PV204 Security Technologies

Overview of the subject

Petr Švenda & Zdeněk Říha & Vít Bukač &

Václav Lorenc & Milan Brož

CROCS

Centre for Research on
Cryptography and Security

Requirements

- **Basic knowledge of computer networks**
- Basic knowledge in applied cryptography and IT security
- User-level experience with Windows and Linux OS, ability to configure tools and/or interfaces
- Practical experience in programming with imperative languages like C/C++ or Java

Organization

- Lectures + seminars + assignments + project + exam
- Assignments
  - Assigned regularly (nearly) every week
  - individual work of each student
  - expected workload: 4+ hours/week/participant
  - Network lab available to students
- Project
- Exam
  - Written exam, mostly open questions

Project organization

- Groups of several (usually three) students
- Project defense / report
- Expected workload: 16 hours/project/participant
- Theme: design and implement simple security application with aid secure hardware (two factor auth)

Grading

- Credits
  - 2+2+2 credits, plus 2 for the final exams
- Points
  - Homework (30) – min 15 required
  - Project (30) – min 15 required
  - Written exam (90)
- Grading
  - A ≥ 90% of maximum number of points
  - B ≥ 80% of maximum number of points
  - C ≥ 70% of maximum number of points
  - D ≥ 60% of maximum number of points
  - E ≥ 50% of maximum number of points
  - F < 50% of maximum number of points

Attendance

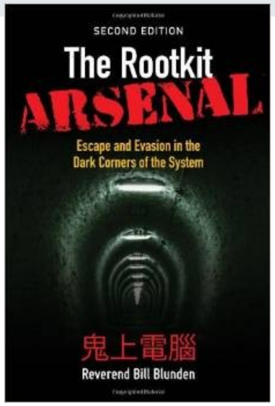
- Lectures
  - Attendance not obligatory, but highly recommended
  - Not recorded (small lecture room without video facilities)
- Seminars
  - Attendance obligatory
  - Absences must be excused at the department of study affairs
  - 2 absences are ok
- Assignments and projects
  - Done during students free time (e.g. at the dormitory)
  - Access to network lab and CRoCS lab is possible
    - Some assignments indeed require access to the network lab

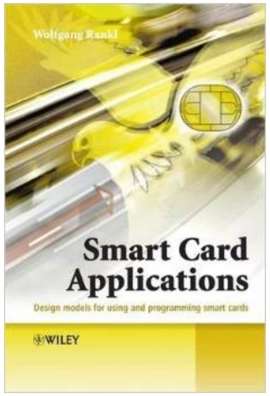
Course resources

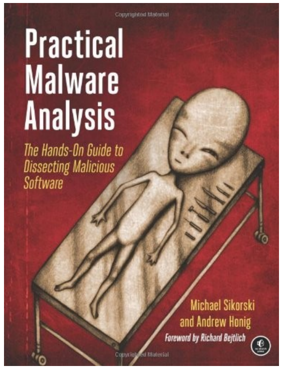
- Lectures (PDF) available in IS
  - IS = Information System of the Masaryk University
- Assignments (what to do) available in IS
  - Submissions done also via IS
- Additional tutorials/papers/materials from time to time will also be provided in IS
  - To better understand the issues discussed
- Recommended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

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.






Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich

Plagiarism

- 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
- 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