Aim of the course

The aim of the course is to acquaint students with problems of computer security, the development of Students awareness of cybercrime threats and good habits to protect the confidentiality of information and the dissemination of good practices in the field of ensuring information security. will be presented the basic tools to protect information, such as encryption programs,

firewalls . IPS etc., but the lecture discusses not only the technical but also the legal, ethical, psychological and sociological aspects of computer security.

This course does not require pre-preparation of students in the field of computer security or special computer knowledge and is intended mainly for younger students.

Form of classes

30 will take two-hour meeting, wherein the first half term (15 matches) will be lecture to take place, and in the second half of the semester will be held 15 seminars conducted by the students. The lecture will discuss the basic issues of computer security. On seminars will be presented selected more specific questions. Each student in the course of 3 semester write essays (in any language they lead, in particular, it may be Polish or English). The pass mark for exercise is to get a positive assessment of the three essays. Fifteen authors of the best essays will be nominated to deliver seminars on the basis of their essays (in Polish or English).

Item will be conducted for the third time, which does not mean that the teacher already knows how to drive it. On the contrary, like the year before spapra it probably completely. People with weak nerves, low the level of empathy toward leading and representing the attitude of entitlement are requested is not written.

The lecture

I. INTRODUCTION

1. Introduction to computer security. Safety culture.
2. Copyright and plagiarism. Copyrights and piracy. The specificity of the media
   e. *Creative Commons* . Fair use. Good practices. To create and disseminate their own work with respect for other people's intellectual property. Discussion how to write essays.
3. Confidentiality of communications. GPG configuration. Creating a database of public keys and *key signing party* .

II. cybersecurity

1. National Cyber. Threats to critical infrastructure and economic order.
   Service established to protect the national security (NSA, GCHQ, ABW, FSB) and

permissions. Controversies. Cyberinwigilacja. WikiLeaks and Edward Snowden. Cyberwar. Cyberterrorism. Industrial espionage.

2. Cyber security entities under. a) culture of hackers and hacking. *White / gray / black hats* . Chaos Computer Club. The most famous hackers and their fate (Kevin Mitnick, Kevin Poulsen, Vladimir Lewin, Adrian Lamo and others). *script kiddies* . "Unsolicited pentesting." And legal problems threat. *Ethical hacking* . b) cyber crime. *spam* . *scam* , Fraud, extortion. *Nigerian 419 scam* . *phishing* . Risks of electronic banking, cybercrime organised. c) cyber vandalism and *trolling* . Vandalism on Wikipedia and other websites social networks. d) Haktywizm. Civil disobedience. Dred Scott. mahatma Gandhi. Thich Quang Duc. Aaron Swartz. Changing the law within the law or outside the law? Social movements. Anonymous. Wikileaks.

3. Cyberprywatność. a) The need for privacy and its protection. Public and private. Privacy at animals. Psychology, sociology and neurology privacy. Embarrassment and shame. Fourth Amendment to the US Constitution. Samuel D. Warren, Louis D. Brandeis, Judge Thomas McIntyre Cooley. b) Violation of privacy by the state. Panopticon, Orwell and Kafka. Universal monitoring. Mass data collection. Metadata. c) Violations Statement by corporations. Cyberprzemysł and "free services". Advertising industry. Google, Facebook and in. Collecting data on the Internet. Web cookies and *browser fingerprinting* .

III. DATA PROTECTION

1. Access Control. AAA protocols. Authentication method. Password. Safe mnemonic. Theory security passwords. Two-factor authentication. Psychological problems, *password fatigue* . CAS protocols. Biometric authentication.

2. Protecting data at rest. Digital forensics. Memory architecture computers. disks mechanical hard drives and SSDs. CIA triad. a) Availability of data. back-up and data archivization. *Failure recovery* . Available tools and techniques. b) Confidentiality and integrity data. Basics of cryptography. Drive Encryption. Available tools. c) Destruction of Data and reconstruction of damaged data.

3. The protection of data in motion. Network Fundamentals. Attacks on data transmission. MITM. *Typosquatting* . *Domain squatting* . *IDN homoglyph attack* . *BGP prefix hijacking* and *DNS spoofing / cache poisoning* . Network protocol stack and the principle of end-to-end. encryption layers of the TCP / IP stack. Encryption at the application layer. OpenPGP and S / MIME. encryption the transport layer. SSL / TLS. Public Key Infrastructure. *Certificate Authorities* and *Web of Trust* . Problems with CA TLS. Certificates in the Web browsers.

Sample topics of essays

1. Leaks of private data clouds. Dropbox Is it safe? Examples of events (eg.
latest leak pictures of naked celebrities). Methods of protection (encfs, duplicati, boxcryptor, cloudfogger, secretsync etc.).

2. CVV2 codes - to increase safety or whitewash?

3. Viruses and OS. Which system is a virus (it seems that Android beat
Windows). Are there viruses under Debian?

4. Internet censorship in the world. China's dispute with Google, Egypt in 2011, Russia.

5. What would happen if suddenly turned off the Internet?

6. Buffer overflow vulnerability - remains the most popular susceptibility enables
construct an attack on the code despite the memory protection, separation of data and code, etc. How possible?

7. Stuxnet - a one-time incident, or proof of concept? Will be continued?

8. Anonymous - history, facts. Why not attack the Russians during a dispute with Ukraine? really
Anonymous were all Russians?

9. SCADA and attacks on them. Can you misalign Wroclaw water supply over the Internet?

10. Keyloggers - how they work and how to defend against them?

11. legally acceptable surveillance. Required by law or by secretly introduced
governmental backdoors in popular protocols. WPS case. Dual_EC_DRBG. Heartbleed - accidental error or deliberate action?

12. The RFID and NFC. Convenience, or a threat? Surveillance by RFID. Attacks on NFC devices.
Attack prolonged terminal.

13. Emission security. Is it possible to construct a remote keylogger acting through a network
energy? Is it possible to capture data eavesdropping noise produced by electronic devices (including power supplies)?

14. How do Google Maps know where the traffic jams?

15. Electronic Signature qualified and trusted profile. Why we are not yet
e-citizens? Experience problems and E-stonia.

16. E-elections and e-voting. Protocols, security, experience.

17. Hardware random number generators. How to construct a good generator? How can
It improve the operation of the / dev / random?

18. Four-digit PIN stored on the card payment. They are doing it again! For what? How much is
Dangerous?

19. List the Robinsons - solution to the problem, or stratagem spammers and telemarketers to get around
right? And maybe one more way to phishing?

20. Electronic money. How it's working? Benefits and risks.

21. Pornography on the Internet and its blocking. Article 4a. Education System Act. Resolution of the Sejm
Polish Minister of the Republic calling for Administration and Digitization guarantee parents the right to the Internet without pornography. David Cameron's declaration of July 22, 2013 the imposition of a default on the Internet in Great Brytfanii filtrówmoralności and blocking

search query "sick people seeking illegal content on the network." is this Internet censorship? Right or dangerous? Is the Internet should be transparent?

22. Holes in the SSL / TLS: BEAST, CRIME TIME, BREACH, heartbleed, POODLE Is ...
    HTTPS connections are secure at all?
23. Buffer overflow vulnerability - remains the most popular susceptibility enables construct an attack on the code despite the memory protection, separation of data and code, etc. How possible?
24. Onion routing - how does it work? How to use it? Is it safe? Tor- who is behind this standing? Why did not prohibit?
25. Is Open Source software is safer than Closed Source?
26. Cyberbullying. Is it a social problem in Poland?
27. Cyber Islamist.
28. United States Cyber Command. History, tasks, methods of operation.
29. Cyberwojska North Korea. There is nothing to be afraid of?
30. Cyberdebilizm. General Petraeus Affair: the head of the CIA may not have the faintest idea cyberpoufności?
31. DNS protocol vulnerabilities to attacks and ways of protection. DNSSEC.
32. NTP and its vulnerability to attacks. CVE-2013-5211.
33. ecological footprint cyberinwigilacji. What is the impact on the environment NSA?

Literature

1. Ross Anderson, *Security Engineering* Wiley, 2008.