

PV204 Security Technologies



Overview of the subject

Petr Švenda & Vít Bukač & Václav Lorenc &
Milan Brož & Petr Ročkai



People

- Main contact: Petr Švenda (CRoCS@FI MU)
 - Office hours: Tuesday 13:00-13:50, A406
 - svenda@fi.muni.cz, @rngsec
 - <https://crocs.fi.muni.cz/people/svenda>
- Other lectures and seminars
 - Milan Brož (RedHat), Petr Ročkai (FI), Vašek Lorenc (Netsuite/Oracle), Vít'a Bukač (Honeywell)

Covered topics

- Authentication, password handling, secure IM
- Trusted elements, side channels
- Secure hardware, smartcards, JavaCards
- Trusted Boot, TPM
- Analysis of compromised systems
- Malware, rootkits
- File and disk encryption, key management in cloud
- Multilevel security, security kernels

Previous knowledge requirements

- Basic knowledge of (applied) cryptography and IT security
 - symmetric vs. asymmetric cryptography, PKI
 - block vs. stream ciphers and usage modes
 - hash functions
 - random vs. pseudorandom numbers
 - basic cryptographic algorithms (AES, DES, RSA, EC, DH)
 - risk analysis
- Basic knowledge in formal languages and compilers
- User-level experience with Windows and Linux OS
- **Practical experience with C/C++/Java language**

Organization

- Lectures + seminars + assignments + project + exam
- Assignments
 - 6 homework assignments (+ 1 bonus)
 - **Individual work of each student**
 - Lab A403 available to students (except teaching hours)
- Project
 - **Team work** (2-3 members)
 - Details at seminars, analysis and modification of cryptographic library with secure hardware
- Exam
 - Written exam, open questions, pencil-only



Plagiarism

- Homeworks
 - Must be worked out independently by each student
- Projects
 - Must be worked out by a team of 3 students
 - Every team member must show his/her contribution (description of workload distribution, git commits)
- Plagiarism, cut&paste, etc. is not tolerated
 - Plagiarism is use of somebody else words/programs or ideas without proper citation
 - IS helps to recognize plagiarism
 - If plagiarism is detected student is assigned -5 points
 - In more serious cases the Disciplinary committee of the faculty will decide

Grading

- Credits
 - 2+2+2 credits, plus 2 for the final exams
- Points [**Notice minimal number of points required!**]
 - Assignments (30) – [**minimum 15 required**]
 - Project (20) – [**minimum 10 required**]
 - Written exam (50) – [**no minimum limit**]
 - Occasional bonuses 😊
- Grading 100 (max)
 - A \geq 90
 - B \geq 80
 - C \geq 70
 - D \geq 60
 - E \geq 50
 - F $<$ 50
 - Z \geq 35 (including minimum numbers from Assignments and Project)

Attendance

- Lectures
 - Attendance not obligatory, but highly recommended
- Seminars
 - Attendance **obligatory**
 - Absences must be excused at the department of study affairs
 - 2 absences are OK (even without excuse)
- Assignments and projects
 - Done during students free time (e.g. at the dormitory)
 - Access to network lab and CROCS lab possible

Course resources

- Lectures (PPT, PDF) available in IS
 - IS = Information System of the Masaryk University
- Assignments (what to do) available in IS
 - Submissions done also via IS
- Additional tutorials/papers/materials from time to time will also be provided in IS
 - To better understand the issues discussed
- Recommended literatures
 - To learn more ...