Testing Software Quality Characteristics – Part 2

Security Testing

Ira A. Fulton Schools of Engineering
Arizona State University

Objective

Objective

Identify basic security testing approaches

Security Testing

- Software correctness and security are not the same
- Most applications contain private data
- Goal of security testing is to ensure private data is protected from unauthorized users

Security Fundamentals

Confidentiality

- Application
- Data

Integrity

- Data modification
- Functions performed

Availability

- Denial of service

Security Testing Context

- Software may have unintended or unknown functionality that may produce side-effects contributing to security problems

- Security flaws require testing software interactions with its environment

Components that Might Exploit Software

- OS
- File System
- GUI
- Other systems (databases, libraries, etc.)

GUI Security Risks

- Verify access control
  - Entry to system
  - Access to functions and data
- Look for all possible access methods to data
  - Cut and paste
  - Screen capture
- Evaluate malicious input
  - Denial of service

File System Security Risks

- Evaluate how data is stored and retrieved

- Focus on encryption and data protection

OS Security Risks

- Evaluate decrypted data storage in memory

- Stress test with low memory
  - System under memory stress may leave data unprotected

Other Component Security Risks

- Consider results of component failure

- Components may consist of libraries, databases, etc.

Security Testing Strategies

- Deny application access to libraries it needs
  - Ensure crashes do not impact security
- Try to overflow input buffers by inputting long strings
- Try special characters as inputs
- Try default or common user names and passwords

Security Testing Strategies (cont’d)

- Attempt to fake the source of data
  - Consider a system with packets sent over the network which contain source identifier
  - Fake source in packet

- Force system to use default values
  - Do not enter data when prompted
  - Exploit time outs

Security Testing Strategies (cont'd)

- Test all routes to perform a task
  - Consider opening a file
  - Ensure all scenarios go through security validation

- Produce each error message and ensure that it does not compromise security

Approaches for Improving Security Testing

- Consult public security databases
  - CERT (www.cert.org)
  - Contain information about published software bugs

- Reason about errors in databases and possible vulnerabilities in your product
  - What caused the failure
  - How might it have been detected during test
  - Is system vulnerable to attack

Summary