Managing Software Security Risk

TDT60
06.09.2005

Risk analysis

Risk = Probability X Consequence

• Used to rank risks – a tool to determine which risks needs to be handled
• Requires the ability to identify risks, calculate probability and define consequence in numbers
• Risk matrix:
Software Risk Management

- Post-development add-on of security is too late!
- Tradeoff: security goals vs software project goals
- Risk analysis is used as a tool in the software development and maintenance process
- Iterative development methodology
- Risks identified, handled and tested at each iteration
- Goal: minimize the risk that a new system is vulnerable

The spiral development model
Roles and responsibility

• "Security lead"
  – Focus on security
  – Should be skilled sw developer as well as knowledgeable about security issues, known vulnerabilities and attacks
  – Objective
  – Participate in all project phases
    • Requirements
    • Risk assessment
    • Design
    • Implementation
    • Testing

Requirements

• Identify security requirements
  – What needs to be protected
  – From whom
  – For how long
  – Value
  – Why

• All requirements should be verifiable

• Use existing guidelines
Risk assessment

• Based on system specification – requirements, design, prototype

• Risk manager – should be objective

• Rank risks in order of severity
  – Resource allocation – testing, analysis

• Basis for security testing

Design for security

• Focus on security implications of all design decisions
  – How data flow between components
  – Users, roles and rights
  – Trust relationships of each component
  – Solutions to identified problems – use well-known and tested solutions
Implementation

- Language dependant vulnerabilities
  - Requires in-depth knowledge of the security issues of the programming language(s) used
- Consistency with design
- Code review – auditing software

Security testing

- Probing/provoking a system – looking for weaknesses
  - Strange/unexpected behavior indicates possible vulnerability
- Black box
- White box
- Code coverage