PV181 Laboratory of security and applied cryptography

Course organization

Marek Sýs
syso@mail.muni.cz, A405

CROCS
Centre for Research on Cryptography and Security

Course info

- Practical focus (hands-on) - working with tools and libraries
- Style of seminars may vary (different lecturers) but:
  - small intro at the beginning of every seminar (no lectures) with materials and tasks
  - individual work = coding
- Discussion:
  - Ask tutor within the seminar when you got stuck,
  - IS discussion group if everybody might be interested (e.g. if assignment is not clear)

Seminars overview

- 1x RNG (Sys)
- 1x ASN1 (Sys)
- 2x Basic Crypto concepts (Chmielewski)
- 3x Crypto libs in C (Broz) - OpenSSL and various libs
- 1x Advanced crypto concepts (Chmielewski) – OpenSSL, EC (python)
- 1x Standards (Riha)
- 1x Java crypto Architecture and Extensions (Chmielewski)
- 1x Crypto-libraries protected against hardware attacks (Chmielewski)
- 1x Biometrics (Kruzikova, Galanska)

- Extra (voluntary, bonus points): 28.09 Binary Exploitation (Patnaik)

Assignments

- Homeworks/assignments
  - 10 points maximum
  - 10 assignments (100 points + 10), one extra seminar (28.09) with bonus points
  - 65 % required (i.e. 65 points or 50 points)
  - Submit files into is.muni.cz
  - Points for your HW within one week in is.muni.cz
  - **plagiarism is strictly forbidden**:
    - source of the copied code must be cited

Credit/colloquium

- To get the credit or colloquium
  - You must be present at seminars (2 absences OK)
  - You must be active at seminars
  - You must submit assignments and get:
    - 50 % of maximum number of points for the **credit**
    - 65 % of maximum number of points for the **colloquium**