



O-ISC '07
Ohio Information Security Conference

Oracle Software Security Assurance

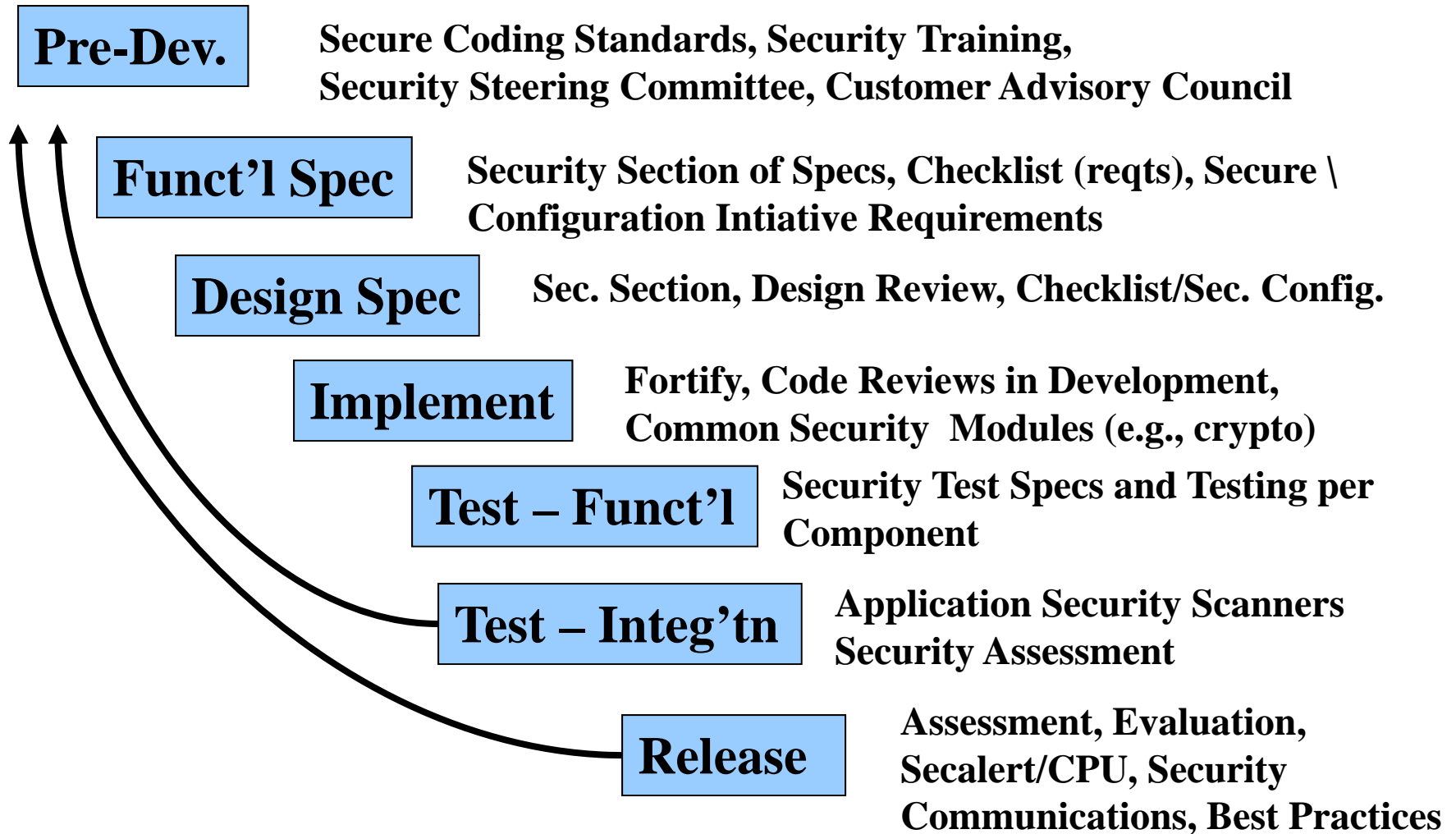
John Heimann
Oracle

Speaker Biography



John Heimann is Director, Security Programs at Oracle, where he is responsible for managing programs to improve the security assurance of Oracle's products. He has worked at Oracle since 1996. Prior to Oracle, Mr. Heimann worked for GTE Government Systems and BBN Communications, doing government funded research and development in applied cryptography, secure networking and distributed Systems. Mr. Heimann has a BA in Physics from Harvard Universit.

Software Security Assurance



Secure Product Definition



- Oracle Secure Coding Standards
 - Complements C and Java coding standards
 - Revised frequently for new hacks
 - Uses Oracle “true stories” as examples
- Oracle Secure Coding Standards Training
 - Web-based, interactive class
 - Mandatory for development, up to VP, including PMs, QA, release management...
 - Status: has been rolled out across ST, Apps in process

Secure Product Definition



- Product Security Steering Committee
 - Security representatives from all development groups
 - Focus on common problems and common solutions
- Customer Advisory Council
 - More than 20 organizations, from banking, manufacturing, pharma, government, education, and all major geographic areas
 - Customers from every product family in Oracle are security CAC members

- Development processes include security requirements through all phases:
 - Functional specs
 - Design specs
 - Test specs
- Additional design reviews for security
- Core, vetted security modules facilitate stronger security
 - Crypto libraries (including database encryption)
 - Identity management (SSO, provisioning, etc.)
 - “Build security once, use many” means developers are not “rolling their own” core security

- Security testing - proactive
 - Regression tests for security modules exercises security features/functions
 - We run full regress for releases and patch sets
- Security testing - destructive
 - In-house tools (e.g., checks for SQL injection, buffer overflows)
 - Licensed static analysis tool from Fortify; is being deployed across Server Technologies
 - Web application vulnerability tool licensed for App Server
 - Oracle can also turn our 250K regression suite into destructive security tests

- Security release checklists
 - All components on bill-of-materials validate against secure coding standards
 - Exceptions are tracked, resolved and deal-breakers stop releases
- Secure configuration
 - Global Product Security initiative focused on “default secure” product delivery across the stack
 - Benchmark under development for 11g, based on Center for internet Security guidelines

- Security Evaluations
 - Third party product validation against standards of 'what you mean when you say you are secure'
 - Evals vet specific security functionality and the development processes used to build them
 - Core evaluations standards
 - International Common Criteria (ISO 15408)
 - US Federal Information Processing Standard-140
 - Database has most evals (19), but we evaluate other products, as well (App Server – 1, OID –1)
 - Evals are required by some customers for some implementations (NSTISSP #11)

- Product Assessments
 - Core group of ethical hackers in Global Product Security
 - Focus is on new/critical modules
 - Knowledge transfer (coding standards...)
 - Augmented by use of external hacking firms (e.g., Pentest, Ltd.)
- Security best practices guides
 - Multiple, typically part of the doc set and/or on OTN or Metalink

- Security Configuration Management and Validation Tools (Oracle Enterprise Manager Grid Control)
 - Validate / customize secure configurations
 - Build from over 200 product specific security configuration issues
 - OEM also can determine whether critical security patches are missing
 - Provides security reports and security dashboard
 - Policy violations can trigger email or pager to admin

Critical Patch Updates



- Bigger than one-offs; smaller than patch sets
- Updates contain new security fixes and...
 - pre-requisite fixes required by security fixes
 - merged fixes that would conflict with security fixes
 - fixes required by E-Business Suite, SAP, PeopleSoft and JD Edwards
 - previous Security Alerts and CPUs

Cumulative Patches

- Patches are cumulative for Database, Application Server, Enterprise Manager, Collaboration Suite, PeopleSoft and JD Edwards
- eBusiness Suite patches are not cumulative, but some are bundled
 - A tool to bundle patches is available for download

CPU Release Dates



- Tuesday closest to the 15th of January, April, July and October
- In 2007:
 - 16 January 2007
 - 17 April 2007
 - 17 July 2007
 - 16 October 2007

CPU schedule was designed with customer input in order to avoid typical “black-out” dates when changes to production environment are difficult or impossible.

Current Objectives

- Focus on patch quality
 - Faulty patches may “break” systems
 - Faulty patches may require patch re-application by customers
- Enhance security in default configuration
 - “Secure Configuration Initiative”
 - Limit number of services enabled by default
 - Limit number of default accounts/passwords
 - Implement “least privilege principle”
- Simplify patch application
 - JDEdwards now on CPU system
 - “Default Password Scanner”
 - Enhancement to CPU documentation

Default Password Scanner



- Released as part of CPUApr2006
- Checks for unlocked default database accounts with default passwords

- Adoption of Common Vulnerability Scoring Standard (CVSS) –10/06
 - Provides customers with standardized way to evaluate risk associated with vulnerabilities
- Specific Identification Of Most Critical Vulnerabilities - “Remotely Exploitable Without Authentication” – 10/06
- Executive Summary – 1/07
 - Plain English
 - Available shortly before the CPU release date

We are validating proposed changes to CPU documentation with our customers council to make sure that enhanced information does not result in more confusion.

Ongoing Assurance



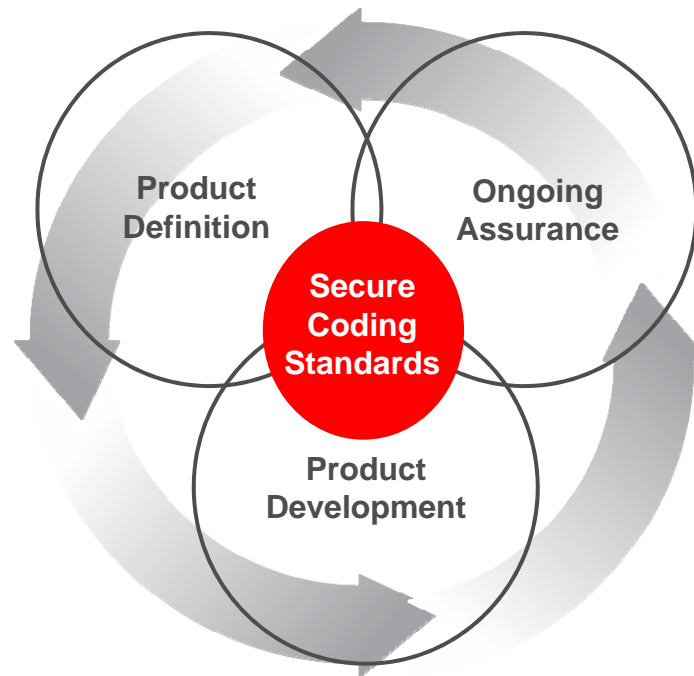
- Customer Communications
 - Proactive response to customer security concerns
 - Respond within days or hours
 - Addresses problems not covered by CPU
 - Problems completely fixable by customer
 - Configuration security problems
 - Response mechanisms
 - eBlast email to all customers (most serious issues)
 - External posting on Metalink and Oracle.com/security
 - Internal posting (sales, consulting, support)
 - Security Blogs

Oracle Software Security Assurance



O-ISC '07
Ohio Information Security Conference

- Security Steering Committee Review
- Customer Advisory Council Feedback
- Secure Coding Standards
- Developer Training



- Security Evaluation
- Security Assessment
- Best Practices
- Configuration Mgt/Validation
- Critical Patch Updates
- Customer Communications

- Common Security Modules
- Design Review
- Security Testing Tools
- Secure Configuration



Questions & Answers



O-ISC '07
Ohio Information Security Conference