



COMP522 PRIVACY AND SECURITY

Dr Alexei Lisitsa
Dept of Computer Science
University of Liverpool
A.Lisitsa@liverpool.ac.uk

Useful information

- Lecturer's details:

Name: Dr Alexei Lisitsa

Office: Ashton 1.18

Email: `A.Lisitsa@Liverpool.ac.uk`

- Lectures: Mondays, 15.00-17.00, Proudman LT
- Practical sessions: Tuesdays, 10.00-11.00 **or** 12.00-13.00
or Wednesdays, 12.00--13.00
(starting week 2, no session week 1)
- Assignments deadlines: TBC
- Check website
<https://www.csc.liv.ac.uk/~alexei/COMP522/>

Textbooks

- Richard R. Brooks, **Introduction to Computer and Network Security, Navigating Shades of Gray**, CRC Press, Taylor and Francis Group, 2014 (and later editions). **CNS**
- William Stallings , **Network Security Essentials: Applications and Standards**. Prentice Hall, 2000 (and later editions). **NSE**
- Simson Garfinkel, **Web Security, Privacy and Commerce**. (Second Edition, O'Reilly), 2002 (and later editions). **WSPC**

Additional books

- 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

- Two lectures per week, Mondays, 15.00 and 16.00
- 1 practical session a week (from week 2)

Assessment weightings

- 60% Exam;
- 40% Coursework;
- Course work will be divided into two assignments of 20%.
CA1 and CA2

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.

Various aspects of P&S.

Or what makes it interesting.

- **Science:**
 - **Computer Science:** Application of advance programming & system design
 - **Mathematics:** non-trivial mathematics behind many solutions
 - **Physics:** rise of quantum cryptography and computing
 - **Biology:** Biometric based authentication
- **Technology:** networking, cloud computing, systems architecture
- **Economical issues:** cost, global influence.
- **Legal & Political Issues:** Hacking, nation state attacks, monitoring
- **Social and moral aspects:** shall we trade privacy for better security?

Cybersecurity

- The worldwide information security market is forecast to reach \$170.4 billion in 2022. [1]
- 62% of businesses experienced phishing and social engineering attacks in 2018[2]
- 68% of business leaders feel their cybersecurity risks are increasing.[3]
- Data breaches exposed 4.1 billion records in the first half of 2019. [4]
- The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%.[5]

Global impact

- The average cost of a malware attack on a company is \$2.6 million.[\[1\]](#)
- \$3.9 million is the average cost of a data breach.[\[2\]](#)
- The financial services industry takes in the highest cost from cybercrime at an average of \$18.3 million per company surveyed.[\[3\]](#)
- The industry with the highest number of attacks by ransomware is the healthcare industry. Attacks are set to quadruple in 2020.[\[4\]](#)

Jobs

- 82% of employers report a shortage of cybersecurity skills.[1]
- By 2021, it's projected that there will be 3.5 million unfilled cybersecurity jobs globally.[2]
- Since 2016, the demand for Data Protection Officers (DPOs) has skyrocketed and risen over 700%, due to the GDPR demands.[3]

What can hackers do with my information?

- **Sell your data to other hackers**
 - One way hackers profit from stolen data is selling it in masses to other criminals on the dark web. These collections can include millions of records of stolen data. The buyers can then use this data for their own criminal purposes.
- **Identity theft**
 - using the victim's credit card or taking loans in their name.
- **used to target phishing attacks and extortion**
 - With stolen personal information criminals can target victims with phishing attacks. In phishing scams victims are lured into giving information like credit card details willingly to criminals by masking the scam as something legit. If criminals get access to very sensitive information, they can also extort the victim.

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

Self-driving cars as a target?

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

Content of the course


- **Part 1: Identification and authentication**
 - Passwords vs tokens vs biometrics; Multi factor vs single factor
 - Data aggregation, anonymity and pseudoanonymity;
 - Introduction to biometrics – finger print, facial, Iris/Retina, ECG, gait
- **Part 2: Monitoring & management**
 - Network management
 - Operation / administration / maintenance / provisioning
 - FCAPS (fault/config/accounting/performance/security)
 - Intrusion detection/prevention;
 - Techniques (statistics, pattern recognition, etc); and
 - Issues such as accountability vs privacy;
 - Management tools – preventing attacks / issues

Content of the course

- **Part 3: Cryptography & Steganography**
 - Information hiding: steganography & digital watermarking, ; Steganalysis & Cryptanalysis
 - Cryptography for secrecy, for signing, etc;
 - Symmetric key and asymmetric key protocols;
 - Applications, e.g encryption, key distribution, identification, authentication, electronic cash / cryptocurrencies.
 - Cryptographic protocols and their analysis

Content of the course

- **Part 4: Secure Network Design**
 - CIA Triad
 - Network attacks – interruption, interception, modification, fabrication
 - Passive vs active attacks
 - Data integrity (Hash function)
 - Methods of defence – Firewall: Bastion host / host(server) based / personal
 - Packet-filtering routers
 - Application-level gateways
 - Circuit-level gateways
 - Wireless security

- 
- **Part 5: Attacks**
 - Network vs human attack (Social engineering)
 - Intruders
 - Intrusion Techniques
 - Password Protection
 - Password Selection Strategies
 - Intrusion Detection
 - Viruses and Related Threats
 - Malicious Programs
 - The Nature of Viruses
 - Antivirus Approaches
 - Advanced Antivirus Technique
 - Malware: viruses and worms, spyware, denial/manipulation of service, etc;

- 
- **Part 6: Legal and Ethical Issues**
 - Pentesting – consent
 - Employee monitoring
 - **Part 7: Current and Future directions**
 - Fully Homomorphic Encryption;
 - Privacy-Preserving Computations
 - Quantum protocols and cryptography



Content of the course

- **Lab Sessions:**

- Include some programming with Java Cryptographic Architecture/Extensions (JCA/JCE).



Reading

[CNS]: Chapter 1

[NSE]: Chapter 1, sections 1.1 –1.3

[WSPC]: Chapter 1