PA193 - Secure coding principles and practices

Security Code Review

Petr Švenda svenda@fi.muni.cz

CROCS
Centre for Research on Cryptography and Security

Security code review – simple.zip

- Download simple.zip from IS
  - Try to build and run it
- Perform security code review (bottom-up approach)
  - Run static / dynamic analysis tools (more of them)
  - Inspect source code and make high-level overview
  - Make call graph (by hand or automatically)
  - Find and document problems

Problem identification: DSA-1571-1 openssl
Severity: critical
Risk: high - directly exploitable by external attacker
Problem description: crypto/rand/md_rand.c:276 & 473 – The random number generator in Debian's openssl package is predictable…
Remediation: revert back to usage of uninitialized buffer *buff*

Some hints

- Classes of problems
  - Bad usage of cryptography
  - Keys
  - Unsafe functions
  - Race condition
  - Memory corruptions
  - Information leakage
  - Sensitive data handling
- *(Don’t focus on Blowfish.cpp – no intentional issues there)*

Optional: Security code review – large one

- Download larger security project by your selection
  - Winscp, GnuPG, KeePass, Putty, Bitcoin…
- Inspect compiled binary
  - Try to detect what crypto algorithms were used
  - http://at4re.com/download.php?view.30
- Get idea about structure of code
  - Can you find where user password is supplied and processed?

Usage of crypto somehow hidden?