COMP232
CYBERSECURITY

Alexei Lisitsa
Dept of computer science
University of Liverpool
alexei@csc.liv.ac.uk

www.csc.liv.ac.uk/~alexei/COMP232

Useful information

- Lecturer's details:

Name: Alexei Lisitsa
Office: 118, Ashton Building
Email: alexei@csc.liv.ac.uk

- URL: **www.csc.liv.ac.uk/~alexei/COMP232**

  Watch this web site for lecture notes, assignments, reading materials, etc

- Practical sessions: start at week 2, see your personal timetable
- Assignments deadlines: TBA

Textbooks

Main:

- Richard R. Brooks, **Introduction to Computer and Network Security**, **Navigating Shades of Gray, CRC Press,** Taylor and Francis Group, 2014 (and later editions). CNS

Additional:

- William Stallings , **Network Security Essentials: Applications and Standards**. Prentice Hall, 2000 (and later editions). NSE
- A. Menezes, P. van Oorschot, and S. Vanstone, **Handbook of Applied Cryptography**, CRC Press, 1996.

  Available online at http://www.cacr.math.uwaterloo.ca/hac free for personal use;

Organisation of the course

- Three lectures a week (for 8 weeks(+))
  - Monday, 15.00, **ASHT-LR**: Ashton Building Lecture Theatre
  - Tuesday, 14.00, **CHAD-BARKLA**: Chadwick Building, Barkla Lecture Theatre
  - Thursday, 9.00, **NICH-LT**: Nicholson Building , Lecture Theatre;

- 2 practical sessions per week (from week 2) x 10 weeks
  - see your personal timetable

Timetable may change in coming 1-2 weeks, watch your individual timetable!

Assessment weightings

- 60% Exam;
- 40% Coursework;

- Course work will be divided into four assignments (10% each) .

Aims (from Syllabus)

1. To provide students with understanding of the main problems in security, confidentiality and privacy in computers and in networks, and the reasons for their importance.

2. To enable students to understand the main approaches adopted for their solution and/or mitigation, together with the strengths and weaknesses of each of these approaches.

3. To develop knowledge and skills in practical applications of available security solutions.

4. To introduce students to theoretical foundations of cybersecurity and attract their attention to the open problems requiring further research.

CyberSecurity: What does it mean?

Cyberspace:

- ...is an electronic medium used to form a global computer network(s) to facilitate online communication…
- (from Technopedia)

- **Security :**
  - A condition that results from establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences…

(from US Federal Standard 1037C)

Security in Cyberspace

- In the modern world there are various ways in which hostile act and influences can be exercised.

- Many of them are coming via Cyberspace, where in particular, unprecedented amount of data about individuals and organizations being collected, processed, analysed and possibly misused.

Yet Another Important Concept

- **Privacy:**
  - Privacy is the ability of a person to control the availability of information about and exposure of him- or herself. It is related to being able to function in society anonymously… **(from Wikipedia)**

  Not the same, but Interlinked with Security, as

  - Availability of private information may itself constitute a hostile act
  - Availability of (or acquiring) some information may be a pre-condition for some security attacks
  - ….

Various aspects of CyberSecurity. Or what makes it interesting.

- Science:
  - Computer Science: new opportunities/challenges
  - Mathematics: non-trivial mathematics behind many solutions
  - Physics: rise of quantum cryptography
  - Biology: DNA analysis based authentication
- Technology: global networking, cloud computing
- Economical issues: costly cybersecurity
- Legal & Political Issues: is it legal to fight back? Political influence by interfering with elections, etc
- Social and moral aspects: shall we trade privacy for better security?

Almost every statement/argument can be continued with "BUT… "

Costly cybersecurity

- Global cybersecurity spending by critical infrastructure industries estimated as $46 billion in 2013, up 10% from a year earlier, **(Allied Business Intelligence Inc.)**
- For $1 million, Richard Bejtlich, chief security strategist at FireEye Inc said he could assemble a team that could hack into nearly any target. **(Wall Street J., 2014)…**

But $1 million wouldn't be nearly enough for a large company to defend itself.

- Economic impact on 18 software suppliers, including Microsoft, Cisco, IBM when vulnerability in one of their products found:
  - on average 0.6 per cent fall in its stock price
  - $ 860 million fall in the company value

(survey by S.Wattal et al, CMU)

Or, is it?

- A 2009 study by Center for Strategic and International studies estimated that hacking costs the global economy $1 trillion.
- President Obama has cited the cost when pressing for legislation on cybercrime protection.
- It has turned out, however there were several flows in the methodology of the study, and new study by CSIS (2013) has indicated that $300 - $400 billions is the probably range of global cost.

TRUST, but VERIFY

If security is compromised

- **Personal impact:** Hackers stole personal information with details of up to 70 million people – a third of American adults – including phone numbers, email and home addresses, the US retail chain Target admitted on Friday. (10 Jan 2014)

Computer security in Industrial software

Stuxnet

- Computer worm discovered in June 2010
- It targets Siemens industrial software and equipment running on Microsoft Windows
- 60% of the infected computers were in Iran (August 2010) including controllers handling the centrifuges at Natanz nuclear facilities
- Was it a field test of a cyber weapon?

Recent: cyber attacks on cars

- July 2015, two security researches using a laptop and a mobile phone took control of Jeep Cherokee remotely;
- They were able
  - apply the brakes;
  - kill the engine;
  - take control of steering

  Self-driving cars as a target?

- General IoT? Attacks on road message boards, medical electronic equipment's, etc

- Security and Safety. New methods for the systems design: STPA (N. Levenson et al): treat security as safety

Content of the course

- Security and Privacy Overview:

security attributes, authentication and authorization, access permission, audit, social engineering, vulnerabilities and attacks.

- Cryptography:

symmetric encryption, public key encryption, hash functions, key exchange protocols, key management, message confidentiality, steganography, partially and fully homomorphic encryption, quantum cryptography

Security protocols:

key exchange, handshake, SSL/TLS, introduction to verification of protocols.

Content of the course

- Securing Networks:

  firewalls, virtual private networks, wireless security, intrusion detection and prevention systems.

- Insertion attacks:

SQL Injection, Buffer Overflow, SSH insertion, Viruses, Worms.

- Web security:

cross site scripting, cross site request forgery, man-in-the browser, web applications penetration testing

- Applications of cryptographic algorithms and protocols:

  voting protocols, blockchain, cryptocurrencies.

Reading

[CNS]: Chapter 1

[NSE]: Chapter 1, sections 1.1 –1.3