

Security and Privacy

Michael Sonntag

Summary:

The aim of the course is to introduce current problems of security and privacy. How these can be solved through technological approaches, e.g. incident response techniques, is discussed together with their legal and society limitations. Students will be introduced to the foundations of the topics through lectures. Based on this, current research and development are presented and discussed. Some aspects of each topic will be covered through practical work in a lab too. Because of time-constraints, only selected specialty areas will be covered in detail, while others will only be mentioned.

Content (2 semester-hours combined lecture and practice):

Day 1: Lectures on security (Technical day)

Day 2: Lectures on privacy (Legal day)

Day 3: Lectures on computer forensics (Incident response day)

Day 4: Practices on security, privacy, and forensic problems (Practice day)

Day 5: Lectures on hot topics and examination (Discussion day)

Each day is designed for a duration of 8 units á 60 minutes.

In total 36 units plus a 2 unit examination and 1 unit reflection and feedback will be held.

Practical part

On the practice day, some of the theoretical knowledge obtained in the lectures will be applied to practical problems: Security, forensic, and privacy examples will be worked on by the participants under supervision and guidance.

Examination

Participants may take a written examination on the last day. If students cannot take part there, 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 (preferably their own – Laptops are fine)
 - a. Operating system of the computer must be Windows
 - b. CD-ROM drive required
 - c. 512 MB - 1 GB of free hard disk space for software and images to investigate
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:

1. Knowledge about operating systems
2. Knowledge of networks, especially the Internet, and its protocols

Security or legal pre-education/knowledge is **not** required!

Literature, software and other material:

CDs with all presentations (including pointers to further literature), the software, and the scenarios are provided for the participants free of charge.

Detailed course content

Day 1: Technical day

- 2U: 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
- 1U: Cryptography: Asymmetric and symmetric encryption, basic security methods (challenge response protocols, Diffie-Hellman, SSL, ...)
- 1U: Website security: Cross-site-scripting, SQL injection, buffer overflows
- 2U: Current developments and ongoing research: Tools for automating security checks: Availability, limitations, legality; Secure development

Day 2: Legal day

- 2U: EU privacy directive
- 1U: EU telecommunications privacy directive
- 2U: Exemplary privacy cases: Reading a EU court decision, analyzing cases (Bodil Lindqvist, Prosmusicae, Huber)
- 2U: European Convention on Cybercrime: What is illegal, implications for administrators and security professionals (incl. latest court decisions)
- 1U: Current developments and ongoing research: E.g. privacy enhancement techniques, surveillance and data retention countermeasures

Day 3: Incident response day

- 3U: Introduction to computer forensics: What is it, general procedures, equipment ...
- 1U: Duplicating file systems and investigating images for hidden information: Deleted data, File, RAM, and partition slack
- 2U: Investigating web and E-Mail history: Post-analysis (reconstructing viewed webpages, verifying and tracing E-Mail headers) and active techniques (techniques to identify when & where an E-Mail has been viewed)
- 1U: Reading and writing an expertise: Form, structure, content; assessing an expertise
- 1U: Current developments and ongoing research: E.g. new approaches to file carving through syntactic and semantic content analysis

Day 4: Practice day

- 2U: Recovering web browsing history and back-tracing E-Mails
- 2U: Identifying security problems: Vulnerability scanners
- 2U: Analyzing privacy policies: Selecting criteria and comparing examples
- 2U: Recovering information from file systems: Undelete, unformat, file carving etc.

Day 5: Discussion day

- 2U: Data retention: Legal outline (EU directive) and technical feasibility
- 1U: Online searches: Current legal framework, suitability, problems
- 1U: Data loss prevention: Possibilities and limitations
- 2U: Written examination
- 1U: Discussion, feedback, reflection

Abstract:

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 in a lab as well. The course encompasses for example introductions to security (threats to ICT, cryptography, risk analysis), website security, the EU privacy framework (including important decisions of the EuGH), the European Convention on Cybercrime (what security investigators may do legally), computer forensics (file system investigation, Web activity/E-Mail reconstruction, file carving), as well as data retention, the economy of internet crime and data loss prevention. The course requires only basic IT knowledge to attend (no security or legal pre-knowledge is necessary).

Contact details:

Priv.-Doz. Mag. Dipl.-Ing. Dr. Michael Sonntag
Institute for Information Processing and Microprocessor Technology (FIM)
Altenbergerstr. 69
A-4040 Linz
Austria
Telephone: +43(732)2468-9330
Fax: +43(732)2468-8599
E-Mail: michael@sonntag.cc
WWW: <http://www.sonntag.cc/>