Security and Privacy

Michael Sonntag

Summary:

Aim of the course is to give an introduction to current problems of the two areas of security and privacy, and how they interact and can be solved through technological means, e.g. incident response techniques. The technological, legal, and society limitations of these approaches are discussed as well. Students will be introduced to the foundations of these topics through lectures. Based on these, current research and developments are presented and explained. Some aspects of each topic will be covered through practical work or demonstrations as well. The course encompasses for example introductions to security (threats to ICT, virtualization, risk analysis), the EU privacy framework based on the EU privacy regulation (including important decisions of the EuGH according to the previous directive) and computer forensics (basics and file system investigation).

Content (2 semester-hours combined lecture and practice)

Day 1: Lectures on security (Part 1)
Day 2: Lectures on security (Part 2)
Day 3: Lectures on privacy
Day 4: Practices on security and privacy (Practice day)
Day 5: Lectures on hot topics and examination (Discussion day)

Each day is designed for a duration of 8 units á 45 minutes.

Practical part

On the practice day (presence) resp. the practical parts (online version), some of the theoretical knowledge obtained in the lectures will be applied to practical problems: Security and privacy examples will be demonstrated or worked on by the participants under supervision and guidance.

Examination

Participants may take a written examination on the last day (online exam in case of the online version of the course). If students cannot take part there and then, submission of research papers are possible as well (this is only a subsidiary option).

Required environment for practical part:

1. One computer for each student (personal Laptops are fine)
    a. Operating system of the computer must be Windows
2. Possibility to install additional programs: Various software for forensic analysis
    a. Evaluation/full versions will be provided by the teacher
    b. Administrator rights on this computer are required!

Basic knowledge required by participants:

Knowledge about operating systems, networks (especially Internet and its protocols).
Security or legal pre-education/knowledge is **not** required!

Literature, software, and other materials:

All presentations (including pointers to further literature), the software, and the scenarios are provided to the participants online.

Distance teaching

Depending on the Covid situation and the rules of the university, the course will be held either at presence at the university in Prague, or via distance teaching (with students at home and/or at the university). This will be announced as soon as possible, but might occur only shortly before the course.

If this course is held via distance, the content stays exactly the same, but the organization is as follows:

- Each day starts with 2 units lecture via video conference (Zoom)
- Then follows 2 units independent work period based on tasks described in a document. Students complete these independently and prepare a two pages long report on it. The lecturer is available via chat the whole time (also via Zoom) for support.
- After a lunch break, again 2 units video conference lecture follows
- Afterwards are again 2 units independent work (similar to above)
- The day concludes with a brief (5-10 minutes) video conference for feedback by students & teacher. Students also submit both reports via E-Mail to the teacher.

In the distance version the daily reports will be part of the final mark, i.e. combined with the results from the (short) online exam. After each day a report with the results of the work done in both independent periods has to be sent **immediately** by E-Mail as PDF. Formatting etc is not important but should be as typically used (e.g. 12 point Times, 1.5 lines spacing, 2 cm borders - or similar). This should be a documentation of what you did and cover about two pages per 2 units assignment.

Daily plan (online/remote variant only!)

Video lecture: 8:30-10:00

Short break: 10:00-10:15

Independent work: 10:15-11:45

Lunch break: 11:45-12:45

Video lecture: 12:45-14:15

Short break: 14:15-14:30

Independent work: 14:30-16:00

Video wrap-up: 16:00-16:15

Submission of daily reports: Until 18:00

Detailed course content – Presence variant

Day 1: Security day 1

- 4U: Introduction to computer security: Attack profiles, security vs. protection, internal vs. external threats etc.
- 2U: Threats for computers and networks: Viruses, Trojans, Worms, Phishing; Firewalls, Intrusion Detection Systems, Anti-Virus software, CVSS: What are they, how do they work, what are their limitations
- 2U: Virtualization security: Sandboxes, containers etc.

Day 2: Security day 2

- 2U: Secure enclaves (Intel SGX): Computing in the cloud while keeping the data hidden from the cloud service provider
- 6U: Introduction to computer forensics: What is it, general procedures, equipment …

Day 3: Privacy day

- 4U: The EU privacy regulation (GDPR)
- 2U: Exemplary privacy cases: Reading a EU court decision, analyzing cases (Bodil Lindqvist, Promusicae, Huber, Gonzalez, …)
- 2U: Privacy enhancement techniques, surveillance and data retention countermeasures; secure destruction of data

Day 4: Practice day

- 3U: Analyzing privacy policies: Selecting criteria and comparing examples
- 3U: Information collection: NMap, Google cache/Web archive, Wireshark
- 2U: Network forensics and creating a timeline

Day 5: Related topics and practical application

- 2U: Cloud Security
- 1U: SCADA Security: Security aspects of industrial control systems
- 1U: Anonymity and Reidentification
- 2U: Discussion, feedback, reflection

Detailed course content – Online/remote variant

Overview – Online/remote variant

Day 1: Security day 1

- 2U lecture: Introduction to computer security: Attack profiles, security vs. protection, internal vs. external threats etc.
- 2U independent work: Introduction to computer security
- 2U lecture: Threats for computers and networks: Viruses, Trojans, Worms, Phishing; Firewalls, Intrusion Detection Systems, Anti-Virus software, CVSS: What are they, how do they work, what are their limitations
- 2U independent work: Virtualization security: Sandboxes, containers etc.

Day 2: Security day 2

- 2U lecture: Introduction to computer forensics: What is it, general procedures, equipment …
- 2U independent work: Introduction to computer forensics
- 2U lecture: Introduction to computer forensics
- 2U independent work: Secure enclaves (Intel SGX): Computing in the cloud while keeping the data hidden from the cloud service provider

Day 3: Privacy day

- 2U lecture: The EU privacy regulation (GDPR)
- 2U independent work: Exemplary privacy cases: Reading a EU court decision, analyzing cases (Bodil Lindqvist, Promusicae, Huber, Gonzalez, …)
- 2U lecture: The EU privacy regulation (GDPR)
- 2U independent work: Privacy enhancement techniques, surveillance and data retention countermeasures; secure destruction of data

Day 4: Practice day

- 2U practice: Network forensics and creating a timeline
- 2U independent work: Analyzing privacy policies: Selecting criteria and comparing examples
- 1U practice: Analyzing privacy policies
- 1U practice: Information collection: NMap, Google cache/Web archive, Wireshark
- 2U independent work: Information collection

Day 5: Related topics and practical application

- 2U lecture: Cloud Security
- 1U independent work: SCADA Security: Security aspects of industrial control systems
- 1U independent work: Anonymity and Reidentification
- 2U: Discussion, feedback, reflection

Contact details:

Assoc.Prof. Mag. Dipl.-Ing. Dr. Michael Sonntag
Institute of Networks and Security
Altenbergerstr. 69
A-4040 Linz
Austria
Telephone: +43(732)2468-4137
Fax: +43(732)2468-4125
E-Mail: michael.sonntag@jku.at
WWW: http://www.sonntag.cc/

Content:

Aim of the course is to give an introduction to current problems of the two areas of security and privacy, and how they interact and can be solved through technological means, e.g. incident response techniques. The technological, legal, and society limitations of these approaches are discussed as well. Students will be introduced to the foundations of these topics through lectures. Based on these, current research and developments are presented and explained. Some aspects of each topic will be covered through practical work or demonstrations as well. The course encompasses for example introductions to security (threats to ICT, virtualization, risk analysis), the EU privacy framework based on the new EU privacy regulation (including important decisions of the EuGH according to the previous directive) and computer forensics (basics and file system investigation).