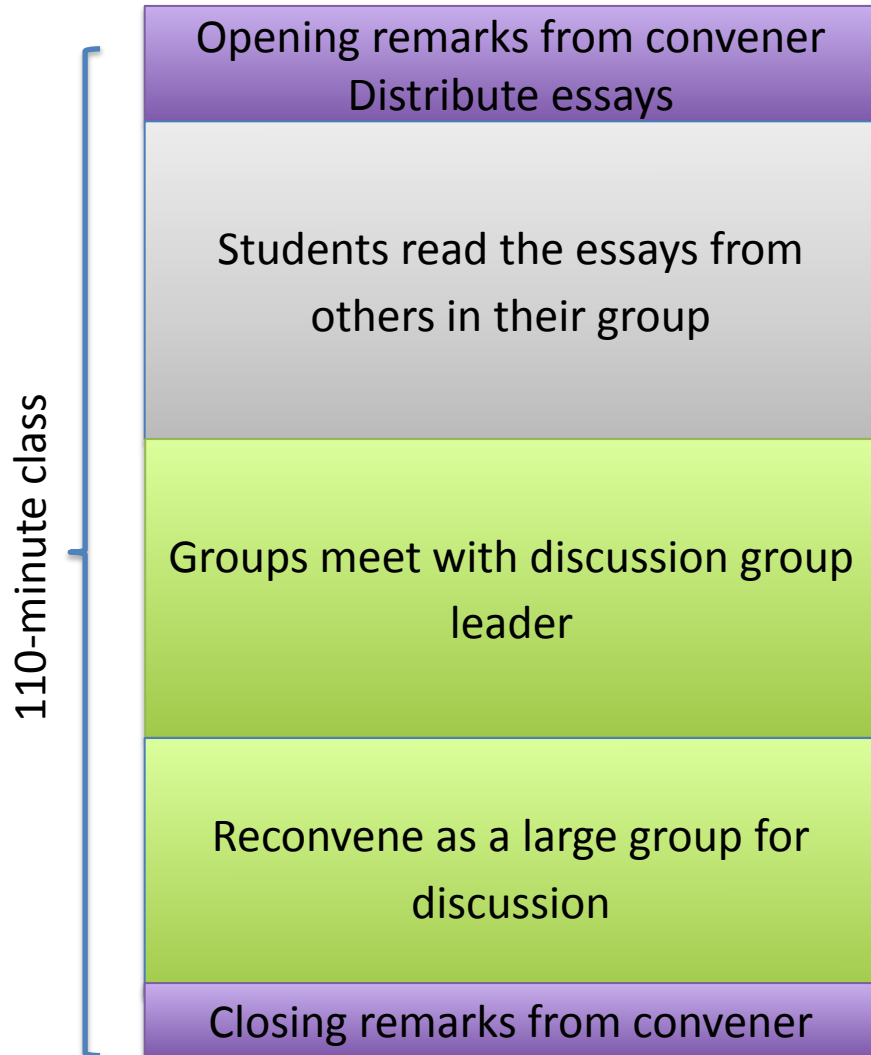
- Weeks 3-8
- 3x 15–to–20-minute student presentations **(do not run shorter/longer!)**
- 3x 15–to–20-minute student-led discussions
- Discussions are cumulative: pull ideas forward as we look at later papers

Essay discussion weeks (1x)

In week 2 you will:

1. Critically read three original papers/reports
2. Submit synthesis essays across all readings
3. Participate in classroom discussion of the readings and essays, first as smaller groups, and then as a single large group

Class structure (essay discussions)



- Week 2 only
- Introductions to the week; distribute essays to others
- Read the essays from others in group
- Group discussion at 14:45
- Reconvene at 15:25 as a large group for discussion
- Closing remarks

Assessment

- One presentation or essay a week
 - R209: Seven total (none today)
- 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 heavily penalizes late submissions
 - Instructors cannot grant extensions
 - Contact the graduate education office **as early as possible**

WEEKLY ESSAY

Synthesis Essays

- **Synthesis writing** reports, organizes, and interprets the works of others
 - Not an original research paper!
 - More a series of short answers than an actual essay
- Your essays **will** have the following section 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)
- All essays **must** include a bibliography
- Word limit (1,250) enforced (excl. bibliography)
- **See Assessment page on module website**

Notes on essay marking

- 10 divided equally across four sections plus 2 marks for overall delivery (quality of writing, ...):

0	failed to submit
1-4	seriously lacking
5-6	poor or (minimally) adequate
7-8	good
9-10	strong or 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 via Moodle**
- Bring discussion questions to class and be prepared to ask (and answer) them
- Marks/comments returned via Moodle
- We attempt to return essays to you within two weeks, but sometimes this is not possible

Weekly Presentations

- 6 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

R209 Weekly Presentations

Date	Topic	Paper	Presenter
24 Oct	Access Control	Bell & LaPadula (1973) Wagner & Tribble (2002) Watson (2013)	pd538 kw543 mbg34
31 Oct	Correctness v. Mitigation	Klein et al. (2009) Bessey et al. (2010) Davis et al. (2019)	ak2427 rm2084 ots28v
7 Nov	Inference Control	Adams & Wortmann (1989) Dwork et al. (2006) Narayanan & Shmatikov (2007)	zw420 qz312 dgk27
14 Nov	Adversarial Reasoning II	Razavi et al. (2016) Bond et al. (2014) Kocher et al. (2019)	dg612 wta22 yx375
21 Nov	Security Economics	Anderson & Moore (2009) van Eeten et al. (2010) Vasek & Moore (2015)	jw2282 at2008 jp862
28 Nov	Passwords	Morris & Thompson (1979) Adams & Sasse (1999) Bonneau et al. (2012)	psjm3 zyj20 mcf61

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 Presentations

- **You will present with slides**
 - Slides will be in **PDF format** – no fancy animations
- Submit slides no later than 12:00 on the Monday:
 - Submit slides via Moodle
 - Failure to prepare or submit will be heavily penalized due to disruption it will cause
- Usually presented in syllabus order

Class Discussion

- Presentation weeks: Roughly half of each two-hour class is set aside for discussion
- Essay discussion week: All discussion
- Bring discussion questions to class and be prepared to ask (and answer) them
- No explicit marks for participation...
 - ... but presenters are 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?
 - What methodology do the papers use: 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 alice.hutchings@cl.cam.ac.uk
- Recurring guests (e.g., PhD students, RAs) will be asked to present 1-2 times during the term

Module Website

- Reading list, marking criteria, etc. found here:
<https://www.cl.cam.ac.uk/teaching/2223/R209/>
- Look at the 'Materials', 'Assessment' pages

R209 Weekly Meetings

Date	Topic	Convener(s)
10 Oct	Adversarial Reasoning	Anderson, Watson, Hutchings
17 Oct	Usable Security	Hutchings
24 Oct	Access Control	Watson
31 Oct	Correctness v. Mitigation	Watson
7 Nov	Inference Control	Anderson
14 Nov	Adversarial Reasoning II	Anderson
21 Nov	Security Economics	Anderson
28 Nov	Passwords	Hutchings

How to Reach Us

ross.anderson@cl.cam.ac.uk

robert.watson@cl.cam.ac.uk

alice.hutchings@cl.cam.ac.uk

Security Group Seminars & Meetings

- Seminars every Tuesday at 2pm
<https://www.cl.cam.ac.uk/research/security/seminars/>
- Security group meetings every Friday at 4pm
<https://www.cl.cam.ac.uk/research/security/meetings/>

QUESTIONS

TODAY'S READINGS