PV204 Security Technologies

Overview of the subject and grading
(updated 20200514 – one assignment less)

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

CROCS
Centre for Research on
Cryptography and Security

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), Milan Patnaik (U. Madras), Vašek Lorenc (Netsuite/Oracle), Víťa Bukač (Honeywell)

Covered topics

- Authentication, password handling, secure IM
- Trusted elements, side channels
- Microarchitectural attacks – Meltdown, Spectre
- Secure hardware, smartcards, JavaCards
- Trusted Boot, TPM
- Analysis of compromised systems, malware
- File and disk encryption, key management in cloud

Planned lectures (tentative)

17. 2.	Authentication and passwords (Petr Svenda)
24.2.	Disk/file encryption (Milan Broz)
2. 3.	Trusted element, side channels attacks (Petr Svenda)
9. 3.	Introduction to smart cards as secure elements (Petr Svenda)
16. 3.	JavaCard platform (Petr Svenda)
23. 3.	Micro-Architectural Attacks I. (Cache Timing, Prime+Probe, Meltdown (Milan Patnaik)
30. 3.	Micro-Architectural Attacks II. (Spectre) (Milan Patnaik)
6. 4.	Secure authentication and authorization (Petr Svenda)
13.4.	HSMs (Petr Svenda)
20. 4.	Trusted boot (Petr Svenda)
27. 4.	Blackbox malware analysis (Vit Bukac)
4. 5.	Forensic memory analysis (Vaclav Lorenc)
11. 5.	Bitcoin, Secure Multiparty Computation (Petr Svenda)

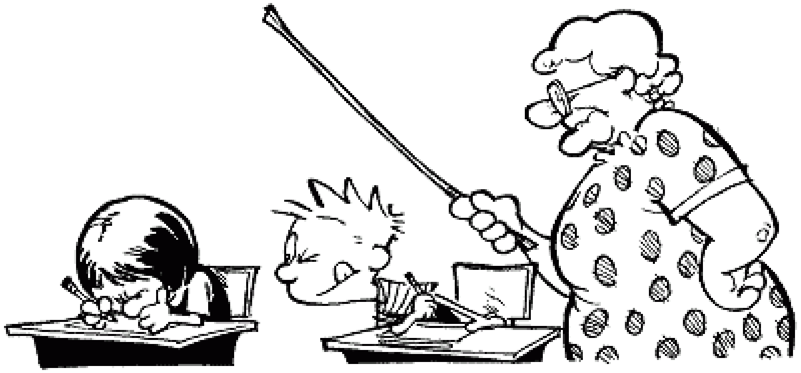
Previous knowledge requirements

- 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
  - 10 regular homework assignments
  - **Individual work of each student**
  - Lab A403 available to students (except teaching hours)
- Project
  - **Team work** (2-3 members)
  - Details later at seminars, analysis of certified security products
- Exam
  - Written exam, open questions

Plagiarism



http://dkdavis.weebly.com

- 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

Original version before Covid-related restrictions

- Credits
  - 2+2+2 credits, plus 2 for the final exams
- Points [Notice minimal number of points required!]
  - Assignments (50) – [minimum 25 required]
  - Project (30) – [minimum 15 required]
  - Written exam (50) – [no minimum limit]
  - Occasional bonuses ☺
- Grading 130 (max)
  - A ≥ 110
  - B ≥ 100
  - C ≥ 90
  - D ≥ 80
  - E ≥ 65
  - F < 65
  - Z ≥ 65 (including minimum numbers from Assignments and Project)

Grading – updated

- Credits
  - 2+2+2 credits, plus 2 for the final exams
- Points [Notice minimal number of points required!]
  - Assignments ~~(50~~ 45) – [minimum ~~25~~ 22.5 required]
  - Project (30) – [minimum 15 required]
  - Written exam (50) – [no minimum limit] + 95% correct from drill questions
  - Occasional bonuses ☺
- Grading ~~130~~ 125 (max), limits decreased by 5 points
  - A ≥ 105
  - B ≥ 95
  - C ≥ 85
  - D ≥ 75
  - E ≥ 60
  - F < 60
  - Z ≥ 60 (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 student 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 …