Integrating the Common Weakness Enumeration into a Secure Programming Course

Pascal Meunier, M.Sc., Ph.D., CISSP

CS390S: Secure Programming
• Since Fall 2002
• Review common mistakes
• Buffer Overflows
• Format String Vulnerabilities
• etc...

• Concepts
• Trust Management
• Input Validation
• Meta-Characters and escapes
• Character encodings
• etc...

• Is the coverage representative?
• Is the coverage done correctly?
• How do employers know what students learned in the class?

New Slides Based on View

The Common Weakness Enumeration
• Compatibility declarations, Spring 2007
• Group CVE entries by similarity
• CWE ID given to each
• Entries are linked in a tree (parent/children)
• Tree is huge! (see on right)
• Organization is often more appropriate for code scanners than teaching
• Example: No branch matching trust management concepts

New CWE Views Needed For Teaching
Goal: Re-organize CWE entries in a tree that matches the concept to be taught

Example: Trust

Legend: Matched CWE IDs Missing CWE IDs

• Trust Boundary Problems
  • Inconsistent validation mechanisms
    • Same source handled differently in different code locations
    • At different times
    • In different circumstances
    • From different sources
  • Authentication Bypass by Alternate Path/Channel, ID 288
    • Unprotected Alternate Channel, ID 420
  • Ill-defined trust boundaries
  • Trust Boundary Violation, ID 501

• Displaced or Absent Trust Boundaries

• Self-reported information
  • Trusting self-reported IP address, ID 291
  • Self-reported & reverse DNS name, ID 292
  • Using referer field for authentication, ID 293

• Trusting the client
  • Client-side makes server security decisions
  • Server trusting client-side-controlled data

• Cryptographic Trust Assurance
  • Certificate issues, ID 296
    • Failure to follow chain of trust in certificate validation, ID 296
    • Failure to validate host-specific certificate data, ID 287
    • No OpenSSL Certificate Check Performed before this Use, ID 599
  • Failure to validate certificate expiration, ID 298
  • Failure to check for certificate revocation, ID 299
  • Race condition in checking for certificate revocation, ID 370

Conclusions
• Creating views is work intensive
• Views highlight missing CWE IDs
• Feedback improves the CWE
• Course declared CWE compatible
• Course quality improved
• More examples and cases
• Strong linkage of concepts to a systematic empirical collection
• Views could help form the basis of new taxonomies or ontologies