PV181 Laboratory of security and applied cryptography

Course organization

Łukasz Chmielewski
chmiel@fi.muni.cz, A406

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 (us) when stucked (within the seminar),
  - IS discussion group if everybody might be interested (e.g. if assignment is not clear)

Seminars overview

- 3x Symmetric, Asymmetric, and Advanced Crypto-topics (Łukasz Chmielewski)
- 1x RNG (Marek Sys)
- 1x ASN1 (Marek Sys)
- 3x Crypto libs in(C, C++) (Milan Brož)
  - OpenSSL and various libs
- 1x Certificates and OpenSSL in Python (Łukasz Chmielewski)
- 1x Standards (Zdeněk Říha)
- 1x Biometrics: face detection/recognition (Agáta Kružíková and Katarína Galanská)
- 1x CISC (Intel) Binary Exploitation (Milan Patnaik)
- 1x Crypto-libraries protected against hardware attacks (Łukasz Chmielewski)

Preliminary Schedule

- 20.09: Basic Crypto by Lukasz
- 27.9: RNG by Marek
- 4.10: Asymmetric Crypto by Lukasz
- 11.10: ASN1 by Marek
- 18.10: Crypto libs in(C, C++) [Part 1] by Milan B.
- 25.10: Crypto libs in(C, C++) [Part 2] by Milan B.
- 1.11: Crypto libs in(C, C++) [Part 3] by Milan B.
- 8.11: Microarchitectural Attacks by Milan P. (online)
- 15.11: Standards by Zdeněk
- 22.11 Advanced Crypto by Lukasz
- 29.11: Biometrics by Agata & Katarina
- 6.12: Crypto-libraries protected against hardware attacks by Lukasz
- 13.12: Passwords Security by Alessia and Lukasz

Assignments

- Homeworks/assignments
  - 10 points maximum
  - 10 assignments (100 points)
    - There will be some extra points
  - 65 % required (i.e. 65 points or 50 points)
  - Submit files into is.muni.cz:
    - code + write-ups (word, pdf, or txt with markups)
  - Points for your HW within one week in is.muni.cz
  - **Deadline:** usually until the next seminar (approx. 1 week)
  - **plagiarism is strictly forbidden**:
    - The 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

People

- Main contact: Łukasz Chmielewski (CRoCS@FI MU)
  - Office hours (consultation): Friday 9:00-11:00, A406
  - chmiel@fi.muni.cz,
  - https://keybase.io/grasshoppper

- Other seminars:
  - Milan Brož (CRoCS@FI), Marek Sýs (CRoCS@FI), Zdeněk Říha (European Commission), Agáta Kružíková (CRoCS@FI), and Katarína Galanská (CRoCS@FI).