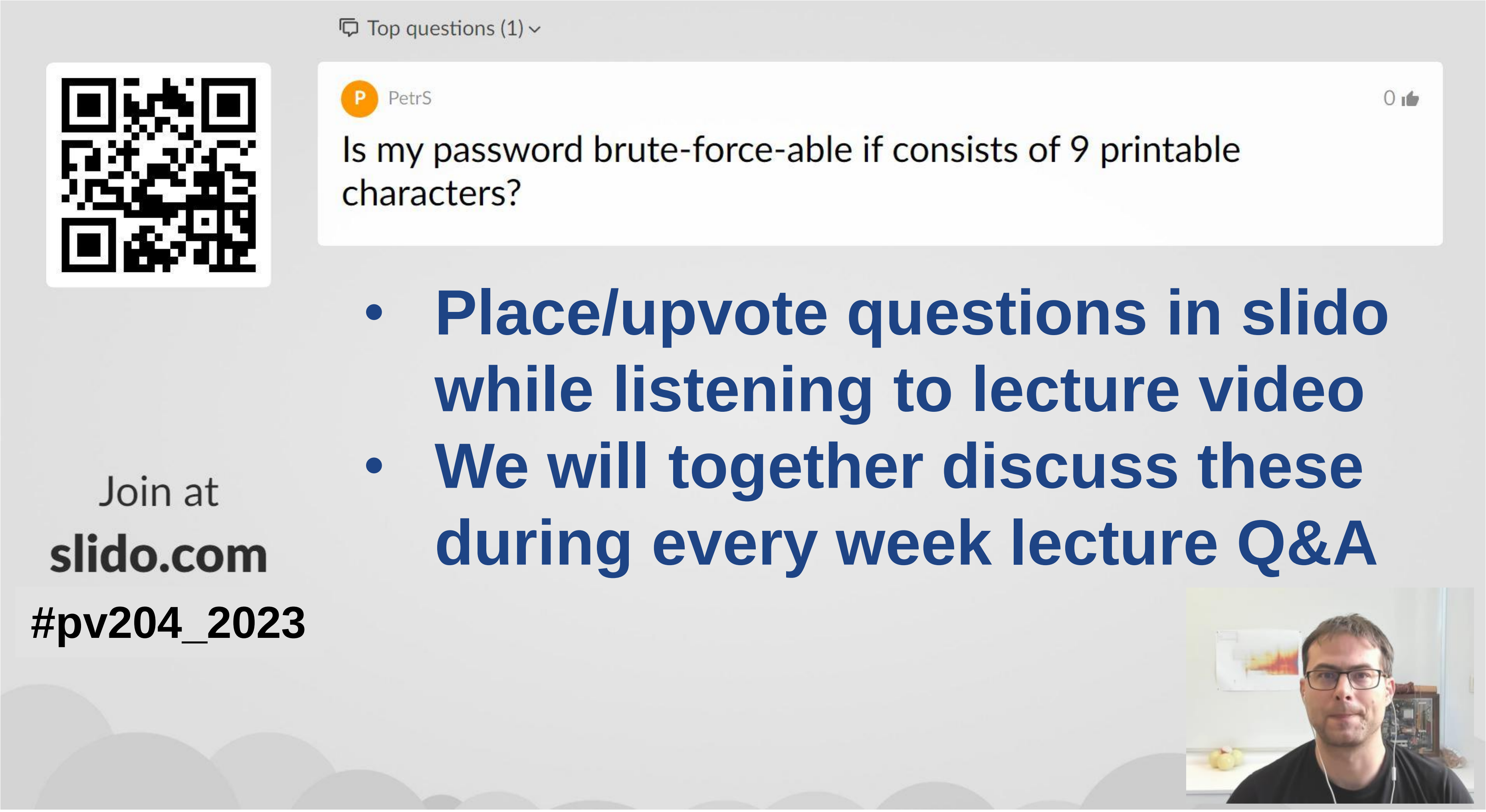
PV204 Security Technologies

Overview of the subject and grading

IS,1998

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

CROCS
Centre for Research on
Cryptography and Security



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_2023

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), Víťa Bukač (HERE)
- Spring 2023 semester is in person
  - Sometimes pre-recorded/online lectures
  - Interactive lectures + Q&A lecture sessions
  - In-person standard seminars

Spring 2023 semester organization

- Lectures
  - Different format based on the lecturer (in person, pre-recorded, online)
- In-person lecture & Q&A sessions (every Monday from 12:00)
  - Discussion of topics, interactive activities, flipped classroom style
  - Come, it will be fun ☺
- In-person hands-on seminars (every Thursday 10/14/16:00)
  - Mandatory attendance
  - Questionnaire from the lecture (at very beginning)

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, key management in cloud

Planned lectures (tentative)

13.2.	Authentication and passwords (Petr Svenda)
20.2.	Secure authentication and authorization (Petr Svenda)
27.2.	Smartcards, JavaCards programming and management (Petr Svenda)
6.3.	SmartCards II., Multi Party Computation (Petr Svenda)
13.3.	Disk/file encryption (Milan Broz)
20.3.	Cryptocurrencies I. - Bitcoin basics (Petr Svenda)
27.3.	Cryptocurrencies II - related topics (Petr Svenda)
3.4.	Side-channels and constant-time (Lukasz Chmielewski)
10.4.	Trusted boot Hardware Security Modules and Cloud (Petr Svenda)
17.4.	Advanced side-channels (Lukasz Chmielewski)
24.4.	Blackbox malware analysis (Vit Bukac)
1.5.	Memory analysis (Vaclav Lorenc)
8.5.	- nothing -
15.5.	Project presentation (Antonin Dufka)

PB173 – Binary exploitation module

- Reverse engineering, binary exploits, microarchitectural attacks
- Milan Patnaik, block teaching in April
  - Lecture Tuesday 16:00–18:00
  - Seminar Thursday 12:00-14:00 or 16:00-18:00
- If sounds interesting to you, enroll now

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_2023.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/jaro2023/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