ESTABLISHING ENTERPRISE SECURITY AND RISK MANAGEMENT PROGRAM IN AN AGILE SOFTWARE DEVELOPMENT ORGANIZATION

Houston Java User Group
Srini Penchikala (srinipenchikala@gmail.com / @srinip)
01.25.12
GOALS AND SCOPE

Goal
- How to establish Security Arch. & Risk Mgmt Program in Agile development context

Scope
- Less focus on software development (coding)
- Focus on the four pillars of enterprise business and security architecture
  - People, Process, Information and Technology

Target Audience
- Architects:
  - Application, Solution, Security
- Security/Risk Managers
- Product/Process Managers

Format
- ~60 min presentation + 10 min Q&A
- Interactive
- Case Study
Location: Austin, TX
Current Focus: Security Architecture Program Mgmt
Past: Application Architecture, Project Management
Certified Scrum Master, TOGAF 9 Certified Architect
Co-Author: “Spring Roo in Action” Book
Editor (InfoQ.com)
Areas of Interest: Agile and Lean Architectures, Role of Leadership in Organizational Agility
WHO ARE YOU

- Developers, Technical Leads, Architects
- Product Owners / Project Managers
- Business / System / Process Analysts
- QA / Testing Engineers
- Security or Risk Managers, Auditors
- Other
HOW ARE YOU - 2

- How many are currently using Agile or Lean methodologies in their organizations?
- Working in a Financial Services organization?
- Regulatory compliance requirements
  + Federal, State, Local
  + Health Care
  + Finance
BACKGROUND

- Financial services
- Agile software development (Scrum)
- Regulatory compliance and its impact on IT
- J2EE security model
- Software architecture
AGENDA

- Part 1: Architecture Changes
- Part 2: Process Changes
- Part 3: Organizational Changes
- Part 4: What’s Next
AGENDA

- Security Architecture Program
- Strategy and Framework
- Architecture Process Lifecycle
- Security Risk Assessments
- Center of Excellence
- Architecture Engagements
- Training and Awareness
- Lessons Learned
- Conclusions
PART 1: ARCHITECTURE CHANGES
AGENDA

- Security Architecture Program
- Strategy and Framework
- Architecture Process Lifecycle
- Security Risk Assessments
- Center of Excellence
- Architecture Engagements
- Training and Awareness
- Lessons Learned
- Conclusions
PROGRAM

- **Goals:**
  - Security & Risk Management at Enterprise level
  - Build Security In
  - Sustainable Compliance

- Risk based Security Architecture Strategy
- Architecture Framework
- Process
**ORGANIZATIONAL AGILITY**

- **Vertical:**
  - Strategy
  - Portfolio
  - Project
  - Release
  - Iteration/Sprint
  - Daily Sprints

- **Horizontal:**
  - Process
  - People
  - Tools/Technologies
**ORGANIZATIONAL AGILITY - 2**

- **Vertical:**
  - Strategy (3 years)
  - Portfolio (1 year)
  - Project (3-9 months)
  - Release (major: quarterly; other: monthly)
  - Iteration/Sprint (3 weeks)
  - Daily Sprints

- **Horizontal:**
  - Process (Policies, Procedures, Standards, Governance, Architecture Enforcement Framework)
  - People (Roles & Responsibilities, CoE Teams, Training & Awareness)
  - Tools/Technologies
SECURITY ARCHITECTURE PROGRAM

Strategy
- Communication Plan / Metrics
  - Stakeholder Matrix
  - CoE Team
- Framework
  - Disciplines
  - Components
  - Activities
- Process
- Initiatives / Engagements
  - Projects
  - R&D
AGENDA

- Security Architecture Program
- Strategy and Framework
- Architecture Process Lifecycle
- Security Risk Assessments
- Center of Excellence
- Architecture Engagements
- Training and Awareness
- Lessons Learned
- Conclusions
FRAMEWORK

- Defines “Structure” and “Lifecycle” of the Architecture Strategy
- **Structure**: Framework Components
- **Lifecycle**: Process Activities
- Components’ mapping with Process Activities
- **Structure:**
  - Disciplines
  - Components
  - Activities
REFERENCE FRAMEWORKS

NIST 800-53  
FISMA  
TOGAF 9  
Microsoft Secure Development Lifecycle (SDL)

BSIMM  
SAFECode  
OWASP Standards
DISCIPLINES

- Security Assessment & Authorization
- Security Architecture & Design
- Identity and Access Management (IAM)
- System & Information Integrity
- Systems & Communications Protection
- SIEM
- Technologies & Tools
- Governance
COMPONENTS

Security Assessment & Authorization
- Risk Assessment
- Regulatory Compliance

Architecture and Design
- Threat Modeling
- Reference Architecture and RI
- Model Driven Security

Identity and Access Management
- Identification and Authentication
- Access Control
- ESSO

System & Information Integrity
- Data Security
- Encryption
- Application Security

Systems & Communication Protection
- Message Security

Governance
- Standards and Best Practices
- Reviews (Arch, Design and Code)
- R&D
Standards at all levels of product development
- Architecture
- Design & Coding (based on OWASP Standards)
- Technologies & Tools

Standards Enforcement
- Automatic scans
- Manual Reviews

Lifecycle:
- Identify exceptions/waivers at beginning of project
- Continuous feedback to refine standards (via Agile retrospectives)
PART 2: PROCESS CHANGES
AGENDA

- Security Architecture Program
- Strategy and Framework
- Architecture Process Lifecycle
- Security Risk Assessments
- Center of Excellence
- Architecture Engagements
- Training and Awareness
- Lessons Learned
- Conclusions
Integrate security risk assessment and management into all phases of product development

Security touch-points with PMLC & SDLC processes

Reviews to ensure architecture compliance

Reviews v. Sign-offs
PRODUCT LIFECYCLE (PMLC)
AGENDA

- Security Architecture Program
- Strategy and Framework
- Architecture Process Lifecycle
- Security Risk Assessments
- Center of Excellence
- Architecture Engagements
- Training and Awareness
- Lessons Learned
- Conclusions
PRODUCT INITIATION

- Preliminary Risk Assessment
Product/Project information
Protected data including NPI or PII
Application recovery classification
Third party acquisition
External users
External hosting (Cloud)
Mobile interface
ARCHITECTURE

- Security Architecture Assessment
Product/Project information
Related framework components
Security controls
Network/System architecture overview
Information/Data Security
Identity and Access Management
Segregation of Duties Analysis
Auditing and Logging
SECURITY REQUIREMENTS

- Non-functional requirements
- Based on OWASP Secure Coding Practices
- Categories:
  - Authentication
  - Authorization (access control)
  - Session management
  - Input validation
  - Cryptography
  - Data Protection
  - HTTP Security
- Product specific security requirements
DESIGN AND DEVELOPMENT

- Architecture validation
- Automated (part of CI process)
- Aspect-oriented programming (AOP) based custom framework
- Compile time & execution time architecture standards enforcement
ARCHITECTURE ENFORCEMENT DEMO

- Factory Object Pattern
- Boundary Enforcement
- Strategy Injection
- Validator Injection
TOOLS

- AspectJ, Eclipse, AJDT
- Spring AOP
- Custom AOP Based Architecture Enforcement Framework
- Sonar
- Hudson
- Fortify, QAInspect
- OWASP LAPSE+
- OWASP Web Testing Environment (WTE) Project
- Metasploit
PART 3: ORGANIZATIONAL CHANGES
AGENDA

- Security Architecture Program
- Strategy and Framework
- Architecture Process Lifecycle
- Security Risk Assessments
- Center of Excellence
- Architecture Engagements
- Training and Awareness
- Lessons Learned
- Conclusions
Center of Excellence Team

- Cross-team Security Architecture and Risk Management group
- Champion the management and governance of all aspects of security architecture program
- Core and Extended Teams
TEAM STRUCTURE

- Enterprise Security
- Business Units / Operations
- Product Management
- Enterprise Architecture
- Applications and Systems Development
- Enterprise Technology Services
- Internal Audit
COE ACTIVITIES

- Risk Assessments
- Security Architecture and Design Consulting
- Communicate architecture decisions & guidelines to project teams
- Review & present security architecture related proposals to ARB
- Escalate critical security issues
- Awareness & Education (via Newsletters, Wiki, Brown Bag sessions)
- Security Training
- Security Reviews (Architecture, Design, and Development)
- Threat Modeling (Future)
- Guidance on Code Scans, Pre-deployment Scans & Penetration Testing
- Assist in product development and product acquisition
AGENDA

- Security Architecture Program
- Strategy and Framework
- Architecture Process Lifecycle
- Security Risk Assessments
- Center of Excellence
- Architecture Engagements
- Training and Awareness
- Lessons Learned
- Conclusions
ENGAGEMENTS

- Collaboration between team members
- Communication at the right places in the process
- Security requirements & test cases during Sprint Planning
- Security architecture walk-throughs
- Architecture retrospectives (end of sprint)
- Projects, Initiatives, Ad-Hoc Consulting
- Governance Model
- Research Labs (for R&D)
Security Architecture Program
Strategy and Framework
Architecture Process Lifecycle
Security Risk Assessments
Center of Excellence
Architecture Engagements
Training and Awareness
Lessons Learned
Conclusions
TRAINING AND AWARENESS

- Education focused - Learning v. Teaching
- Stakeholder specific
  - Business Analyst, Product / Project Manager
  - QA Testing Engineer
  - Technical Lead, Developer
  - DBA, Network Admin
- Topic/Module Specific
  - Requirements Management
  - Testing and Validation
  - Development: User Interface, Services, Data, SQL Injection, XSS
- Internal & External; Online & Classroom based
TRAINING PROCESS LIFECYCLE

- On-going
- Identify training needs at the start of the project
- Feedback mechanism within each project (via Retrospectives)
PART 3: WHAT’S NEXT
AGENDA

- Security Architecture Program
- Strategy and Framework
- Architecture Process Lifecycle
- Security Risk Assessments
- Center of Excellence
- Architecture Engagements
- Training and Awareness
- Lessons Learned
- Conclusions
LESSONS LEARNED

- Manual architecture, design and code reviews
  - Solution: Automated Static & Dynamic Code Analysis Tool

- Skill set challenges
  - Solution: Enhancements to training program

- Assessments overhead
  - Solution: Refinements based on project experience
ROADMAP

- Current State: 2+ yrs since the start (3 yrs effort at the previous organization)
- Threat Modeling (Agile Version)
- Security & risk management aspects in:
  + Social Computing*
  + Mobile Development*
  + Cloud Computing
  + NoSQL Databases

*Strategy development is in progress in FY12
AGENDA

- Security Architecture Program
- Strategy and Framework
- Architecture Process Lifecycle
- Security Risk Assessments
- Center of Excellence
- Architecture Engagements
- Training and Awareness
- Lessons Learned
- Conclusions
CONCLUSIONS

- Get commitment from Senior Mgmt. team
- Get involved in the strategic planning process
- Process and Standards are critical
- Automate the process as much as possible
- Agile governance model
- Community of best practices (CoE)
- “Agile or Security” v. “Agile and Security”
- “One Size Fits All” fits nothing
RESOURCES

- TOGAF
- SABSA
- The Building Security In Maturity Model (BSIMM) ([http://bsimm.com](http://bsimm.com))
- Software Security: Building Security In by Gary McGraw
- Secure Programming with Static Analysis by Brian Chess and Jacob West
- Security Metrics ([http://www.securitymetrics.org/content/Wiki.jsp](http://www.securitymetrics.org/content/Wiki.jsp))
RESOURCES - 2

- AspectJ (http://www.eclipse.org/aspectj/)
- Eclipse (http://www.eclipse.org)
- Maven (http://maven.apache.org/)
- Spring AOP (http://static.springsource.org/spring/docs/3.1.x/spring-framework-reference/html/aop.html)
THANK YOU

- Contact Information
  - http://www.infoq.com/author/Srini-Penchikala
  - srinipenchikala@gmail.com
  - @srinip

- Spring Roo in Action Book

- Questions?