

PV204 Security Technologies



Overview of the subject and grading



Petr Švenda & Lukasz Chmielewski & Václav Lorenc &
Milan Brož & Antonín Dufka





Top questions (1) ▾

P PetrS

0 👍

Is my password brute-force-able if consists of 9 printable characters?

- **Place/upvote questions in slido while listening to lecture video**
- **We will together discuss these during every week lecture Q&A**

Join at

slido.com

#pv204_2024

People

- Main contact: Petr Švenda (CROCS@FI MU)
 - svenda@fi.muni.cz, @rngsec
 - <https://crocs.fi.muni.cz/people/svenda>
- Other lectures and seminars
 - Lukasz Chmielewski, Milan Brož (MU), Vašek Lorenc (HERE Technologies)
- Spring 2024 semester fully in person
 - Sometimes pre-recorded/online lectures (holidays)
 - Interactive lectures + Q&A lecture sessions
 - In-person standard seminars

Spring 2024 semester organization

- Lectures
 - Different format based on the lecturer (mostly in person, pre-recorded)
- In-person lecture & Q&A sessions (every Monday from 16:00)
 - Discussion of topics, interactive activities, flipped classroom style
 - Come, it will be fun 😊
 - Questionnaire from the lecture (open till first seminar – do it before)
- In-person hands-on seminars (every Thursday 10/14/16:00)
 - Mandatory attendance
 - Bring own laptops with software prepared in advance (email)

Covered topics

- Authentication, password handling, secure IM
- Trusted elements, side channels
- Secure hardware, smartcards, JavaCards
- Secure Multiparty Computation
- Trusted Boot, TPM, secure enclaves
- Analysis of compromised systems, malware
- File and disk encryption
- Bitcoin-related security topics

Planned lectures (tentative)

- 19.2. Authentication and passwords (Petr Svenda)
- 26.2. Secure authentication and authorization (Petr Svenda)
- 4.3. Smartcards, JavaCards programming and management (Petr Svenda)
- 11.3. SmartCards II., Multi Party Computation (Petr Svenda)
- 18.3. Disk/file encryption (Milan Broz)
- 25.3. Trusted boot Hardware Security Modules and Cloud (Petr Svenda)
- 1.4. Bitcoin I - Bitcoin basics (Petr Svenda)
- 8.4. Bitcoin II. - related topics (Petr Svenda)
- 15.4. Trusted systems, side-channels and constant-time (Lukasz Chmielewski)
- 22.4. Advanced side-channels (Lukasz Chmielewski)
- 29.4. Advanced fault injection (Lukasz Chmielewski)
- 6.5. Memory analysis (Vaclav Lorenc)
- 13.5. Project presentation (Antonin Dufka)

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 regular homework assignments
 - **Individual work of each student**
- Project
 - **Team work** (3 members)
 - Details in pv204_project_2024.pdf (IS)
 - Secure system design and implementation
- Exam
 - Drill questions, Open book open questions, Oral exam

Plagiarism



- Assignments
 - 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, activity during presentation)
- 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 if exam
- Points [**Notice minimal number of points required!**]
 - Questionnaire from lectures (10) [**no minimum limit**]
 - Assignments (30) – [**minimum 15 required**]
 - Project (30) – [**minimum 15 required**]
 - Exam (30) – [**must know basics**] + 95% correct from drill questions
 - Occasional bonuses 😊
- Grading 100 (max)
 - $A \geq 90$, $B \geq 80$, $C \geq 70$, $D \geq 60$, $E \geq 50$, $F < 50$
 - $Z \geq 50$ (including minimum numbers from Assignments and Project)

Attendance

- Lectures
 - Attendance not obligatory, but highly recommended
 - Interactive Q&A sessions
- Seminars
 - Attendance **obligatory**
 - Absences must be excused at the department of study affairs
 - 3 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

Discussion forum in Information System

- Discussion forum in Information System (IS)
 - <https://is.muni.cz/auth/cd/1433/jaro2024/PV204/>
- Mainly for discussion among the students
 - Not observed by us all the time!
 - Write us email if necessary please
- What to ask?
 - OK to ask about ambiguities in assignment
 - NOT OK to ask for the solution
 - NOT OK to post your own code and ask what is wrong

Course resources

- Lectures (video, PDF) available in IS
 - IS = Information System of the Masaryk University
 - Lecture questionnaires in IS opened till end of Monday
- Assignments (what to do) available in IS
 - Submissions done also via IS (homework Vault)
- Additional tutorials/papers/materials from time to time will also be provided in IS
 - To better understand the issues discussed
- Recommended literature
 - To learn more ...

Questions ?

