PB173 - Tématický vývoj aplikací v C/C++ Domain specific development in C/C++ (Fall 2014)

Skupina: Aplikovaná kryptografie a bezpečné programování

https://is.muni.cz/auth/el/1433/podzim2013/PB173/index.qwarp?fakulta=1433;obdobi=5983;predmet=734514;prejit=2957738;

Petr Švenda svenda@fi.muni.cz
Konzultace: A406, Pondělí 15-15:50

CROCS
Centre for Research on Cryptography and Security

Security code review

- Architecture overview
  - Design choices and possible design flaws
- Code review
  - How well is architecture actually implemented
- Whitebox, greybox & blackbox testing
  - different level of access to code and documentation
- Available tools
  - mainly for code review

Security code review (2)

- You will always have a limited time
  - try to rapidly build overall picture
  - use tools to find low hanging fruit
- Focus on most sensitive and problematic areas
  - use tools to focus your analysis scope
- More eyes can spot more problems
  - experts on different areas

Architecture overview

Architecture overview

- Get all information you can quickly
- 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?

Architecture overview (2)

- Usage of well established techniques and standards
- Comparison with existing schemes
  - What is the advantage of new scheme?
  - Why changes were made?
- Security tradeoffs documented
  - Possible threat, but unmitigated?
  - Is documented or overlooked?

Sensitive data flow mapping

- Identify sensitive data
  - password, key, protected data...
- Find all processing functions
  - and focus on them
- Create data flow between functions
  - e.g. Doxygen call graph
- Inspect when functions can be called
  - Is key schedule validity checked?
  - Can be function called without previous function calls?
- Where are sensitive data stored between calls?

Protocol design (and implementation)

- Packet confidentiality, integrity and authenticity
- Packet removal/insertion detection
- Replay attack
- Reflection attack
- Man in the middle

Practical assignment

- Every team uploads project documentation
  - Upload to IS, today
- Download and analyze other projects
- Points will be awarded according to:
  - number and severity of the problems found
  - quality of own architecture

Practical assignment

- Some tips what to analyze:
  - Which functions are manipulating with sensitive information?
  - Where is random numbers coming from?
  - What are key lengths?
  - How to impersonate user?
  - Can be older communication replayed?
  - …
- Not only outsider remote hacker…

Practical assignment (2)

- Summarize your findings
  - problem identification + severity + applicability + short description
  - 2 pages enough (per project)
  - Submit before 20.10.2014 23:59
- Present your findings next week (5-10 minutes)

Problem identification: A_x (security architecture) / C_x (code, implementation)
Severity: low / middle / high / not deciable
Practicability: easy (directly by external attacker) / depends on other parts of the system / cannot decide (potential flaw, but attack unknown yet)
Description of the problem: description
Proposed solution: simple description (in case we know some)