ACS/Part III R209 Computer Security: Principles and Foundations

Professor Alastair Beresford
Professor Alice Hutchings
Dr Martin Kleppmann
Professor Robert N. M. Watson

9 October 2025

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: ***Thunderclap: Exploring Vulnerabilities in Operating System IOMMU Protection via DMA from Untrustworthy Peripherals***
3. Presentation and discussion: ***Spy-oT: Understanding how users learn to use Internet of Things devices for abusive purposes***
4. 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, security economics, …
- **R354: Cybercrime** (Lent)
  - Interdisciplinary perspective
  - Focus on key debates, research and policy
  - What cybercrime is, how it is regulated, policed, detected, and prevented
- **P79: Cryptography and Protocol Engineering** (Lent)
  - "From math to metal": practical details of implementing cryptographic algorithms
  - Focus on good engineering practice, testing, robustness
- 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, computer architecture, cryptography …
- 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.

Free chapters available from https://www.cl.cam.ac.uk/archive/rja14/book.html

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

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
- 1x session: Instructor-led presentations
- 1x session: Small-group discussions of the essays
- 6x sessions: Instructor and student-led presentations + discussion
- In-person, with remote attendance via Zoom possible for anyone unwell. No recordings. Please give us as much warning as possible so we can make arrangements.

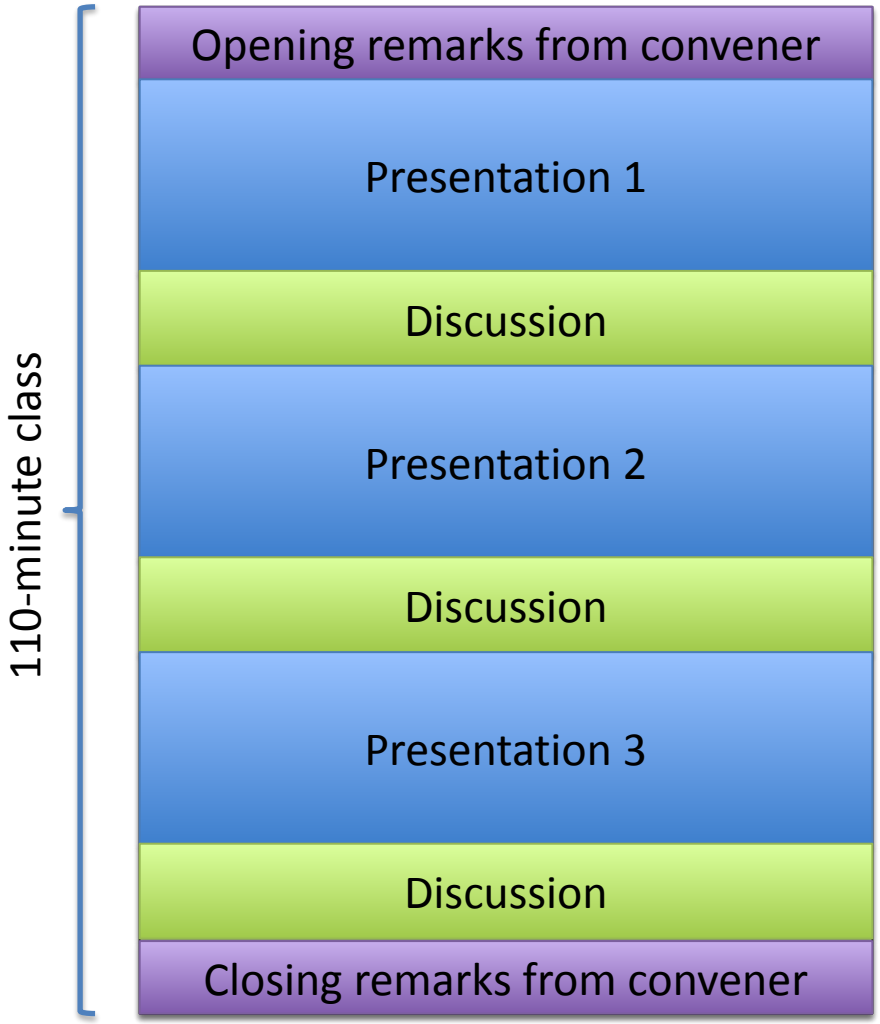
Presentation weeks (6x)

Each presentation week you will:

1. Critically read three original papers/reports
2. If assigned, submit synthesis essays across all readings
3. If assigned, present and lead discussion on a specific reading
4. 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 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)

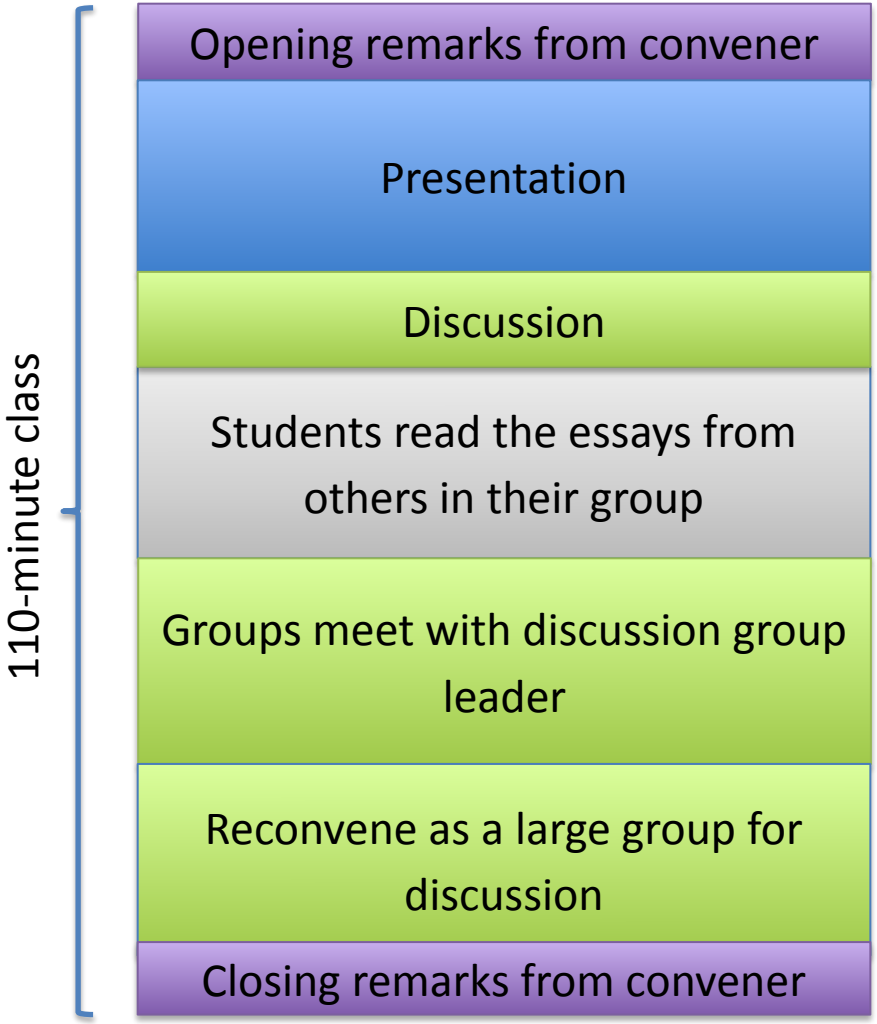
In week 2 you will:

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
- Introduction and one 15 min presentation
- Discussion
- Distribute essays in groups, time for reading
- Group discussion
- Reconvene as a larger group for discussion
- Closing remarks

Assessment

- Four essays and one presentation, each worth 20%
- Topics to be randomly allocated at the start of term
- 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**

R209 Weekly Essays

Date	Topic	Essay allocation
15/10	Usable Security	All students
23 Oct	50 Years of Access Control	zz479, jd2125, va371, ip442, mafr2
30 Oct	Leveraging hardware vulnerabilities	fk407, bs735, va371, mjc316, mafr2
6 Nov	Security Economics	sn630, jd2125, ip442, mjc316
13 Nov	Correctness v. Mitigation	fk407, zz479, bs735, mafr2
20 Nov	Cryptographic Identity	sn630, zz479, jd2125, ip442
27 Nov	Metadata-Private Communications	sn630, fk407, bs735, va371, mjc316

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

Essay Submission

- Deadline 11:00 on the Tuesday 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 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

R209 Weekly Presentations

Date	Topic	Paper	Presenter
23 Oct	50 Years of Access Control	Bell & LaPadula (1973) Wagner & Tribble (2002)	sn630 fk407
30 Oct	Leveraging hardware vulnerabilities	Razavi et al. (2016) Kocher et al. (2019)	zz479 jd2125
6 Nov	Security Economics	van Eeten et al. (2010) Vasek & Moore (2015)	bs735 hp509
13 Nov	Correctness v. Mitigation	Klein et al. (2009) Bessey et al. (2010)	va371 ip442
20 Nov	Cryptographic Identity	Melara et al. (2015) McKelvey et al. (2021)	qw304 mjc316
27 Nov	Metadata-Private Communications	Dingledine et al. (2004) Piotrowska et al. (2017)	mafr2 ap2453

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 11:00 on the day you present:
  - 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

- Roughly half of each two-hour class is set aside for discussion (more for week 2).
- 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/2526/R209/

- Look at the ‘Materials’, ‘Assessment’ pages

R209 Weekly Meetings

Date	Topic	Convener(s)
9 Oct	Adversarial Reasoning	Watson, Hutchings
16 Oct	Usable Security	Hutchings
23 Oct	Fifty Years of Access Control	Watson
30 Oct	Adversarial Reasoning II	Beresford
6 Nov	Security Economics	Hutchings
13 Nov	Correctness v. Mitigation	Watson
20 Nov	Cryptographic Identity	Kleppmann
27 Nov	Metadata-Private Communications	Kleppmann, Beresford

How to Reach Us

Alastair Beresford: arb33@cam.ac.uk

Alice Hutchings: ah793@cam.ac.uk

Martin Kleppmann: mk428@cam.ac.uk

Robert Watson: robert.watson@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 2pm
  https://www.cl.cam.ac.uk/research/security/meetings/

QUESTIONS

TODAY'S READINGS