PV181 Laboratory of security and applied cryptography



Course organization

Marek Sýs syso@mail.muni.cz, A405



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

Seminars overview

- 1x RNG (Marek Sys)
- 2x Basic crypto, Advanced crypto (Arnab Roy)
- 1x ASN1 (Marek Sys)
- 1x Certificates (Arnab Roy)
- 3x Crypto libs in(C, C++) (Milan Broz)
 - OpenSSL and various libs
- 1x OpenSSL in python (Arnab Roy)
- 1x Standards (Zdenek Riha)
- 2x Biometrics (Martin Ukrop, Agata Kruzikova)
 - also partly in PV080
- Extra(voluntary, bonus points): 17.11 Exploits (Milan

Patnaik)

Assignments

- Homeworks/assignments
 - 10 points maximum
 - 10 assignments (100 points + 10), one extra seminar (17.11) 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