Lecture 3 Outline

April 5, 2016

Reading: *text*, §16.4; [Chr11,OWA13] **Assignments due:** Homework 1, on Apr. 5

1. Greetings and felicitations!
2. Puzzle of the Day
3. Capabilities
   a. Revocation: use of a global descriptor table
4. MULTICS ring mechanism
   a. Rings, gates, ring-crossing faults
   b. Used for both data and procedures; rights are REWA
      (b_1, b_2) access bracket—can access freely; (b_3, b_4) call bracket—can call segment through gate; so if a's access bracket is (32, 35) and its call bracket is (36, 39), then assuming permission mode (REWA) allows access, a procedure in:
      rings 0–31: can access a, but ring-crossing fault occurs
      rings 32–35: can access a, no ring-crossing fault
      rings 36–39: can access a, provided a valid gate is used as an entry point
      rings 40–63: cannot access a
   c. If the procedure is accessing a data segment d, no call bracket allowed; given the above, assuming permission mode (REWA) allows access, a procedure in:
      rings 0–32: can access d
      rings 33–35: can access d, but cannot write to it (W or A)
      rings 36–63: cannot access d
5. Some common vulnerabilities
   a. Catalogues: CVE (Common Vulnerabilities and Exposures), CWE (Common Weakness Enumeration)
   b. 2011 MITRE/SANS Top 25 Most Dangerous Software Errors
   c. OWASP Top 10 – 2013 rc1 The Ten Most Critical Web Application Security Risks
6. MITRE/SANS list
   a. Insecure interactions among components
      i. SQL injection
      ii. OS command injection
      iii. Cross-site scripting
      iv. Unrestricted upload of file with dangerous type
      v. Cross-site request forgery
      vi. URL redirect to untrusted site
   b. Risky resource management
      i. Buffer copy without checking size of input
      ii. Improper limitation of a pathname to a restricted directory
      iii. Download of code without integrity check
      iv. Inclusion of functionality from untrusted control sphere
      v. Use of potentially dangerous function
      vi. Incorrect calculation of buffer size
      vii. Uncontrolled format string
      viii. Integer overflow or wraparound
   c. Porous defenses
      i. Missing authentication for critical function
      ii. Missing authorization
      iii. Use of hard-coded credentials
      iv. Missing encryption of sensitive data
      v. Reliance on untrusted inputs in a security decision
      vi. Execution with unnecessary privileges

   vii. Incorrect authorization
   viii. Incorrect permission assignment for critical resource
   ix. Use of a broken or risky cryptographic algorithm
   x. Improper restriction of excessive authentication attempts
   xi. Use of a one-way hash without a salt

7. OWASP list
   a. Injection
   b. Broken authentication and session management
   c. Cross-site scripting
   d. Insecure direct object references
   e. Security misconfiguration
   f. Sensitive data exposure
   g. Missing function level access control
   h. Cross-site request forgery
   i. Using known vulnerable components
   j. Unvalidated redirects and forwards
8. Comparison
   a. Everything on the OWASP list is also on the MITRE/SANS list
   b. Injection is #1 on both lists
   c. The MITRE/SANS list covers vulnerabilities generally; OWASP covers only web vulnerabilities

---

Discussion Problem. You discover a security flaw in the operating system on your company's computer. The flaw enables any user to read any other user's files, regardless of their protection. You have several choices: you can keep quiet and hope no-one else discovers the flaw, or tell the company, or tell the system vendor, or announce it on the Internet.

1. Suppose an exploitation of the vulnerability could be prevented by proper system configuration. Which of the above courses of action would you take, and why?
2. If an exploitation of the vulnerability could be detected (but not prevented) by system administrators, how would this change your answer to the first question?
3. Now suppose no exploitation of the vulnerability can be detected or prevented. Would this change your answer, and if so, how?