

Computer Security: Administrative matters

Myrto Arapinis
School of Informatics
University of Edinburgh

January 12, 2015

1 / 15

Teaching staff

Lecturer: Dr. Myrto Arapinis

Course TA: Joseph Hallett

Course secretary (ITO): Victoria Swann

2 / 15

Course webpage

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

Contains important info:

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

3 / 15

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

4 / 15

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

5 / 15

Computer Security: Introduction

Myrto Arapinis
School of Informatics
University of Edinburgh

January 12, 2015

6 / 15

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

7 / 15

Online banking

The screenshot displays the Halifax online banking dashboard for Ms Bridget Johnson. The interface is blue and white. At the top, it shows the Halifax logo, a 'Securely signed in' status, and navigation links for 'More info' and 'Change details'. Below this, the user's name 'Ms Bridget Johnson' and a 'Sign Out' button are visible. The main section is titled 'My accounts' and includes a 'Last login: 25 May XXXX (01:26 PM)' timestamp. There are three main account cards: 1. 'Reward Current Account' with a balance of £745.82, an overdraft limit of £0.00, and a 'Make a payment' button. 2. 'ISA Saver Online' with a balance of £6,019.23 and a 'Make a transfer' button. 3. A 'Your current offers' section for Halifax Personal Loans with an 'Apply online' button. On the right side, there are three expandable menu items: 'Contact us', 'Help & support', and 'Apply online'. Below these is a 'My account tools' section with links for 'Mobile Alerting Service', 'Start / stop paper statements', and 'Rates, rewards & fees'.

8 / 15

Social networks



9 / 15

Mobile telephony



10 / 15

Electronic voting



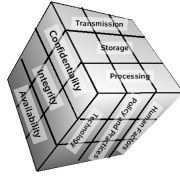
11 / 15

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 - steal secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content

12 / 15

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

13 / 15

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



14 / 15

Course topics

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

15 / 15