Security & Legal Aspects of the WWW

Michael Sonntag

Summary:

The aim of the course is to introduce current problems of security and privacy, especially regarding the web. How these can be solved through technological approaches, e.g. incident response techniques, system design/implementation, 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. Selected aspects of each topic will be covered through practical work and in demonstrations. Because of time-constraints, only some specialty areas will be covered in detail, while others will only be mentioned.

Basic layout for the course (2 semester-hours combined lecture & practice):

Day 1: Lectures on security
Day 2: Lectures on security and computer forensics
Day 3: Lectures on computer forensics, security and legal aspects
Day 4: Practices on computer forensics, security and legal aspects
Day 5: Lectures on hot topics and examination

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

In total 36 units plus a 2-unit examination and 2-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, legal, and forensic examples will be worked on by the participants under supervision and guidance, respectively demonstrated by the lecturer.

Examination

Participants may take a written examination on the last day. 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 (preferably their own – Laptops are fine)
    a. Operating system of the computer should be Windows (Linux/Mac is possible, but the students must then download & install the software on their own)
    b. 12 GB of free hard disk space for software and images to investigate
2. Possibility to install additional programs: Various software for forensic analysis and for executing virtual machines (will be provided on DVD/memory stick)
    a. Evaluation/full versions will be provided by the teacher
    b. Administrator rights on the computer are required!

Literature, software and other material:

Memory sticks with all presentations (including pointers to further literature), the software, and the scenarios are provided to the participants to copy the material from them.

Detailed content:
Security & Legal Aspects of the WWW

Day 1: Security day

- 8U: Website security: Cross-site-scripting, SQL injection, buffer overflows...

Day 2: Security and incident response day

- 6U: Website security - Continued
- 2U: Investigating web history: Forensic analysis of which web pages have been visited and partly which actions where performed on them (reconstructing viewed webpages, intentionality)

Day 3: Incident response and legal day

- 2U: Windows forensics (e.g. typed URLs, printed pages, Registry...)
- 2U: Live Forensics (Linux): Investigation of a running system, exemplified by Linux
- 2U: Domain name disputes: UDRP + .eu-ADR
- 1U: E-Commerce directive: Provider liability
- 1U: European Convention on Cybercrime & EU Cybercrime directive: What is illegal, implications for administrators and security professionals

Day 4: Practice day

- 2U: Recovering web browsing history
- 2U: Web site security: SQL injection, Cross-Site-Scripting
- 2U: Windows Forensics: Recycle bin, Prefetch, USB, Thumbnails etc.
- 1U: Live Forensics: Finding a rootkit in a Linux system
- 1U: Password cracking

Day 5: Discussion day

- 2U: Anonymisation in the Internet, especially Tor
- 1U: Protecting web pages (obfuscation, captchas, session-ids…)
- 1U: Data loss prevention: Possibilities and limitations
- 2U: Written examination
- 2U: Reflection and feedback

Basic knowledge required by participants for the course:

1. Knowledge about operating systems
2. Knowledge of networks, especially the Internet, and its protocols
3. Basic knowledge of computer security, e.g. from the course in 2019

Legal pre-education/knowledge is **not** required!

Contact details:

Assoc.Prof. Mag. Dipl.-Ing. Dr. Michael Sonntag
Institute of Networks and Security (INS)
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:

The aim of the course is to introduce current problems of security and privacy, especially regarding the web, through lectures. Contents of the course include: Technical problems of web security (Cross-site-scripting, SQL injection, buffer overflows...), investigation of incidents (Client-side investigation of web activity, Windows & Linux forensics etc.), legal aspects of the web (liability of providers, domain name disputes...) and hot topics (how to protect web pages, anonymization etc). In addition, one day will be devoted to practical work on these issues, where participants will investigate a web-history, check a website for security problems, try to exploit and correct some of them, investigate the disk/system of a Windows user and find a rootkit on a Linux system.