Computer Security: Administrative matters

Myrto Arapinis
School of Informatics
University of Edinburgh

January 12, 2015

Teaching staff

Lecturer: Dr. Myrto Arapinis

Course TA: Joseph Hallett

Course secretary (ITO): Victoria Swann

Course webpage

`http://www.inf.ed.ac.uk/teaching/courses/cs/`

Contains important info:

- Lecture slides
- Tutorial sheet exercises
- Course organization
- etc

Tutorials

- You should receive email from the ITO informing you of preliminary allocation of tutorial groups
- See link on course web page for current assignment of tutorial groups
- If you can't make the time of your allocated group, please email Victoria suggesting some groups you can
- Tutorial attendance is mandatory. If you miss two tutorials in a row, your PT (DoS) will be notified

Grading

- Written Examination: 75%
- Assessed Assignments: 25%
  There are two assessed coursework exercises, each worth 12.5% of the final mark.
  Coursework 1 is due on Mar. 06 at 16:00
  Coursework 2 is due on Mar. 27 at 16:00

Computer Security: Introduction

Myrto Arapinis
School of Informatics
University of Edinburgh

January 12, 2015

What is computer security?

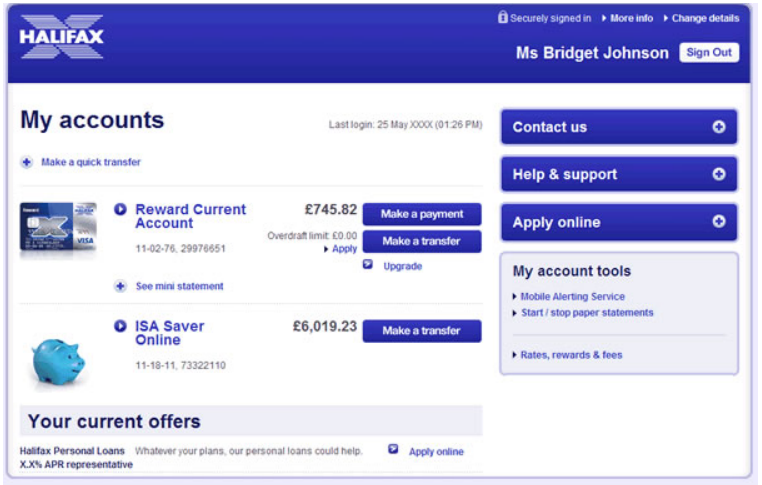
Correctness:

- allow intended use of computer systems

Computer security:

- prevent harmful undesired behavior
- considers a malicious entity actively trying to circumvent any protective measures in place

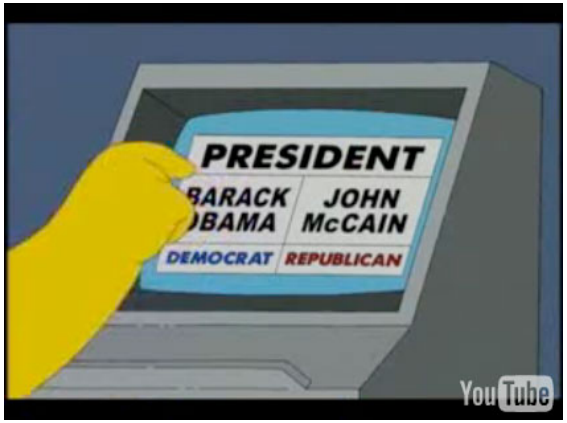
Online banking



Social networks

Mobile telephony

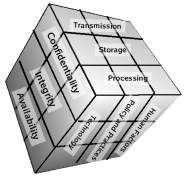
Electronic voting



Some significant security breaches

- **Adobe** (2013) - stole source code, 130 million customer records (including passwords)
- **Target** (2013) - stole around 40 million credit and debit cards
- **Sony Pictures Entertainment** (2014) - stole personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of unreleased Sony films
- **Apple** (2014) - goto fail - encrypted traffic, including usernames, passwords, and even Apple app updates could be captured
- **OpenSSL** (2014) - heartbleed bug - steel secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content

Basic security properties



Confidentiality: some information should never be revealed to unauthorised entities

- Corporate secrets (product plans, source code, . . .)
- Personal information (credit card numbers, . . .)

Integrity: data should not be altered in an unauthorised manner since the time it was created, transmitted or stored by an authorised source

- Installing unwanted software (spyware, botnet client, . . .)
- Destroying records (accounts, logs, plans, . . .)

Availability: Information on and services should be accessible

Security analysis

Is the computer system secure?

- What are the assets?
  - grade database system for this class
  - major online banking site
  - the system to control nuclear weapon launch
- What are the security objectives
  - confidentiality, authentication, anonymity, integrity, unlinkability, non-repudiation, . . .
- What is the threat model?
  - the attacker has physical access
  - the attacker can install malware on the system
  - the attacker controls the network

Course topics

- Cryptography
- Network protocols
- Access control
- Secure coding
- Web security