**COMP522 PRIVACY AND SECURITY**

Alexei Lisitsa  
Dept of computer science  
University of Liverpool  
alexei@csc.liv.ac.uk  
www.csc.liv.ac.uk/~alexei/COMP522

---

**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/COMP522](http://www.csc.liv.ac.uk/~alexei/COMP522)
  
  Watch this web site for lecture notes, assignments, reading materials, etc.

- **Practical sessions:** TBA

- **Assignments deadlines:** TBA

---

**Textbooks**


---

**Additional books**


Organisation of the course

- Three lectures a week
  - Tuesday, 10.00, Brod-105: Room 105, Brody Building;
  - Wednesday, 10.00, GHOLT-H223: Room 223, Holt Building,
  - Thursday, 10.00, BROD-105: Room 105, Brody Building;

- 1 practical tutorial a week (from week 3)
  - Friday, 9.00, Lab 5, Holt Building Further Details TBA

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

Assessment weightings

- 75% Exam;
- 25% Coursework;
- Course work will be divided into two assignments.

Aims (from Syllabus)

- To introduce students to the major problems and solution approaches in the area of computer and Internet privacy, confidentiality and security
- To provide a theoretical framework for subsequent research in these challenging areas

Privacy & Security: What does it mean?

- **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)

- **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)
Privacy and 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.

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)

Various aspects of P&S.

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…”

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 researchers 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
- General IoT? Attacks on road message boards, medical electronic equipments, etc
- Security vs Safety. New methods for the systems design: STPA (N. Levenson et al)

Content of the course

- **Part 1: Identification and authentication**
  - Passwords v.tokens v. biometrics;
  - Data aggregation, anonymity and pseudoanonymity;
  - Information hiding: steganography & digital watermarking;
- **Part 2: Monitoring**
  - Intrusion detection/prevention;
  - Techniques (statistics, pattern recognition, etc); and
  - Issues such as accountability v. privacy;
Content of the course

- **Part 3: Algorithms and Protocols**
  - Protocol design;
  - Cryptography for secrecy, for signing, etc;
  - Symmetric key and asymmetric key protocols;
  - 3DEA and RSA protocols;
  - Logical representation of protocols;
  - Formal properties of protocols;
  - Applications, e.g encryption, key distribution, identification, authentication, electronic cash / cryptocurrencies.

- **Part 4: Attacks and defences**
  - Malware: viruses and worms, spyware, denial/manipulation of service, etc; and
  - Web security

- **Part 5: Legal and Ethical Issues**

- **Part 7: Current and Future directions**
  - Fully Homomorphic Encryption;
  - Quantum protocols and cryptography

Content of the course

- **Practicals:**
  - we will do some programming with Java Cryptographic Architecture/Extensions (JCA/JCE),
  - we will do some practicals on Web security

Reading

[CNS]: Chapter 1
[NS]: Chapter 1, sections 1.1 –1.3
[WSPC]: Chapter 1