PV204 Security Technologies

Overview of the subject

Petr Švenda & Vít Bukač & Václav Lorenc &

Milan Brož & Petr Ročkai

CROCS

Centre for Research on Cryptography and Security

People

- Main contact: Petr Švenda (CRoCS@FI MU)
  - Office hours: Tuesday 15:00-15:50, A406
  - svenda@fi.muni.cz, @rngsec
  - https://crocs.fi.muni.cz/people/svenda
- Other lectures and seminars
  - Milan Brož (RedHat), Petr Ročkai (FI), Vašek Lorenc (Netsuite/Oracle), Víťa Bukač (Honeywell)

Covered topics

- Trusted elements, side channels
- Secure hardware, smartcards, JavaCards
- Authentication, password handling, secure IM
- Reverse engineering of binary applications
- Analysis of compromised systems
- Malware, Rootkits
- Trusted Boot, TPM
- Multilevel security, security kernels
- Disk encryption

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 homework assignments (+ 1 bonus)
  - **Individual work of each student**
  - Lab A403 available to students (except teaching hours)
- Project
  - **Team work** (2-3 members)
  - Details at seminars, secure hardware-related application
- Exam
  - Written exam, open questions, pencil-only

Grading

- Credits
  - 2+2+2 credits, plus 2 for the final exams
- Points [Notice minimal number of points required!]
  - Assignments (30) – [minimum 15 required]
  - Project (20) – [minimum 10 required]
  - Written exam (50) – [no minimum limit]
  - Occasional bonuses ☺
- Grading

	100 (max)
A ≥ 90% of maximum number of points	90
B ≥ 80% of maximum number of points	80
C ≥ 70% of maximum number of points	70
D ≥ 60% of maximum number of points	60
E ≥ 50% of maximum number of points	50
F < 50% of maximum number of points	

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 students free time (e.g. at the dormitory)
  - Access to network lab and CRoCS lab possible

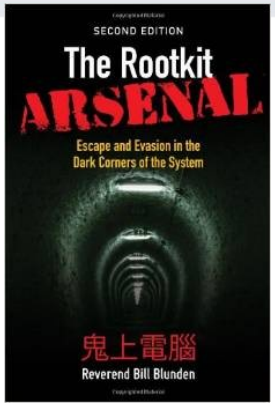
Course resources

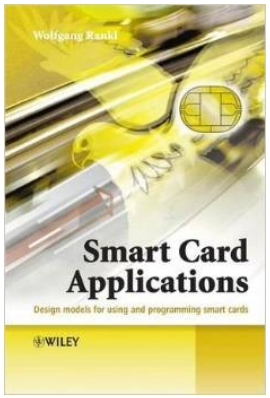
- Lectures (PPT, PDF) available in IS
  - IS = Information System of the Masaryk University
- Assignments (what to do) available in IS
  - Submissions done also via IS
- Additional tutorials/papers/materials from time to time will also be provided in IS
  - To better understand the issues discussed
- Recommended literatures
  - To learn more …

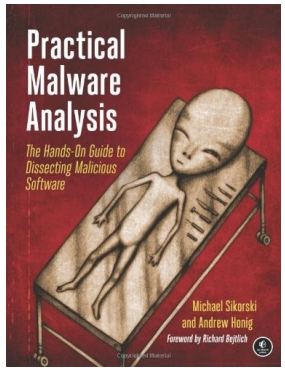
Discussion forum in Information System

- Discussion forum in Information System (IS)
  - https://is.muni.cz/auth/cd/1433/jaro2018/PV204/
- Mainly for discussion among the students
  - Not observed by stuff all the time!
  - Write us email if necessary
- 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

Recommended literature







- Bill Blunden. The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System. Wiley; 1 edition, 2007. ISBN-10: 1593272901.
- Wolfgang Rankl, Kenneth Cox. Smart Card Applications: Design models for using and programming smart cards. ISBN-10: 047005882X
- Michael Sikorski, Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press; 1 edition, 2012.ISBN-10: 1593272901.

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