Improving Security in the Application Development Life-cycle

*Migchiel de Jong*

*Software Security Engineer*

*mdejong@fortifysoftware.com*

*March 9, 2006*

General contact: Jurgen Teulings, 06-30072736  
*jteulings@fortifysoftware.com*
Business Issues

- Staying off of the front page because of a hack
- Protect your customer assets and goodwill
- Risk with outsourced software
- Insecurity of third party and business partner software
- Protect against malicious insider activity
- Document and monitor a secure development lifecycle in support of regulatory compliance

The total cost impact on the financial services sector from an inadequate software-testing infrastructure is estimated to be $3.3 billion, according to the National Institute of Standards & Technology.
Security: Layered Solutions To Mitigate Risk

- Hackers
- Worms & Viruses
- Malicious Insiders

Traditional network/perimeter defenses

Critical Software Automation Of Key Operational Processes
Software Apps Cut Through The Layers

Outsourcing

Legacy App Integration

Web Facing Applications

Employee Self-Service

Connectivity w/ Partners & Suppliers
Today Hackers (and Insiders) Use The Software

There is an emerging and robust science of “hacking” software:

- SQL Injections
- Buffer Overflows
- Information Leakage
- Numerous Other Categories

According to Gartner Group, “Over 70 percent of security vulnerabilities exist at the application layer, not the network layer.” It’s not just operating systems or web browsers, but all types of applications—particularly applications that automate key business processes.
Leading Organizations Starting To Address The Problem

Security Design
Reviews

Network-based
Solutions

Source Code
Audits

Developer
Training

Application
Penetration Tests
Steps to take to deliver more secure Code

- Evaluate and Plan
- Specify the Risk and Threats to the Software
- Review the Code
- Test and Verify the Code
- Build a Gate
- Measure
- Educate
A simple Check List

- Internal Security experts exist and have been identified
- Threat analysis completed for every project
- Education programs for security occur regularly
- Specific tools and resources have been acquired and allocated
- Post-deployment security if fully integrated in the overall process
- Vulnerability response maximizes benefits and prevents repeats
Software Security as a Gate

- Used as final check pre-deployment
- Acceptance of outsourced software
- A first step in a comprehensive program
Second Step

Software Security With Specialists At Discrete Process Points

- Automation make specialists more productive
- Central repository makes comparisons possible
- Build awareness of security within development process

2 Software Security Specialists

PLAN  DESIGN  CODE  FUNCTIONAL TEST  ACCEPTANCE TEST  DEPLOY
Ultimate Goal

Software Security Throughout Development Process

- Eliminate vulnerabilities when they are least costly
- Continual artifacts for compliance and secure quality assurance
- Built in protection

Integrated Adoption through the Software Lifecycle

1. PLAN
2. DESIGN
3. CODE
4. FUNCTIONAL TEST
5. ACCEPTANCE TEST
6. DEPLOY
Automation support

Source Code Analysis
- Source Code Security Audits

Security Testing
- Security Automation For QA

Application Defense
- Run-Time Protection

Software Security Management
- Software Security Metrics and Reporting

PLAN
DESIGN
CODE
FUNCTIONAL TEST
ACCEPTANCE TEST
DEPLOY
Source Code Analysis

CODE
C, C++, .Net
Java, JSP,
PLSQL, TSQL,
XML, Cold Fusion

3RD PARTY IDE PLUG-INS
Microsoft
Borland
eclipse
IBM

ANALYSIS ENGINE
Semantic
Global Data
Flow
Control Flow
Configuration
Structural

SECURE CODING RULES
Packaged
Custom

MANAGER
AUDITOR / DEVELOPER
Data Flow Analysis

- Ability to follow data flow across tiers
  - Doing this kind of analysis is really time consuming (at least without automation)

- Ability to follow data flow across languages
  - Reduces audit, development and testing skill set
Source code analysis demonstration

- Static analysis of OWASP’s WEBGOAT version 3.7
- Metrics
Thank You

General contact: Jurgen Teulings, 06-30072736
jteulings@fortifysoftware.com