# PV204 Security Technologies

## Overview of the subject and grading

Petr Švenda & Milan Patnaik & Lukasz Chmielewski &

Vít Bukač & Václav Lorenc & Milan Brož & Antonín Dufka

CRoCS

Centre for Research on
Cryptography and Security

# 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), Milan Patnaik (U. Madras), Vašek Lorenc (HERE Technologies), Víťa Bukač (HERE)
- Spring 2022 semester is in person (fingers crossed)
  - Sometimes pre-recorded/online lectures
  - Interactive lectures + Q&A lecture sessions
  - In-person standard seminars

# Spring 2022 semester organization

- Lectures
  - Different format based on the lecturer (in person, pre-recorded, online)
  - Typically
    - Pre-recorded video, uploaded into IS on Friday previous week
    - Watch before Tuesday next week, fill questionnaire
- In-person lecture & Q&A sessions (every Tuesday from 12:00)
  - Discussion of topics, interactive activities, flipped classroom style
  - Come, it will be fun ☺
- In-person hands-on seminars (every Thursday 10/14:00)
  - Mandatory attendance (time flexibility in picking the seminar group)

# Covered topics

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

# Planned lectures (tentative)

| | |
|---|---|
| 15.2. | Authentication and passwords (Petr Svenda) |
| 22.2. | Secure authentication and authorization (Petr Svenda) |
| 1.3. | Smartcards, JavaCards programming and management (Petr Svenda) |
| 8.3. | Disk/file encryption (Milan Broz) |
| 15.3. | Side-channels and constant-time (Lukasz Chmielewski) |
| 22.3. | Cryptocurrencies I. - Bitcoin basics (Petr Svenda) |
| 29.3. | Cryptocurrencies II - related topics (Petr Svenda) |
| 5.4. | Trusted boot Hardware Security Modules and Cloud (Petr Svenda) |
| 12.4. | Micro-Architectural Attacks I. (Spectre) (Milan Patnaik) |
| 19.4. | Micro-Architectural Attacks II. (Cache Timing, Prime+Probe, Meltdown (Milan Patnaik) |
| 26.4. | Blackbox malware analysis (Vit Bukac) |
| 3.5. | Thread modelling / Memory analysis (Vaclav Lorenc) |
| 10.5. | 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**
  - Lab A403 available to students (except teaching hours)
- Project
  - **Team work** (2-3 members)
  - Details in pv204_project_2022.pdf (IS)
  - Secure system design and implementation
- Exam
  - Drill questions, Oral exam

# Plagiarism

http://dkdavis.weebly.com

- 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

# Project organization

- Groups of three students
- Project defense / report
- Theme: Selection of applied cryptography topics
- GitHub repository, commits from all participants required

# 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 ≥ 90, B ≥ 80, C ≥ 70, D ≥ 60, E ≥ 50, F < 50
  - Z ≥ 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/jaro2022/PV204/
- Mainly for discussion among the students
  - Not observed by stuff 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 questionares 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