PA193 Security technologies

Team projects: Static and dynamic analysis for open-source projects

Petr Švenda
Faculty of Informatics, Masaryk University, Brno, CZ

CROCS
Centre for Research on
Cryptography and Security

Project idea

1. Prepare and run static & dynamic analysis tools on existing open-source project (fuzzing, sanitizers)
2. Analyze the results, identify bugs, false positives…
3. Create patches for several bugs and pull request

Project

1. Run static & dynamic analysis tools on existing open-source project
   - Select project from pre-approved list or suggest another (needs to be confirmed)
   - Use git (GitHub), fork original repository (contributions from all members required)
   - Run suitable static analyzers over the source code
   - Setup environment for fuzzing (AFL preferred), make long-time fuzzing
   - Prepare repository and compile with Clang sanitizers, analyze results
2. Analyze bugs found, classify them, make report
   - Prepare presentation with findings
   - Types of bugs found, false positives vs. true positives ratio…
3. Implement bugfixes for at least three issues found and create pull request
   - Discuss suitability of bugs and fixes with course teacher and project maintainers

Teams

- 3 people per team
  - Assigned today (within the same seminar group)
- Teams must use GitHub for cooperation
  - Distribute work load between all members
  - Contribution from all team members must be visible in commits (git commits from the member)
  - Your evaluation will be partially based on your participation
- Start working early, intermediate checkpoints

Projects - timeline

1. Fork & compile, run static analyzers: **4 points**
   - Demonstrate project functionality, GitHub repo
   - Setup and run static analyzers (all available, must argue why not used)
   - Report + presentations [seminar 11.10.2018]
2. Setup, run and evaluate fuzzer: **5 points**
   - AFL preferred (must argue why not used), let run for at least 3 days
   - Report + presentations (types of bugs found) [seminar 1.11.2018]
3. Setup, run and evaluate sanitizers: **4 points**
   - Report + presentations [seminar 15.11.2018]
4. Write patch for at least three bugs/problems: **7 points**
   - Notify me once patches are committed [before 20.12.2018]

- At least 10 points (total) from the project are required

Immediate next steps

- Form groups, exchange participants emails
- Get together and select your favorite project
- Send me email with your group and selection ASAP
  - First come first served basis, wait for confirmation
  - not later than **4.10.2018**
- Fork/setup repo at GitHub
- Compile the project, run tests, get familiar with its functionality
- Run static analysis, evaluate bugs, prepare for presentation (10 mins max) **11.10.2018**

Projects available for selection

- libp11
  - https://github.com/OpenSC/libp11
- OpenSC
  - https://github.com/OpenSC/OpenSC/
- PCSC
  - https://github.com/LudovicRousseau/PCSC
- PCSC CCID
  - https://github.com/LudovicRousseau/CCID
- libpwquality
  - https://github.com/libpwquality/libpwquality
- Linux PAM
  - https://github.com/linux-pam/linux-pam
- Own suggestion (needs to be agreed with Petr Svenda)

TEAMS

FIXME ☺