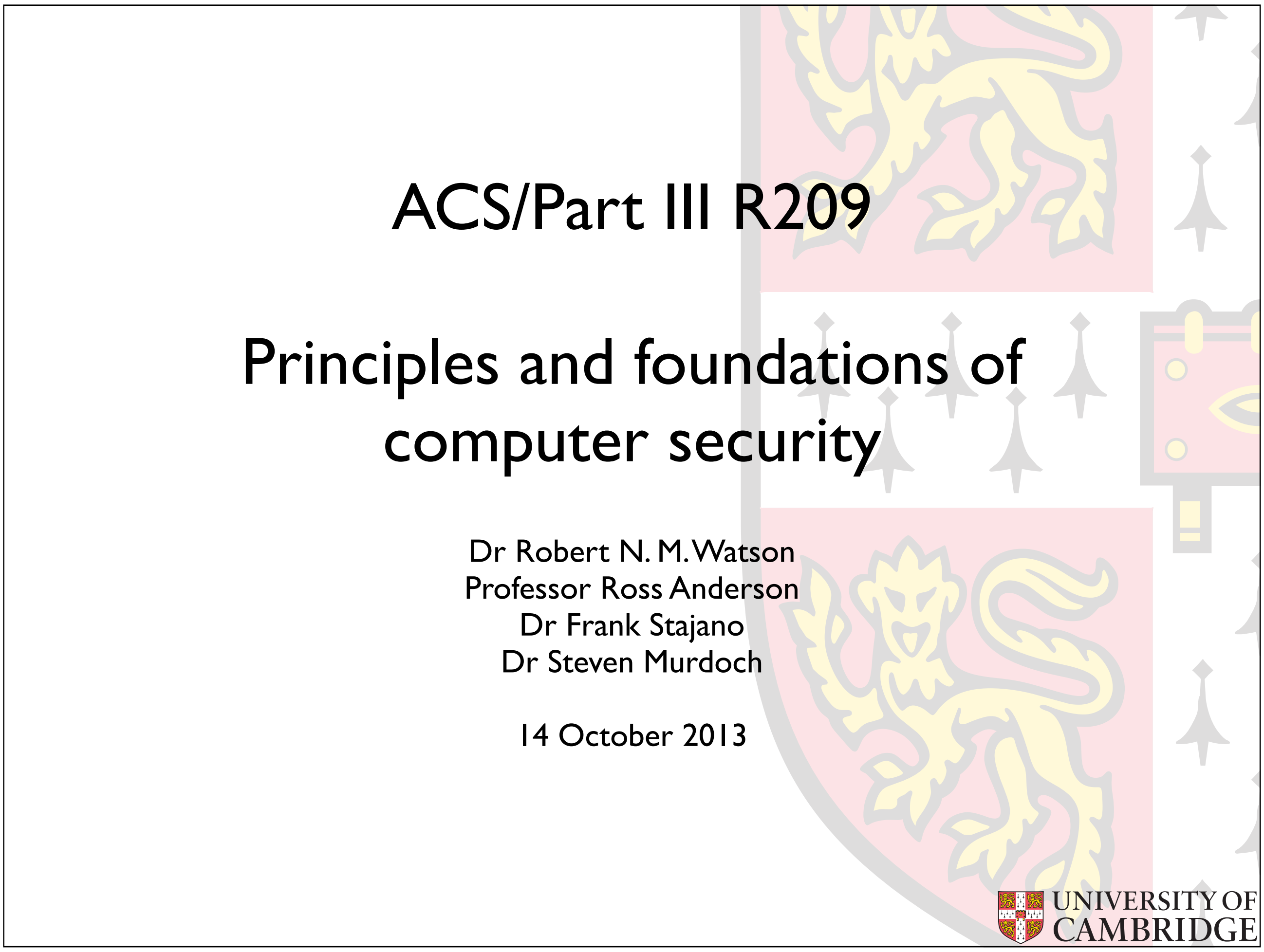
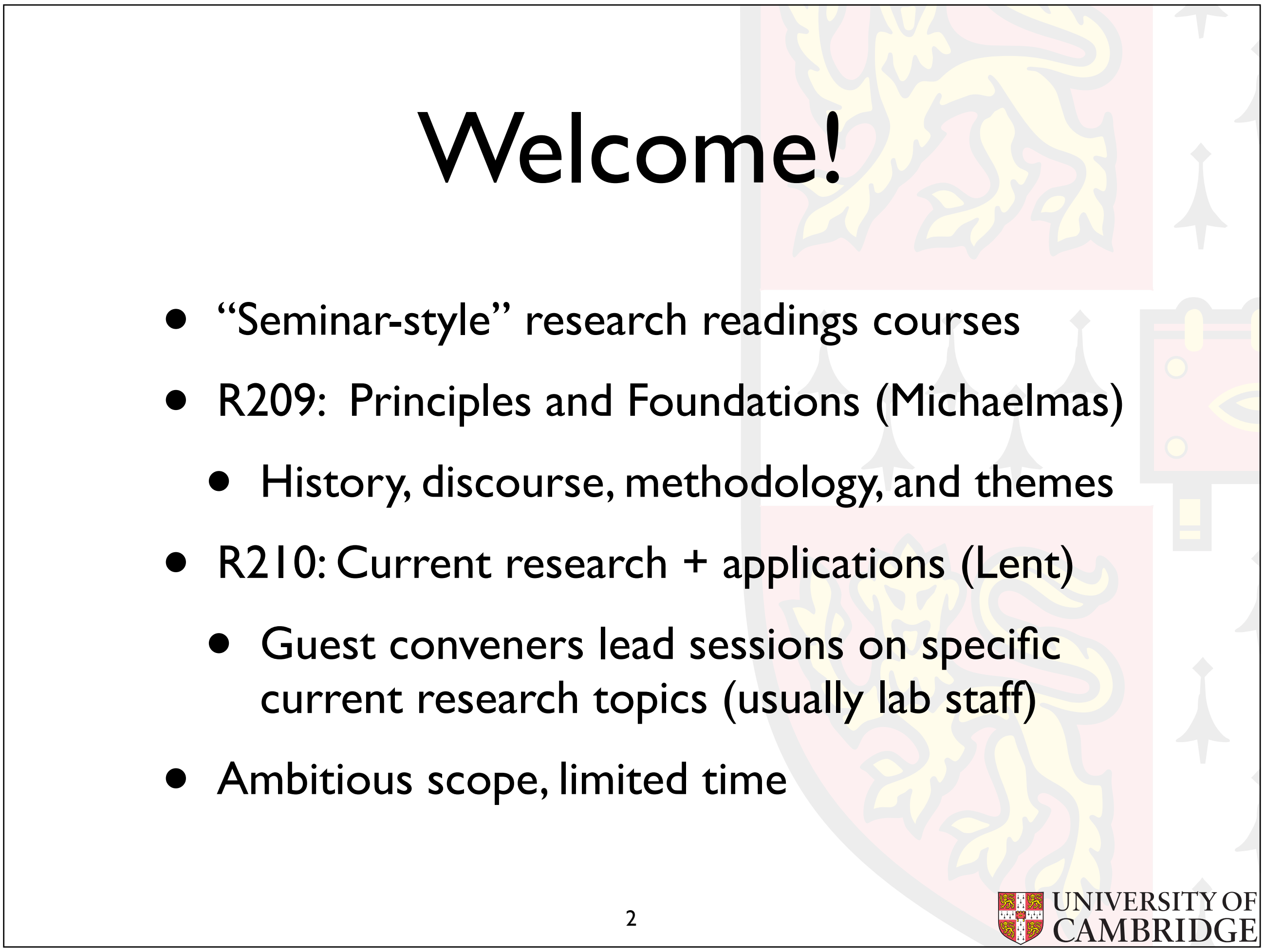


ACS/Part III R209

Principles and foundations of computer security

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

14 October 2013



Welcome!

- “Seminar-style” research readings courses
- R209: Principles and Foundations (Michaelmas)
  - History, discourse, methodology, and themes
- R210: Current research + applications (Lent)
  - Guest conveners lead sessions on specific current research topics (usually lab staff)
- Ambitious scope, limited time

Prerequisites

- Undergraduate degree or a strong grounding in computer science
- At least one past course in operating systems, networking, and/or security
- Some topics will be familiar from taught material at the undergraduate level…
- … but grounded in their original research contexts and presentations

Brushing up on computer security

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

Gollmann, D. (2010). *Computer Security*, Wiley

Seminar-style course

- Preparation for research and development in the field
  - Study vocabulary and discourse; trace intellectual history
  - Appreciate (and critique) original research as published
  - Consider current-day implications; contrast with original context
  - Discuss future research directions
- Each week you will:
  - Critically read three(ish) original research papers or reports
  - Submit synthesis essays across all readings **or** present and lead discussion on a specific reading
  - Particulate in class discussion of the readings

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 dropped; remaining scores scaled to a percent
- 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

Weekly essays

Synthesis essay

- *Synthesis writing* reports, organises, and interprets readings
    - Synthesis essays are not original research papers
- Suggested outline covers five areas:
    1. Summaries of readings (1-2 para/reading)
    2. Discussion of a 2-3 key themes spanning readings (2-4 para)
    3. Consideration of ideas in current context (1-2 para)
    4. Literature review (1-2 para)
    5. Class discussion questions (4 is a good number)
- All essays must include a bibliography
- If this is new to you, Google "synthesis essay"

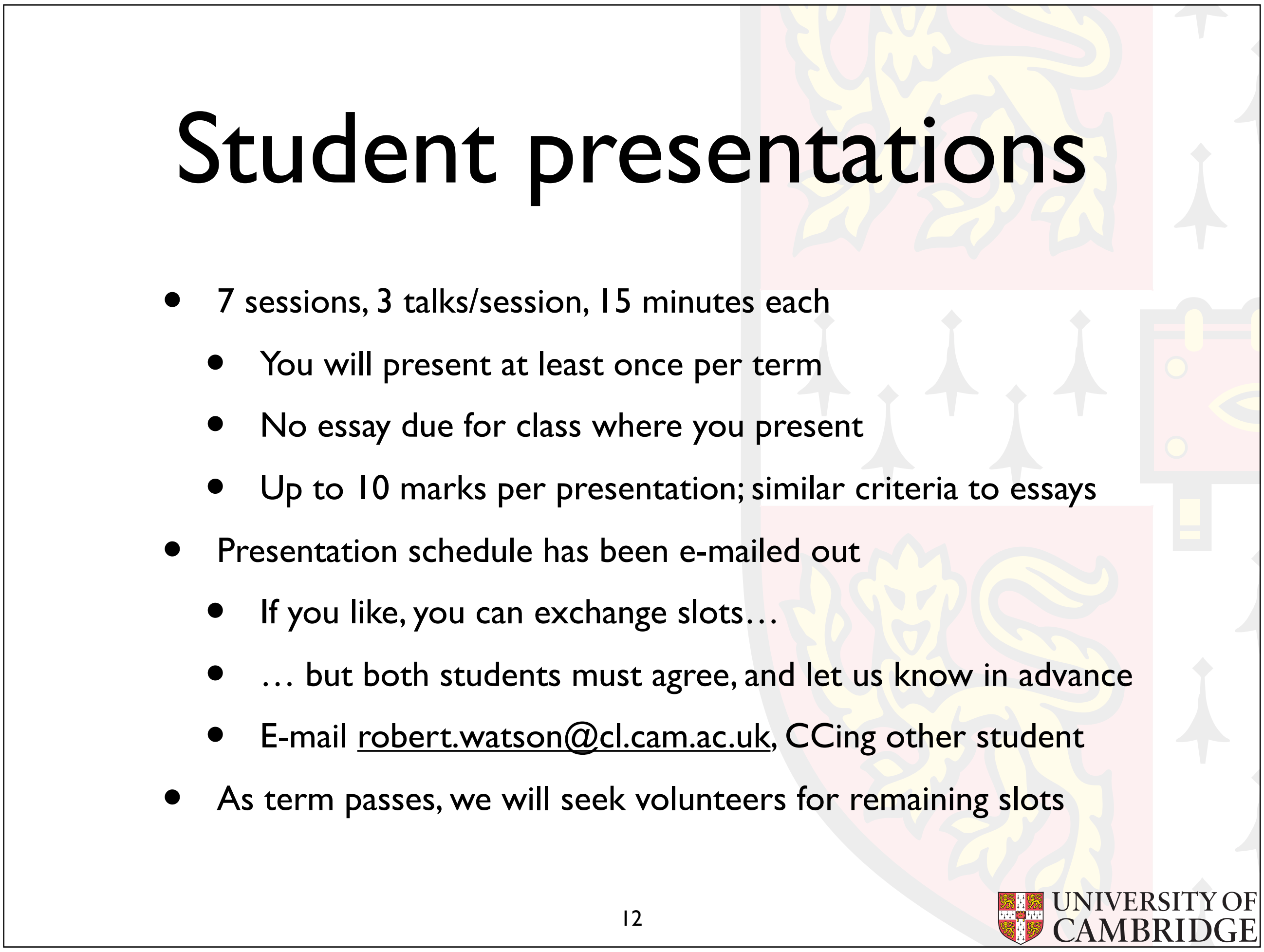
Essay marking notes

- 10 points divided evenly across five aspects:
  - 0 - failed to submit
  - 1-4 - seriously lacking
  - 5-6 - adequate
  - 7-8 - good
  - 9-10 - exceptional

Essay submission

- Submit on paper to the graduate education office
- Must be received by **noon** on the Thursday before we meet (except this week: noon Friday is OK)
- Please **also** e-mail an electronic copy, in PDF format, to acs-2013-r209-essays@cl.cam.ac.uk
- Marks will be returned via the graduate education office; we usually e-mail them as well
- Bring discussion questions to class

Weekly presentations



Student presentations

- 7 sessions, 3 talks/session, 15 minutes each
  - You will present at least once per term
  - No essay due for class 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 slots…
  - … but both students must agree, and let us know in advance
  - E-mail robert.watson@cl.cam.ac.uk, CCing other student
- As term passes, we will seek 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 our 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!

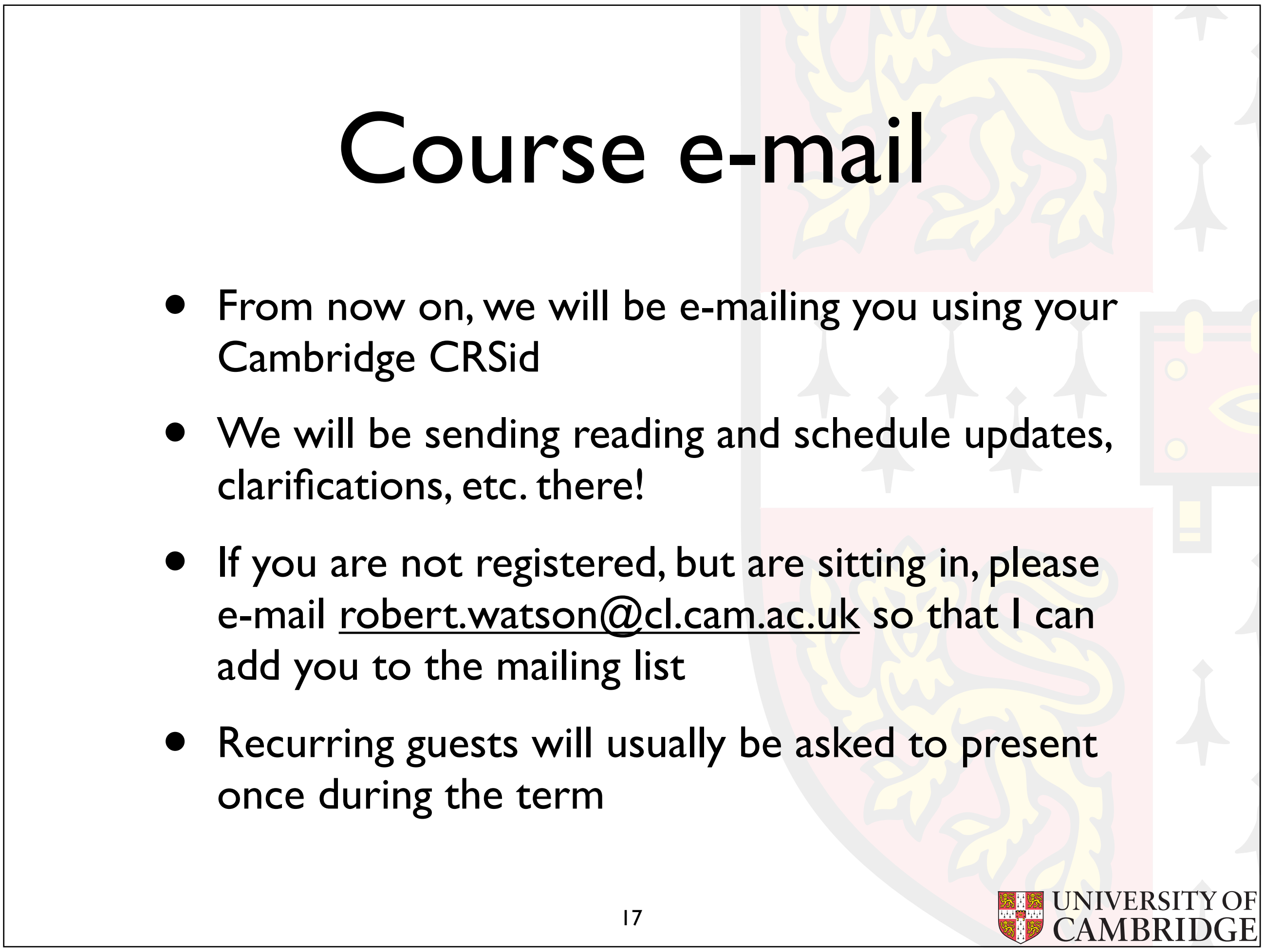
Your slides

- For avoidance of doubt: you will present with slides
- All presentations will be from our notebooks
- Slides must be in PDF format - no fancy animations; builds OK
- Submit slides by e-mail no later than 10:00 on the day of presentation to acs-2013-r209-slides@cl.cam.ac.uk
- Also submit on paper to graduate education office
- Late submission will be **heavily penalised** due to disruption it will cause to other students
- Usually presented within class in roughly syllabus order

Class discussions

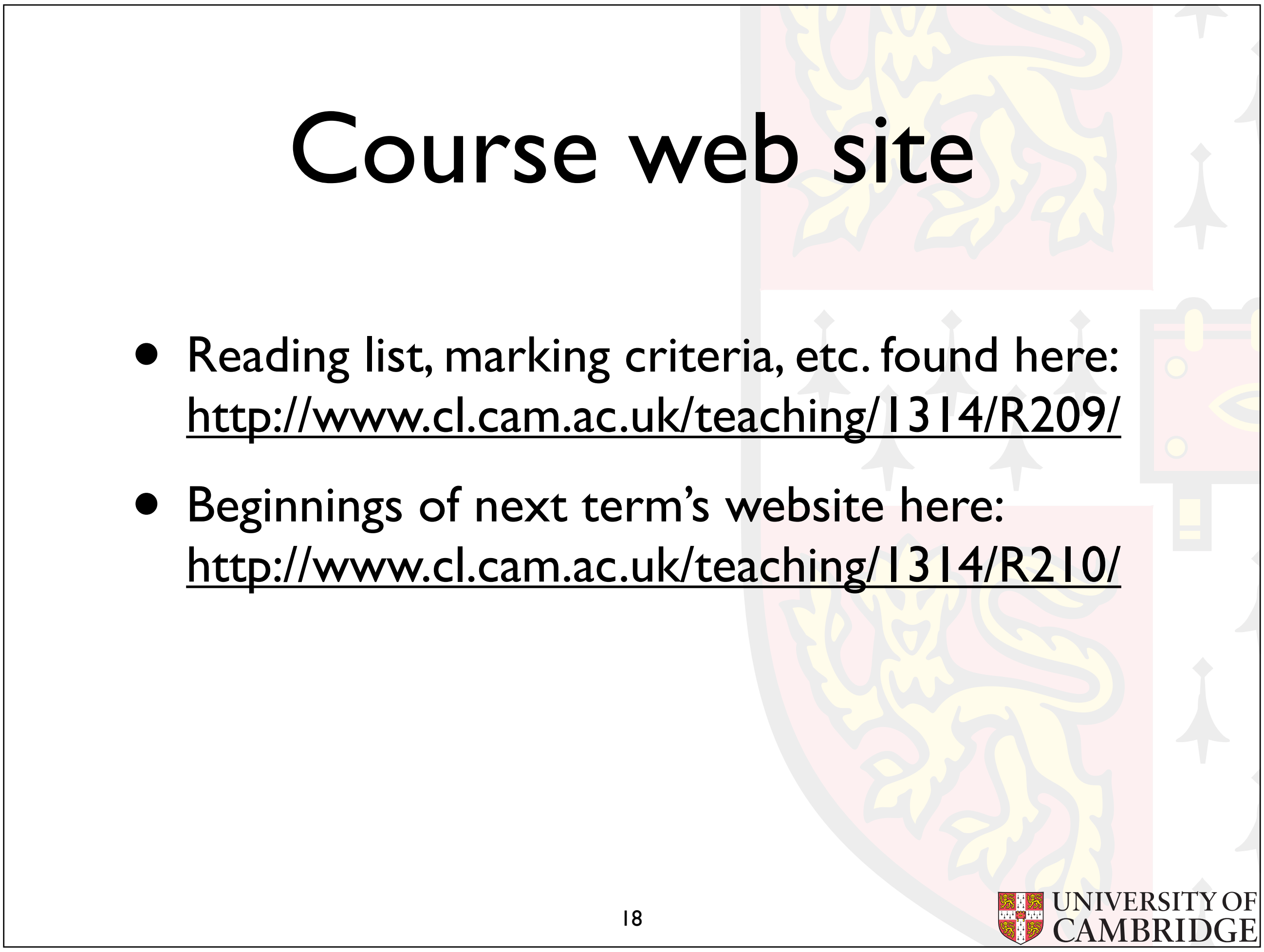
- Roughly half of each two-hour meetings set aside for discussion
- Bring discussion questions to class and be prepared to discuss them
- No explicit marks for participation…
- … but presenter is rewarded for interesting discussion, so mutual benefit to participating!

Other admin things



Course e-mail

- From now on, we will be e-mailing you using your Cambridge CRSid
- We will be sending reading and schedule updates, clarifications, etc. there!
- 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
- Recurring guests will usually be asked to present once during the term



Course web site

- Reading list, marking criteria, etc. found here: http://www.cl.cam.ac.uk/teaching/1314/R209/
- Beginnings of next term's website here: http://www.cl.cam.ac.uk/teaching/1314/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

acs-2013-r209-essays@cl.cam.ac.uk

acs-2013-r209-slides@cl.cam.ac.uk

R209 weekly meetings

Date	Topic	Leader
14 Oct	Origins of computer security*	RNMW, RJA
21 Oct	The economics of security	RJA
28 Oct	Cryptographic protocols: possibilities and limitations	RJA
4 Nov	Passwords: technology, human factors, and what goes wrong	FMS
11 Nov	Access control and adversarial reasoning	RNMW
18 Nov	Hardware and software capability systems	RNMW
25 Nov	Programming language and information-flow security	RNMW
2 Dec	Correctness vs. mitigation	RNMW

*First session is a bit unusual because no student presentations/essays

Last year's R210 topics

(may differ somewhat this year, but should be similar)

Topic
Covert and anonymous communications
Tampering with hardware
Bootstrapping security relationships
Behavioural economics of privacy
Social network security
API security
Mobile system security
Psychology and security

Introductions

Some thoughts on computer security

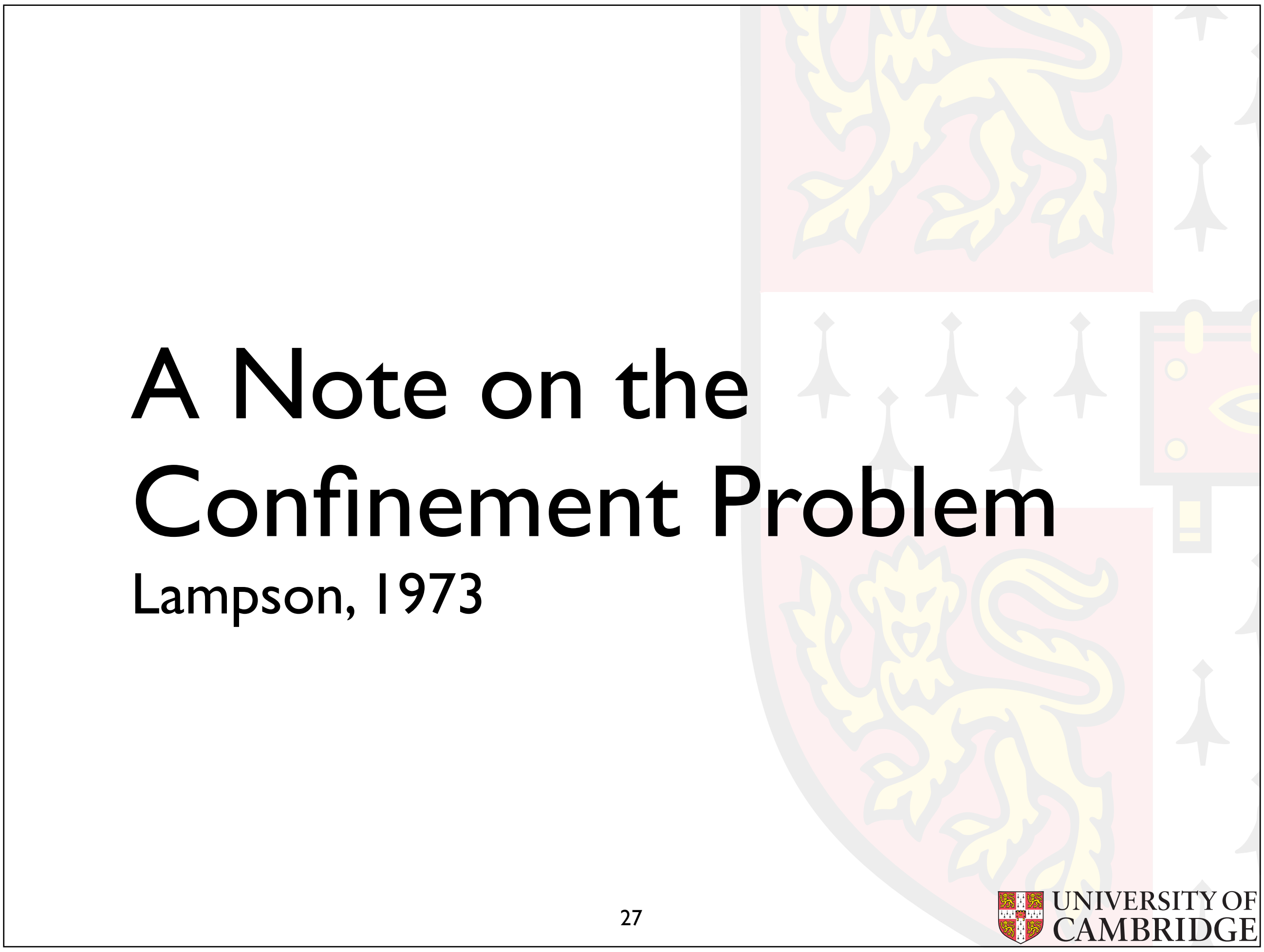
A few key themes

- 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?

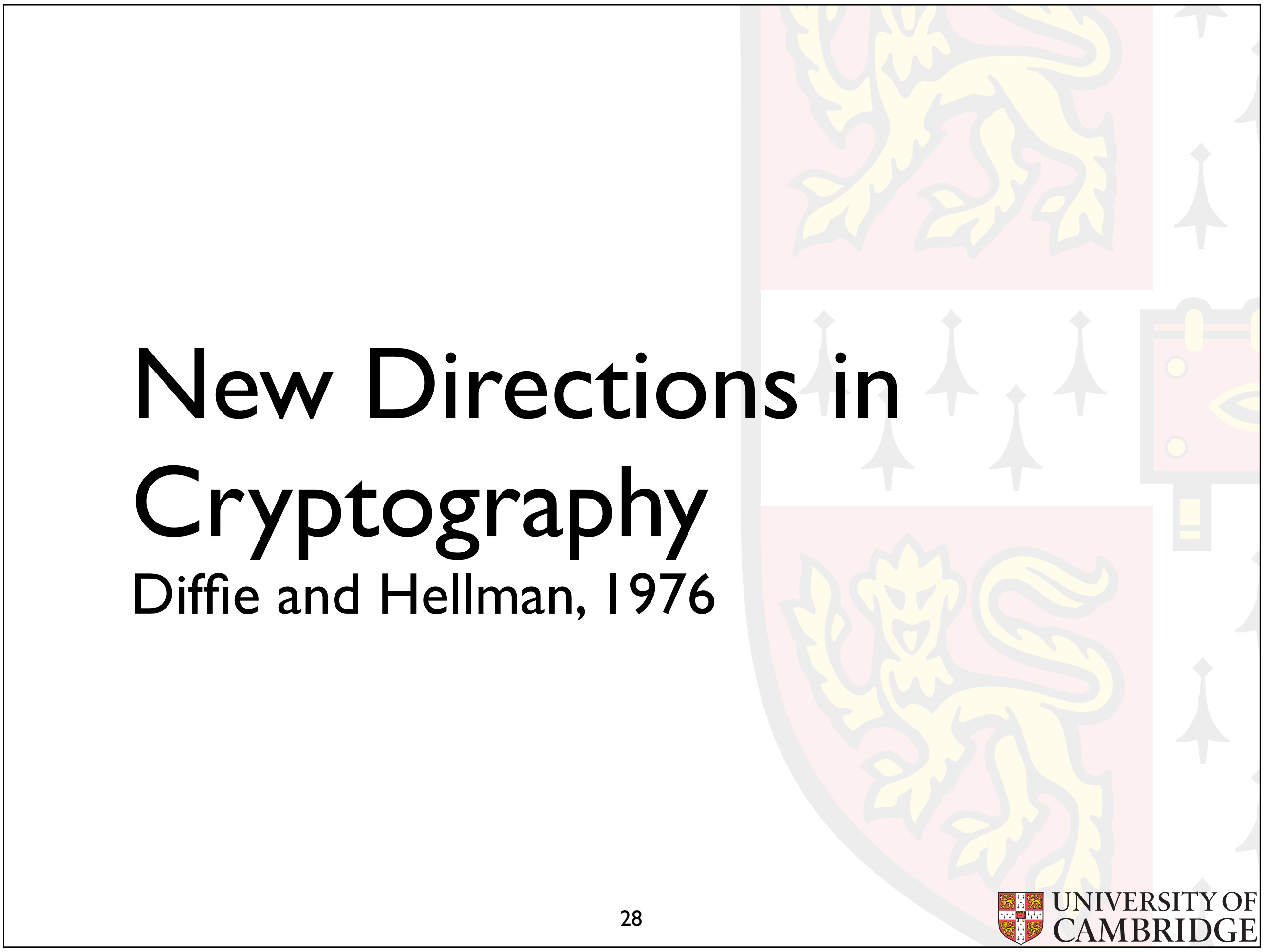
Protection of Information in Computer Systems

Saltzer and Schroeder, 1973-1975



A Note on the Confinement Problem

Lampson, 1973



New Directions in Cryptography

Diffie and Hellman, 1976

Using Encryption for Authentication in Large Networks of Computers

Needham and Schroeder, 1978