PV204 Security Technologies

Overview of the subject and grading

Petr Švenda & Vít Bukač & Václav Lorenc &

Milan Brož & Milan Patnaik & 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
  - Milan Brož (RedHat), Milan Patnaik (U. Madras), Vašek Lorenc (Konica-Minolta), Víťa Bukač (Honeywell)
- Whole Spring 2021 semester is online-only
  - Pre-recorded or online lectures
  - Interactive Q&A lecture sessions
  - Interactive online seminars

Spring 2021 online semester organization

- Whole Spring 2021 semester is online-only (Zoom, link in IS)
- Lectures
  - Pre-recorded videos, uploaded into IS before Thursday 20:00
    - Watch before Monday next week, fill questionnaire
  - Some lectures online with recording (Monday 16:00)
- Interactive lecture & Q&A sessions (every Monday 17:00)
  - Discussion of topics, interactive activities, flipped classroom style
  - Come, it will be fun ☺
- Interactive online hands-on seminars (every Thursday 10/14/16:00)
  - Mandatory attendance (time flexibility in picking the seminar group)
  - Not recorded, but handouts and other materials available

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)

1.3.	Authentication and passwords (Petr Svenda)
8.3.	Secure authentication and authorization (Petr Svenda)
15.3.	Cryptocurrencies I. - Bitcoin basics (Petr Svenda)
22.3.	Cryptocurrencies II - related topics (Petr Svenda)
29.3.	Smartcards, JavaCards programming and management (Petr Svenda)
5.4.	Trusted boot (Petr Svenda)
12.4.	Hardware Security Modules and Cloud (Petr Svenda)
19.4.	Micro-Architectural Attacks I. (Spectre) (Milan Patnaik)
26.4.	Micro-Architectural Attacks II. (Cache Timing, Prime+Probe, Meltdown (Milan Patnaik)
3.5.	Disk/file encryption (Milan Broz)
10.5.	Forensic memory analysis (Vaclav Lorenc)
17.5.	Blackbox malware analysis (Vit Bukac)
24.5.	Project presentation

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_overview_2021.pdf (IS)
  - Analysis of certified security product documents
- 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]
  - Oral exam, three topics (30) – [must known 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/jaro2021/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