ACS/Part III R209
Computer Security:
Principles and Foundations

Professor Ross J. Anderson
Dr Alastair Beresford
Dr Daniel Thomas

8 October 2018

Slides originally by Dr Robert N. M. Watson

Today's Class

1. Module introduction
2. Paper: ***Protection of Information in Computer Systems***
3. Paper: ***Using Encryption for Authentication in Large Networks of Computers***
4. Discussion: security motivations and methodology

Welcome!

- *Seminar-style* research readings module
- **R209: Principles and Foundations** (Michaelmas)
  - History, discourse, methodology, and themes
  - Topics include crypto/protocols, human factors, economics, vulnerability mitigation, …
- **R254: Cybercrime** (Lent)
  - Cybercrime from an interdisciplinary perspective
- Ambitious scope, limited time

Prerequisites

Goal: Transition from **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** (2nd edition), Wiley, 2008.

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 (1)

- Preparation for research and development
  - Trace intellectual history
  - Study evolving vocabulary, discourse, and methodology
  - Discuss and learn from methodological and narrative aspects of the research
  - Appreciate (+critique) research as published
  - Consider contemporary implications; contrast with original research context
  - Discuss future research directions
- Student-led presentation and discussion is central to this format

Seminar-style teaching (2)

Each week you will:

1. Critically read three original papers/reports

2. Submit synthesis essays across all readings

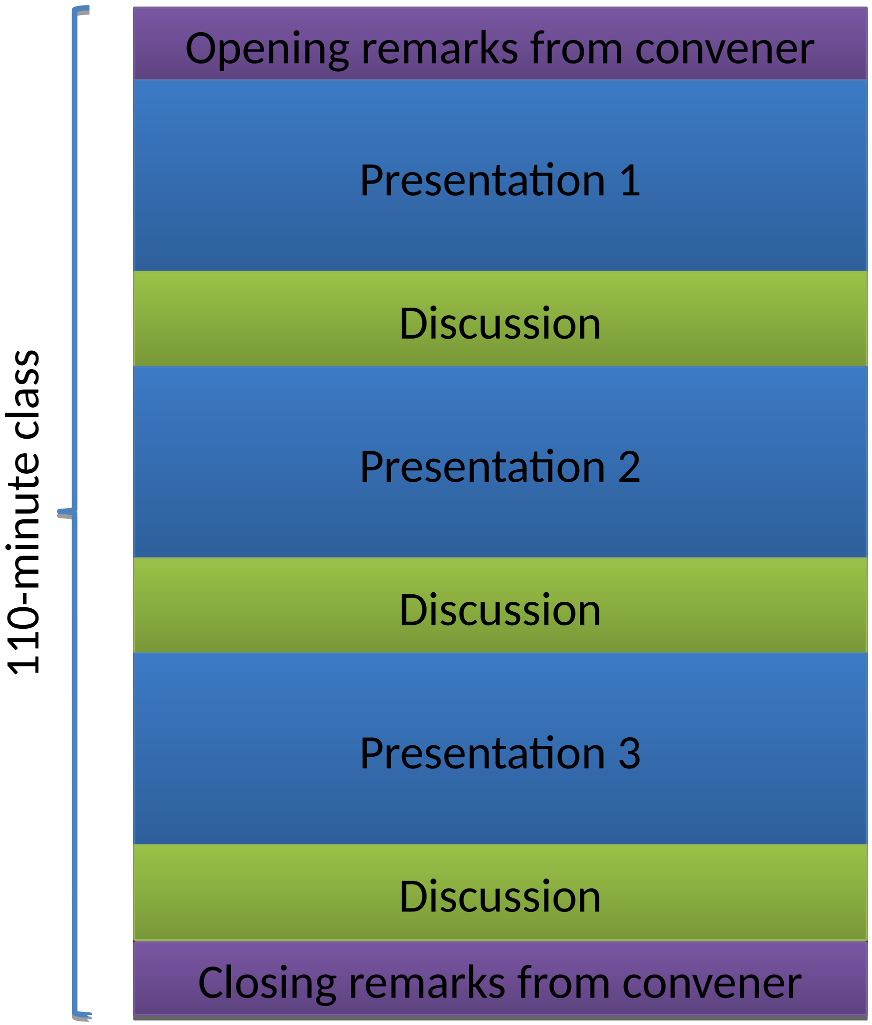
or

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 not present papers or submit essays)

Typical class structure



110-minute class

Opening remarks from convener

Presentation 1

Discussion

Presentation 2

Discussion

Presentation 3

Discussion

Closing remarks from convener

- 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

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

- 7 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

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 Slides

- **You will present with slides**
  - All presentations will be on our computer
  - Slides will be in **PDF format** – no fancy animations
- Submit slides via Moodle no later than 12:00 on the Monday
  - Failure to prepare or submit will be heavily penalized due to disruption it will cause
- Usually presented roughly in 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 ask (and answer) 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 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 daniel.thomas@cl.cam.ac.uk
- Recurring guests may be asked to present times during the term if we develop gaps

Module Website

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

https://www.cl.cam.ac.uk/teaching/1819/R209/

- Next term’s website here:

https://www.cl.cam.ac.uk/teaching/1819/R254/

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

R209 Weekly Meetings

Date	Topic	Convener(s)
8 Oct	Origins and Foundation of Computer Security	Thomas, Anderson, Beresford
15 Oct	Adversarial Reasoning	Anderson
22 Oct	Access Control	Beresford
29 Oct	Cryptographic Protocols	Anderson
5 Nov	Correctness vs. Mitigation	Thomas
12 Nov	Usable Security	Beresford
19 Nov	Security Economics	Anderson
26 Nov	Passwords	Beresford

How to Reach Us

ross.anderson@cl.cam.ac.uk

alastair.beresford@cl.cam.ac.uk

daniel.thomas@cl.cam.ac.uk

Daniel may be on paternity leave from mid November so email Ross and Alastair as well.

QUESTIONS

INTRODUCTIONS
WHAT IS SECURITY?

TODAY’S READINGS

ACS/Part III R209
Computer Security: Principles and Foundations

Professor Ross J. Anderson
Dr Alastair Beresford
Dr Daniel Thomas

8 October 2018

Slides originally by Dr Robert N. M. Watson

Today’s Class

1. Module introduction
2. Paper: ***Protection of Information in Computer Systems***
3. Paper: ***Using Encryption for Authentication in Large Networks of Computers***
4. Discussion: security motivations and methodology

Prerequisites

Goal: Transition from **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** (2nd edition), Wiley, 2008.

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.

What is ‘discourse’?

Seminar-style teaching (2)

Each week you will:

1. Critically read three original papers/reports

2. Submit synthesis essays across all readings

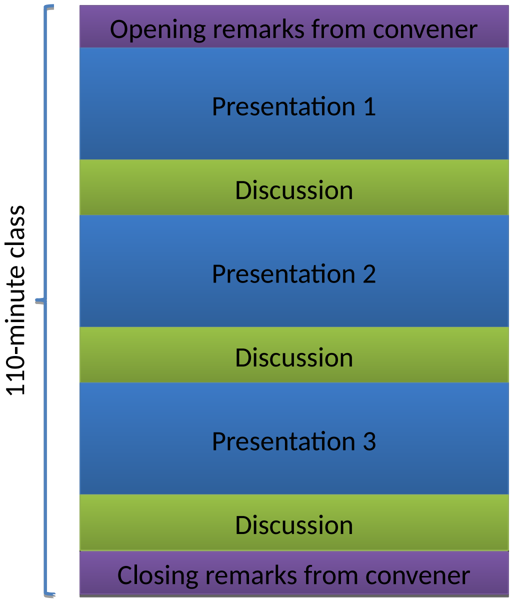
or

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 not present papers or submit essays)

Typical class structure



110-minute class

Opening remarks from convener

Presentation 1

Discussion

Presentation 2

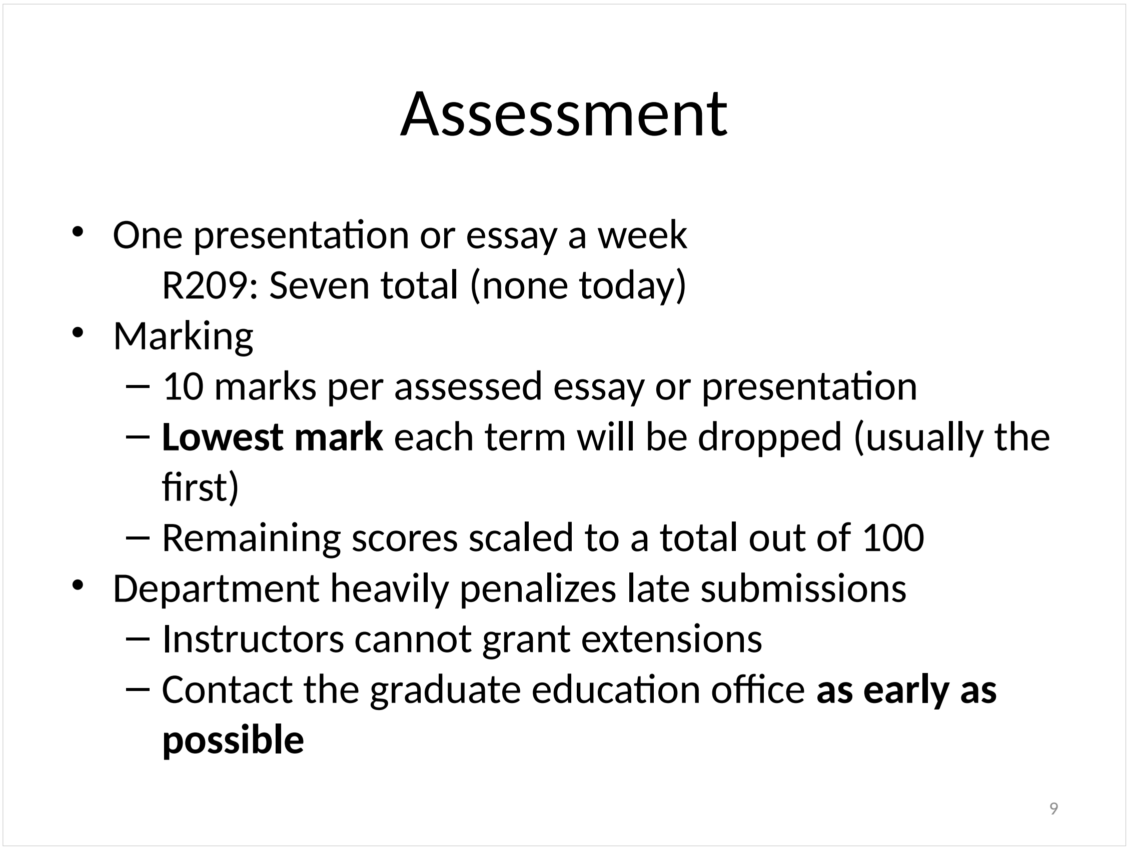
Discussion

Presentation 3

Discussion

Closing remarks from convener

- 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



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

Contemporary = today, not contemporaneous with the original paper

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

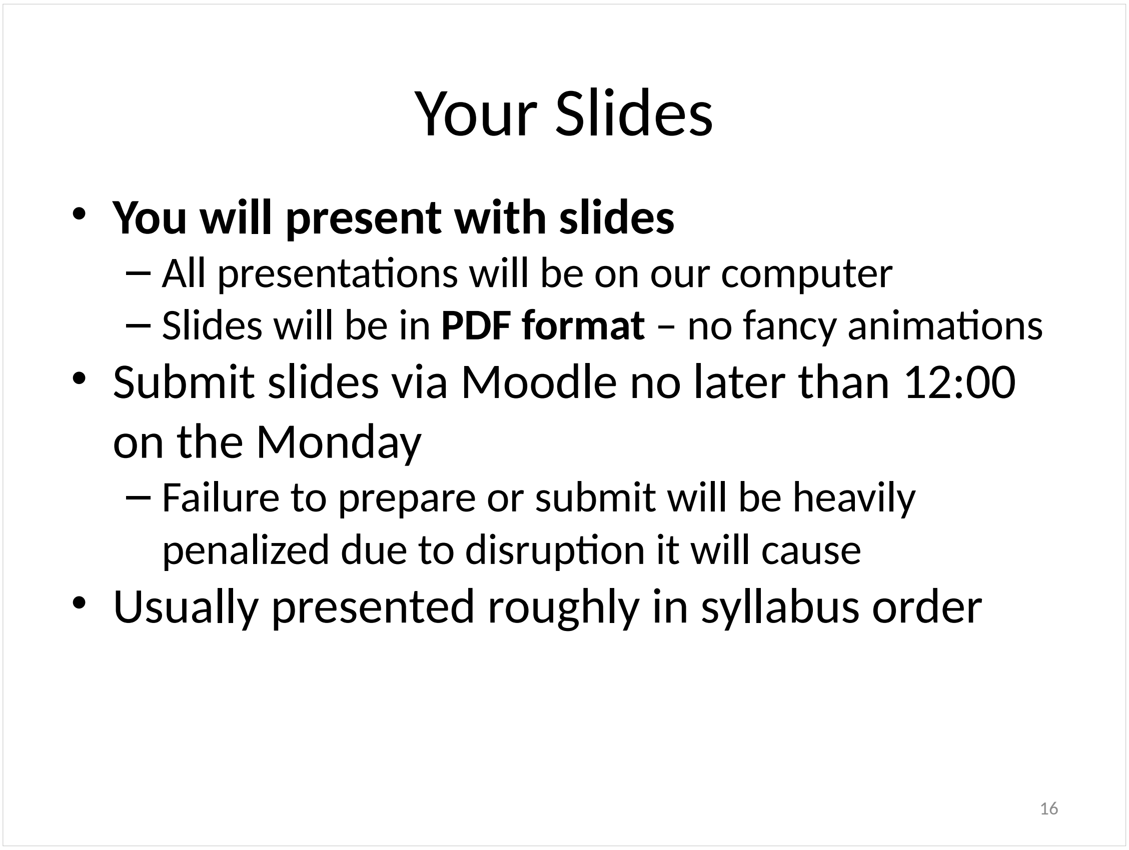
Weekly Presentations

- 7 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

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!

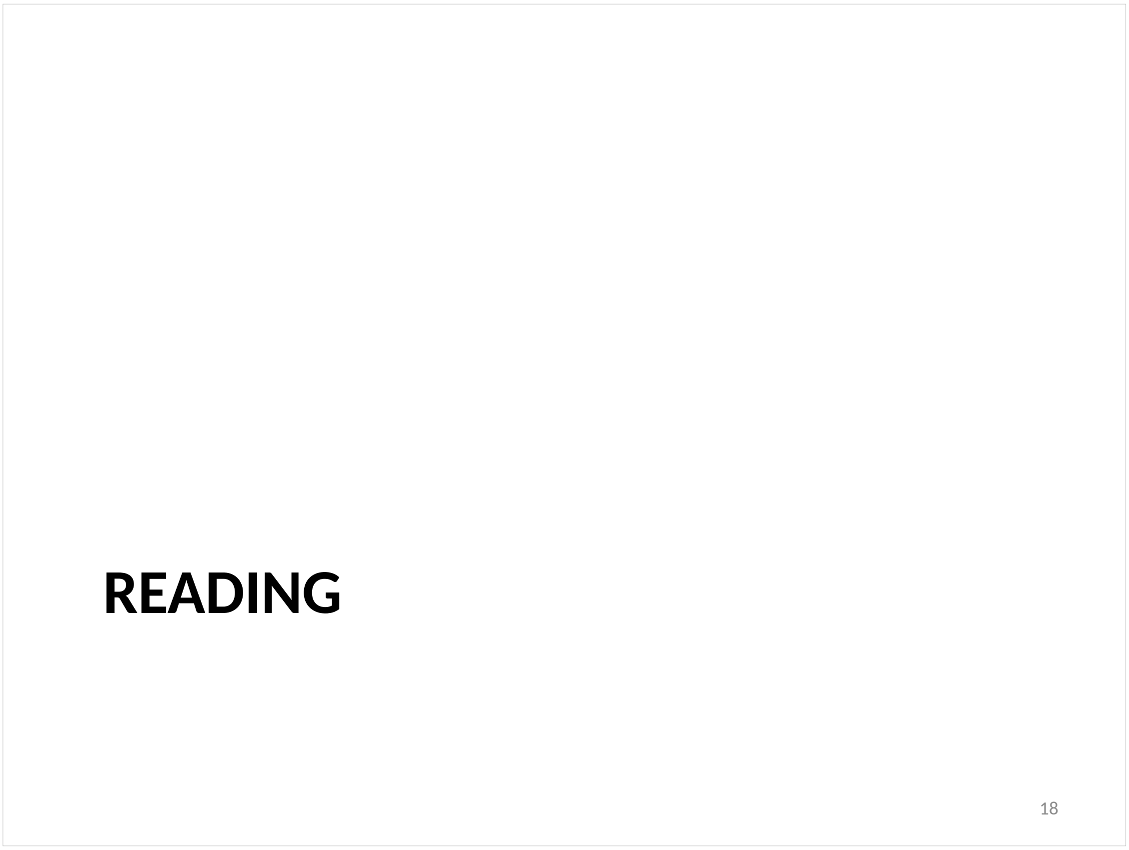


Your Slides

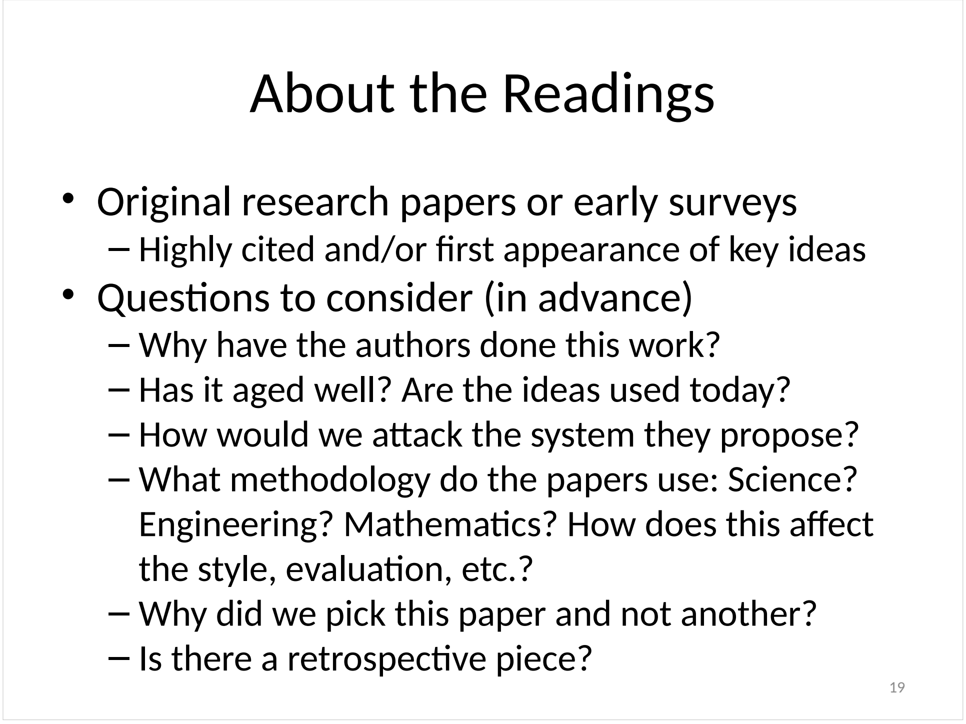
- **You will present with slides**
  - All presentations will be on our computer
  - Slides will be in **PDF format** – no fancy animations
- Submit slides via Moodle no later than 12:00 on the Monday
  - Failure to prepare or submit will be heavily penalized due to disruption it will cause
- Usually presented roughly in 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 ask (and answer) 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 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 daniel.thomas@cl.cam.ac.uk
- Recurring guests may be asked to present times during the term if we develop gaps

Module Website

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

https://www.cl.cam.ac.uk/teaching/1819/R209/

- Next term's website here:

https://www.cl.cam.ac.uk/teaching/1819/R254/

- Look at the 'Materials', 'Assessment' pages

R209 Weekly Meetings

Date	Topic	Convener(s)
8 Oct	Origins and Foundation of Computer Security	Thomas, Anderson, Beresford
15 Oct	Adversarial Reasoning	Anderson
22 Oct	Access Control	Beresford
29 Oct	Cryptographic Protocols	Anderson
5 Nov	Correctness vs. Mitigation	Thomas
12 Nov	Usable Security	Beresford
19 Nov	Security Economics	Anderson
26 Nov	Passwords	Beresford

How to Reach Us

ross.anderson@cl.cam.ac.uk
alastair.beresford@cl.cam.ac.uk
daniel.thomas@cl.cam.ac.uk

Daniel may be on paternity leave from mid November so email Ross and Alastair as well.

QUESTIONS

INTRODUCTIONS
WHAT IS SECURITY?

TODAY’S READINGS