SOFTWARE SECURITY ASSURANCE SUMMIT

December 1, 2010 | Westin Tysons Corner | Falls Church, VA

T.E.N. presented by FORTIFY An HP Company

Understanding Software Security

In Support of Federal Compliance

Pravir Chandra – *Director of Strategic Services, Fortify (an HP Company)*

Alexander Fry – *Software Security Consultant, Strong Crypto LLC*

Is this Software Security?

- FISMA
- NIST 800-53
- NIST 800-53A
- NIST 800-37
- NIST 800-64
- NIST 800-115
- DISA STIG Application Security
- DoDI 8510.01 (DIACAP)
- HSPD-7
- HPSD-12
- ICD 503
- Appendix III to OMB Circular No. A-130

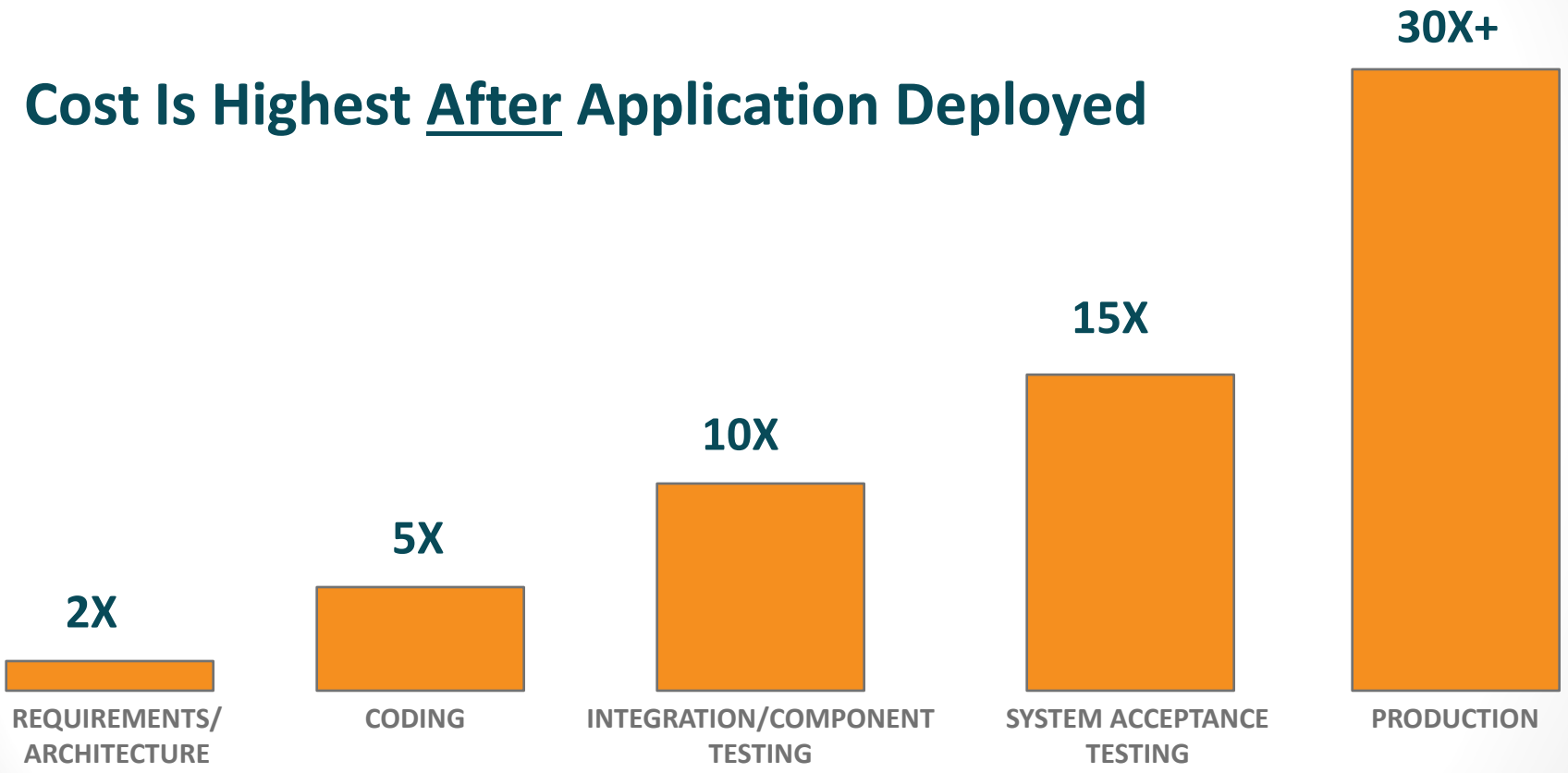
Software Security Assurance

- ***Software*** – the code that we develop, buy, or get for free
- ***Security*** – being free of dangers, threats, or vulnerabilities
- ***Assurance*** – positive declaration of justified confidence

Cost of fixing vulnerabilities

Code Fixes After Release = 30X Fixes During Design

Cost Is Highest After Application Deployed



Source: NIST

Foundation for an SSA Program

Critical SSA Practices

Governance

- Strategy & Metrics
- Policy & Compliance
- Education & Guidance

Construction

- Security Requirements
- Threat Assessment
- Secure Architecture

Verification

- Design Review
- Code Review
- Security Testing

Deployment

- Vulnerability Management
- Environment Hardening
- Operational Enablement

Forging an SSA Program

- ***Given:***
  - Federal regulations are splintered when it comes to software security
  - A complete SSA Program should account for all 12 key security practices
- ***Therefore:***
  - Formulate a set of controls (detective and preventative) for your organization
  - Map these controls back to regulations (where they exist) for compliance auditing
  - Implement the controls in your organization
  - Assess and monitor the controls continuously (and tune them as needed)

SSA Quick Wins & Challenges

Governance

Education & Guidance

EG 1

- Educate ALL programmers
- Leverage HR for on-ramping of employees
- Budget time to bring legacy employees up to speed
- Develop project-specific guidance, e.g., How-Tos
- OWASP Top Ten 2010
- OWASP Development Guide

Construction

Threat Assessment

TA 1

TA 3

- Create at least one threat modeling diagram, e.g., data flow diagram
- Construct abuse cases
- Identify risk from third-party frameworks, e.g., consult the Fortify Open Review Project
  - https://opensource.fortify.com
- OWASP Application Threat Modeling

Construction

Secure Architecture

SA 1

SA 3

- Identify Security Design Patterns for the project
- Build list of recommended software frameworks
- Don’t create secure components from scratch
- OWASP Secure Coding Practices – Quick Reference Guide
- The CSSLP Prep Guide

Construction

Security Requirements

SR 1

SR 3

- Identify how common security tasks will be accomplished
- Integrate into the IDE and automate
- Identify and mitigate common weaknesses in chosen programming languages
- Specify requirements for protecting data at rest and in transit
- OWASP Enterprise Security API (ESAPI) Project
- OWASP Legal Project

- Provide specific remediation advice !
- Use automation to inform manual review
- Delegate different tasks to different roles
- OWASP Code Review Guide

Verification

Security Testing

ST 1

- Provide specific remediation advice !
- Perform security testing in QA
- Correlate black box and white box results
- Use automation to inform manual testing
- OWASP Testing Guide
- OWASP Application Security Verification Standard

Deployment

Environment Hardening

EH 1

- Follow secure configuration guidelines, e.g., CIS, DISA, NIST, OWASP for Web Server, Web Application Server, and Database Server
- Automate hardening process using recommended tools
- Establish secure baseline and document deviations
- OWASP ModSecurity Core Rule Set

Deployment

Vulnerability Management

VM 1

- Establish process for scanning and reporting on Web architecture
- Establish process for Web-architecture security incidents
- Establish process for inventory and tracking of applications

- OWASP Top Ten 2010
- OWASP Development Guide
- OWASP Secure Coding Practices Checklist
- OWASP Application Threat Modeling
- OWASP Legal Project
- OWASP Enterprise Security API (ESAPI) Project
- OWASP Application Security Verification Standard
- OWASP Code Review Guide
- OWASP Testing Guide
- OWASP ModSecurity Core Rule Set
- Many more … http://www.owasp.org

Challenges

- Money is silo'ed at the program or project level
- Agency-wide activity versus program or project-specific activity
- Every program buys a different tool to do the same job
- The Agency doesn't approach the vendor as a unified entity to get the best licensing terms
- You have tools but few resources trained and dedicated
- Accountability when something goes wrong
- Incentives do not exist; no punishment for bad behavior; no reward for good behavior
- Should the contract organization or the government bear the cost?

Q&A