

RSA Conference 2005



DEV-302: Security Patterns and Best Practices for J2EE, Web Services and Identity Management

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



core SECURITY PATTERNS

Best Practices and Strategies for J2EE™,
Web Services, and Identity Management



- Patterns catalog includes 23 new patterns for building end-to-end security
- Security design methodology, patterns, best practices, reality checks, pro-active security assessments, defensive strategies and checklists
- Applied techniques for Web services security, Identity Management, and Service Provisioning
- Comprehensive security guide using J2SE™, J2EE™, J2ME™, and Java Card™



CHRIS STEEL • RAMESH NAGAPPAN • RAY LAI

Forewords by Judy Lin (EVP, VeriSign) and Joe Uniejewsk (CTO, RSA Security)

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

RSA Conference 2005



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

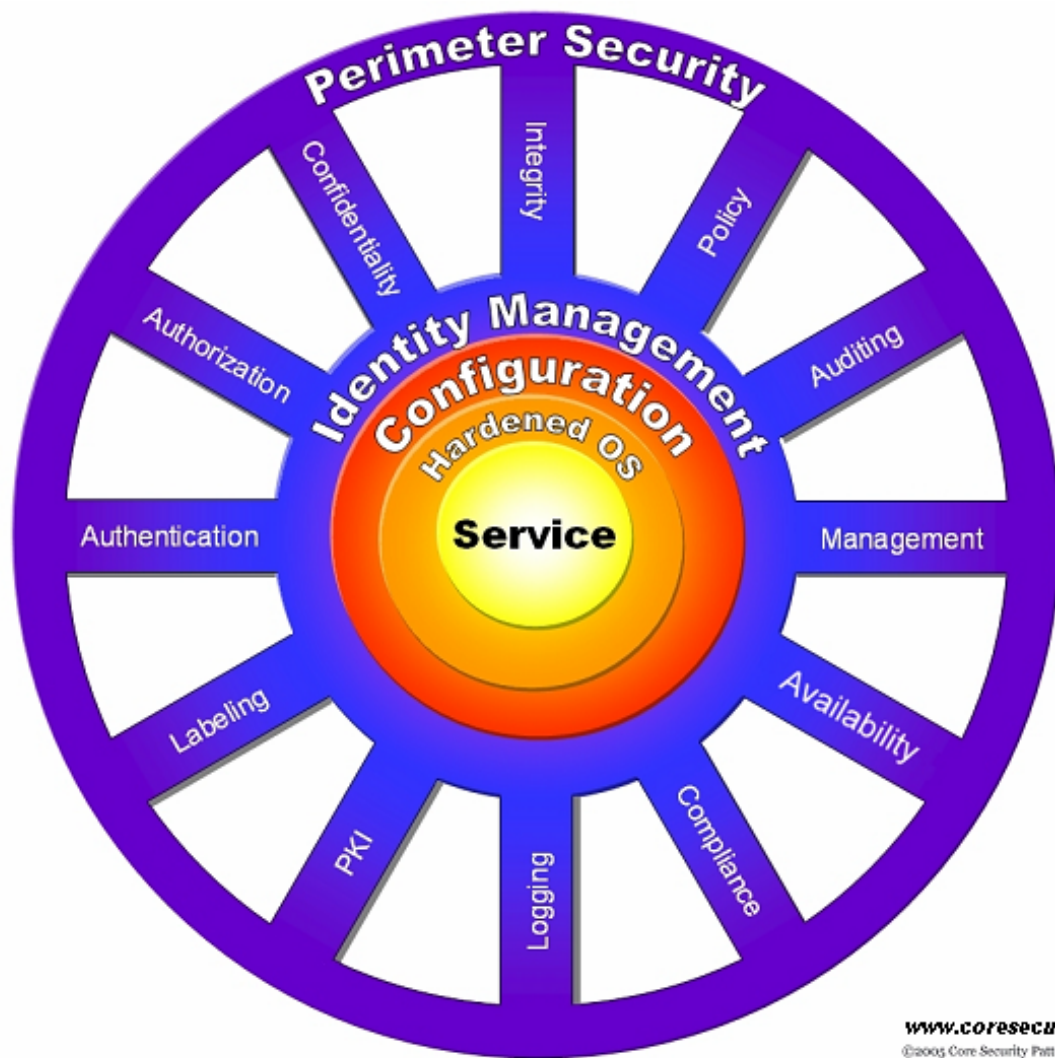


Common Application Security Issues

- 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



Security Wheel



www.coresecuritypatterns.com

©2005 Core Security Patterns

RSA Conference 2005



Secure Unified Process

Development Disciplines

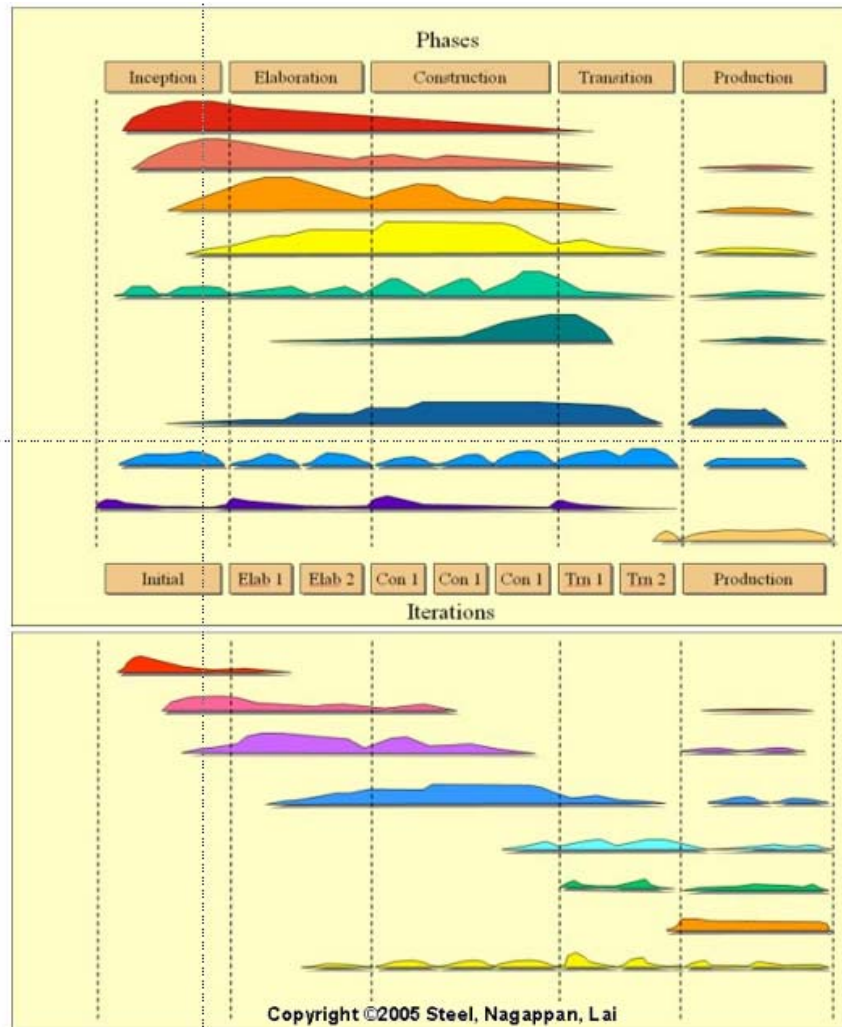
- Business Modeling
- Requirements
- Analysis and Design
- Implementation
- Test
- Development

Support Disciplines

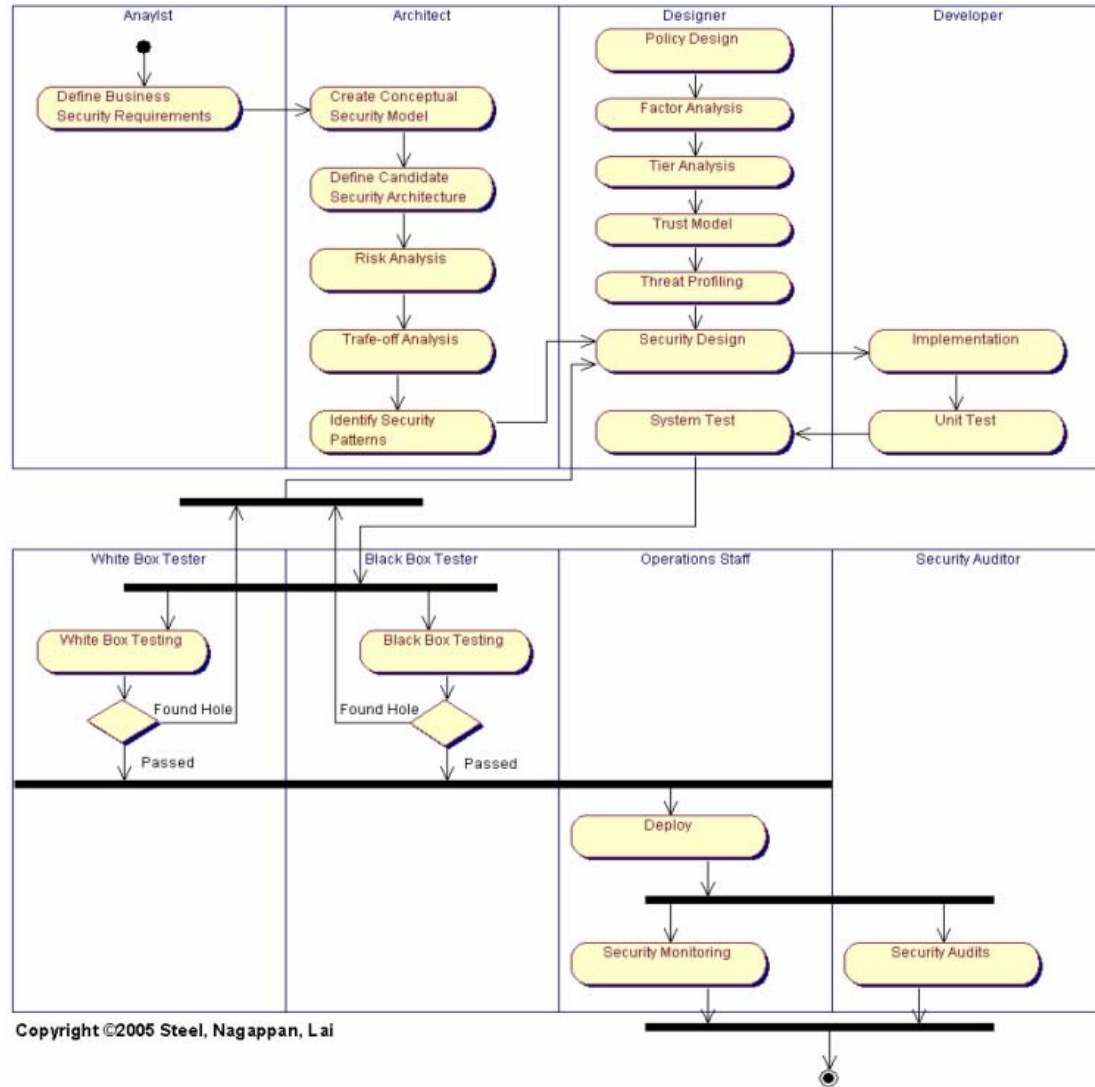
- Configuration Management
- Project Management
- Environment
- Operations and Support

Security Disciplines

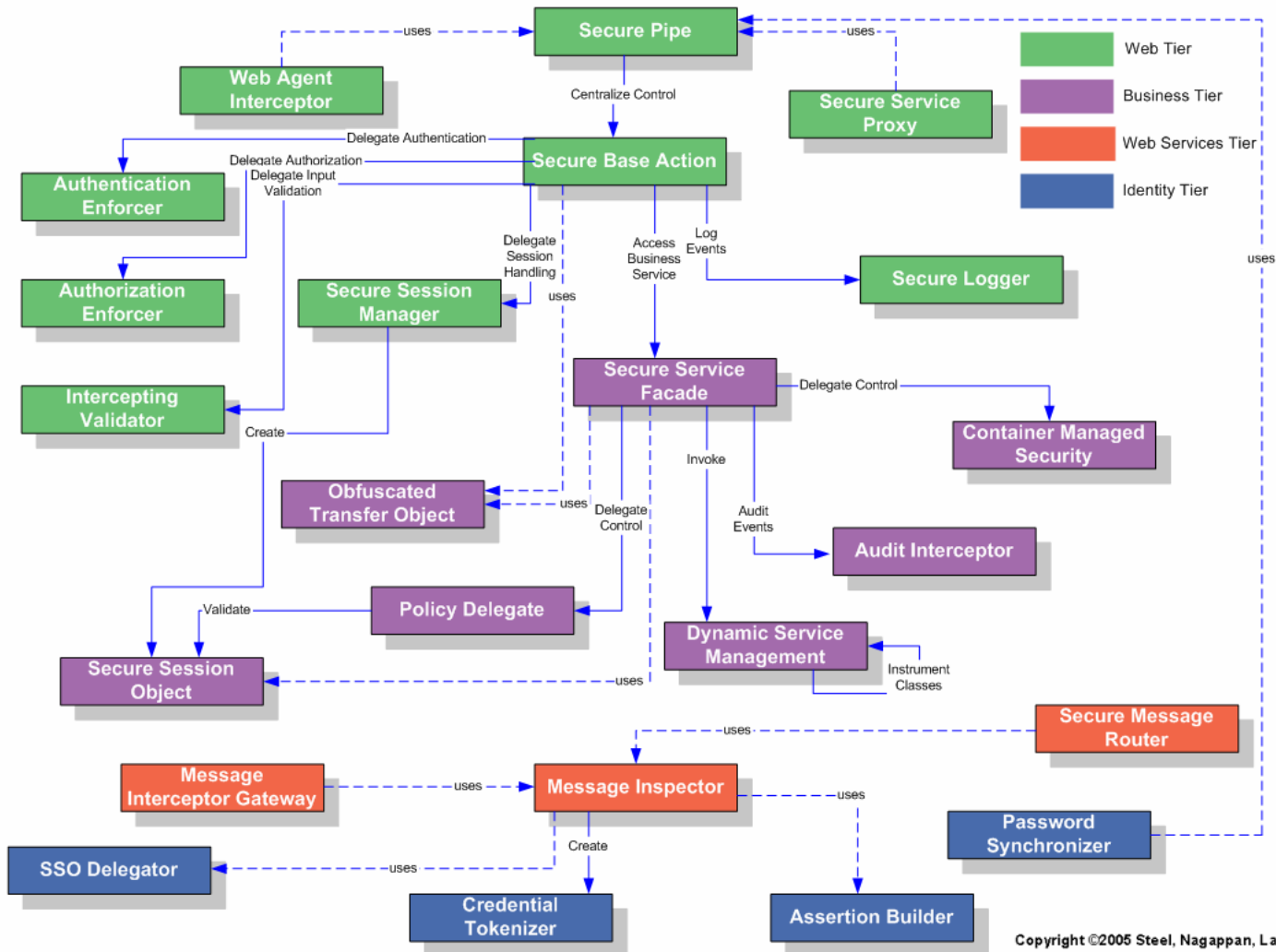
- Security Requirements
- Security Architecture
- Security Design
- Security Implementation
- White Box Testing
- Black Box Testing
- Monitoring
- Security Audits



Secure UP Workflow



Patterns Catalog



Copyright ©2005 Steel, Nagappan, Lai



Pattern Format

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



Questions

