
Chris Steel, Ramesh Nagappan, Ray Lai

&

Brian Chess (Moderator)

February 17, 2005 15:25 – 16:35
About the Panelists

• Chris Steel, CISSP
  Chief Architect, Fortmoon Consulting
  csteel@adelphia.net

• Ramesh Nagappan
  Technology Architect, Sun Microsystems
  Ramesh.Nagappan@sun.com

• Ray Lai
  Principal Engineer, Sun Microsystems
  Ray.Lai@sun.com

• Brian Chess (Moderator)
  Chief Scientist, Fortify Software
  Brian@fortifysoftware.com
About the Session

"From the ground up, the Java platform was designed for security. Read this book to learn how to apply patterns and proven technologies to secure your J2EE applications and beyond."

—James Gosling, father of the Java programming language

Chris Steel, Ramesh Nagappan, Ray Lai
authors@coresecuritypatterns.com
www.coresecuritypatterns.com
Objectives

• Introduce a radical approach for building trustworthy applications
• Proactive and prescriptive guidance
• Patterns-driven security development and deployment
• Best practices and reality checks
Common Security Issues

• Security as an add-on
• Architectural inefficiencies
• Proprietary and incompatibility issues
• Poor infrastructure choices
• Poor operational practices
• Poor identification and verification
• Poor configuration management
• Poor security policies and controls
• Lack of awareness and expertise
• Lack of management priorities
Common Application Security Issues

- Input validation failures
- Output sanitation
- Buffer overflow
- Data injection flaw
- Improper error handling
- Weak session identifiers
- Weak security tokens
- Weak password exploits
- Cross-site scripting
- Session theft
- Insecure configuration data
- Broken authentication
- Access control failure
- Policy failure
- Audit & logging failure
- Denial of Service / XML DOS
- Replay
- Man in the middle
- Multiple sign-on
- Deployment problems
- … A growing list
Secure Unified Process

**Development Disciplines**
- Business Modeling
- Requirements
- Analysis and Design
- Implementation
- Test
- Development

**Support Disciplines**
- Configuration Management
- Project Management
- Environment
- Operations and Support

**Security Disciplines**
- Security Requirements
- Security Architecture
- Security Design
- Security Implementation
- White Box Testing
- Black Box Testing
- Monitoring
- Security Audits

---

Copyright ©2005 Steel, Nagappan, Lai
Secure UP Workflow
Pattern Format

- Problem
- Forces
- Solution
- Structure
  - Participants
  - Responsibilities
- Strategies
- Consequences
- Security factors and risks
- Reality Checks

RSA Conference 2005
Questions