PB173 - Tématický vývoj aplikací v C/C++
Domain specific development in C/C++

Skupina: Aplikovaná kryptografie a bezpečné programování

Petr Švenda svenda@fi.muni.cz

Konzultace: A406, Pondělí 15:00-15:40

CROCS
Centre for Research on Cryptography and Security

PRESENTATIONS OF TEAMS DESIGNS

What to focus on during presentation

- Try to really understand design presented during presentation
- Ask questions if anything is unclear
  - No stupid questions exist, just stupid answers ☺
- Ask questions just to confirm that your understanding is correct
  - Don’t assume that because YOU know how to make particular thing properly, it was done properly by PRESENTER
  - The main goal is to understand how PRESENTER solve that

Architecture overview

- Assets
  - What has the value in the system?
  - What damage is caused when successfully attacked?
  - What mechanisms are used to protect assets?
- Roles
  - Who has access to what?
  - What credentials needs to be presented?
- Thread model
  - What is expected to do harm?
  - What are you defending against?

PRESENTATIONS

Practical assignment

- Update your design documents based on feedback
  - And add into GitHub repo (docs folder)
- Create implementation of server process
  - No network communication yet, just methods + tests!
- Functions to be implemented (and tested!)
  - new user registration (in: user name / password, out: status)
    - New user stored in local “database” (ini file, sqllite…)
  - user authentication to server (in:user/pass, out: status)
    - Check supplied info against info from local database
    - Use PBKDF2 or better function to generate hash to check
  - obtain list of other online users (out: formated list – JSON?)
    - Users that were successfully authenticated now assumed to be online
- Don’t forget to document functions in JavaDoc-style

What should tests cover?

- Add new user
  - New user -> success
  - New user, but existing name -> fail
  - Try to add 2, 100 new users -> success
- User authentication
  - Existing user, correct password -> success
  - Existing user, incorrect password -> fail
  - Non-existing user -> fail
- Get list
  - Expected users in list
- …

Submissions, deadlines

- Upload application source codes as single zip file into IS Homework vault (Crypto - 4. homework (UT))
  - Zip file from current version of repo
  - Updated design documents
- DEADLINE 21.3. 12:00
  - Up to 10 points assigned