
JavaOne™

JavaOne™

Making the Future Secure with Java

Milton Smith
Sr. Principal Security PM

Email: milton.smith@oracle.com
Twitter: @spoofzu

MAKE THE FUTURE JAVA

ORACLE

Notice

"THE FOLLOWING IS INTENDED TO OUTLINE OUR GENERAL PRODUCT DIRECTION. IT IS INTENDED FOR INFORMATION PURPOSES ONLY, AND MAY NOT BE INCORPORATED INTO ANY CONTRACT. IT IS NOT A COMMITMENT TO DELIVER ANY MATERIAL, CODE, OR FUNCTIONALITY, AND SHOULD NOT BE RELIED UPON IN MAKING PURCHASING DECISION. THE DEVELOPMENT, RELEASE, AND TIMING OF ANY FEATURES OR FUNCTIONALITY DESCRIBED FOR ORACLE'S PRODUCTS REMAINS AT THE SOLE DISCRETION OF ORACLE."

JavaOne™ ORACLE®

Who Am I?

Milton Smith

- Responsible for Java platform security: vision/features, internal/ external communications – everything Java except EE.
- 20+ years of programming and specializing in security.
- Recently joined Oracle. My last employer was Yahoo! where I managed security for the User Data Analytics group.

JavaOne™ ORACLE®

Program Agenda

- Security Industry Challenges
- Risk Choices & Methodologies
- Security at Oracle
- Ongoing Security Improvements
- Call to Action

JavaOne™ ORACLE®

Security Industry & Challenges

JavaOne™ ORACLE®

Level of Security Challenge -- Java Ecosystem

- 97 percent of enterprise desktops run Java
- 1 billion Java downloads each year
- 9 million developers worldwide
- More than 3 billion devices are powered by Java technology

JavaOne™ ORACLE®

Security Threat Landscape

A lot has changed since 1995 when Java started…

- *What we saw in the past…*
  - Data Destruction – Format Drive
  - Denial of Service – Computer Lockout
  - Hacktivism – Computer attacks to accomplish an agenda (e.g., defacement)

JavaOne™ ORACLE®

Security Threat Landscape

The landscape has changed…

- *What we see today…*
  - WORMS and Bot Nets
  - State or Terrorist Sponsored Cyber Warfare – Stuxnet
  - Intellectual Property Theft -- Fuzzy Offshore Borders
  - Virtual Currency Manipulation – MMORPGs like World of Warcraft, Bitcoin

- This is the world we live in today…

JavaOne™ ORACLE®

Strong Security is the Expectation…

Challenges across entire industry…

- Security concerns across industry are elevated
- Strong vs. poor security is difficult for users to evaluate

JavaOne™ ORACLE®

Risk Choices & Methodologies

JavaOne™ ORACLE®

Risk vs. Reward

WE MAKE CHOICES BASED UPON RISK EVERY DAY.

THIS IS HOW HUMANS FUNCTION.

JavaOne™ ORACLE®

Everyday Risk Choices

Do animals drink at the water hole? Animals with big teeth may be present.

- Answer = Depends, how thirsty.

Everyday Risk Choices

Everyone treated by a doctor – has or will die. Success rate is precisely zero. Do we continue to visit doctors?

- Answer = Yes!

JavaOne™ ORACLE®

Everyday Risk Choices

Life is risky. Do we visit the doctor every day for a check-up?

- Answer = No!

Risk Based Security Methodology

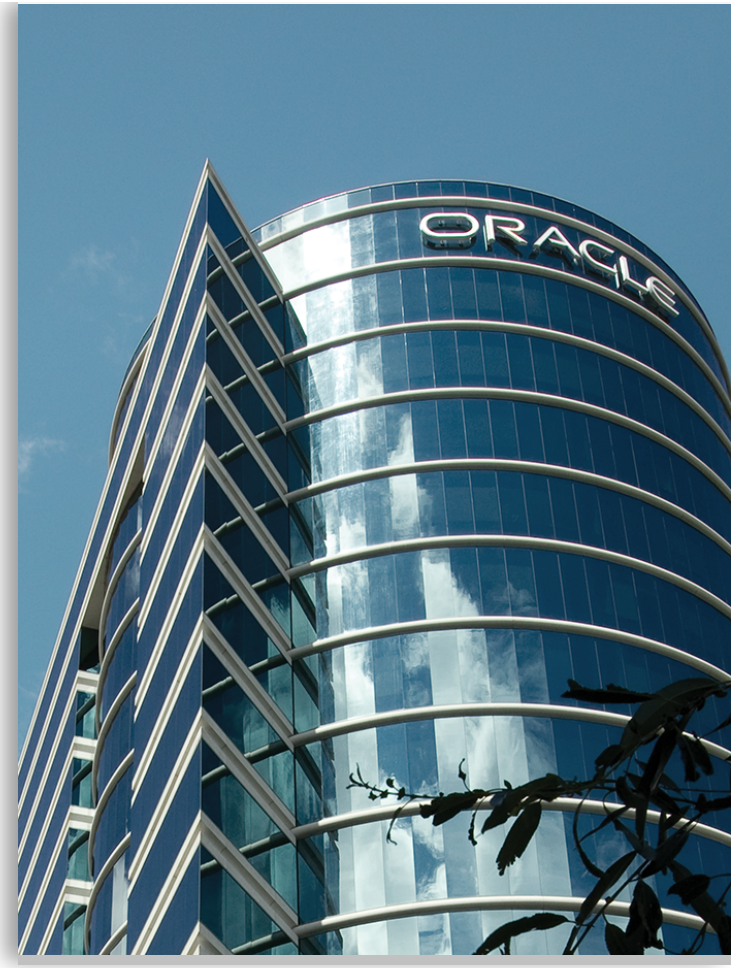
- Many of us today use informal risk based approaches.
- Some don't take the next steps – formalize thoughts about risk and how it governs our behavior.
- Risk methodology helps drive security decisions

Security Risk Applied to a Web Application Example

- A few simple considerations…
  - How important is the application to the business? Dollar loss, compliance requirements, inconvenience?
  - Internet facing application interfaces (web, web data services)?
  - Any unauthenticated application interfaces (no logon)?
  - and many more factors…
- Platforms have different concerns but the approach is similar

JavaOne™ ORACLE®

Security at Oracle



JavaOne™ ORACLE®

Why is Security Important to Oracle?

- Oracle products are built upon Java technology
  …just like your products
- Oracle product teams demand strong security
  …just like you
- Confidentiality, Integrity, and Availability is important to the Java ecosystem

JavaOne™ ORACLE®

Security Policies - Communications

- Security news & alerts are communicated via several channels
  - Security Alerts (RSS feed)
  - Critical Patch Update Advisories
  - eBlasts
  - Blogs (like blogs.oracle.com/security)

- Policy: http://www.oracle.com/us/support/assurance/fixing-policies/index.html

JavaOne™ ORACLE®

Security Policies - Communications

Why we don't respond to published reports of alleged security vulnerabilities in Oracle products…

- Correcting and corroborating articles provides more information to attackers
- Many reports don't provide the required engineering details for proper verification. Technical details like: pre-conditions, impacts, remediation/ mitigation details are light or non-existent.
- Responding to individual reports forces communities to track vulnerabilities in social media sites – not good.

JavaOne™ ORACLE®

Security Policies - Communications

Why we don't respond to published reports of alleged security vulnerabilities in Oracle products…

- The information Oracle releases is: precise, actionable, and everyone receives it at the same time.

- Policy: http://www.oracle.com/us/support/assurance/disclosure-policies/index.html

JavaOne™ ORACLE®

Security Throughout Development Cycle

Concept/ Requirements	Analysis/ Design	Coding
Early Security Influence High Risk? • Yes = intensive review • No = light review	Security Design Review Sec Policy Compliance?	• Peer Review • Manual Assessment

JavaOne™ ORACLE®

Security Throughout Development Cycle

Testing	Delivery
Review Test Cases/ Testing Static Analysis Fuzzing	Java.com

Outside of Development Cycle

- GPS
- Ethical Hacking
- Security Training
- Tech Talks

…and more.

Policy: http://www.oracle.com/us/support/assurance/development/index.html

JavaOne™ ORACLE®

Security Policies - Remediation

- Common Vulnerability Scoring System (CVSS)
- Vulnerabilities reviewed and CVSS score assigned
- Remediation strongly influenced by CVSS score

Policy: http://www.oracle.com/us/support/assurance/fixing-policies/index.html#scoring

JavaOne™ ORACLE®

Security Policies - Remediation

- Critical Patch Updates (CPU) - Security patches
  - October, February, June for Java Platform Group
  - Java Platform Group Different from Oracle CPU
  - Emergency releases are rare but do happen

- Policy: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

JavaOne™ ORACLE®

Java CPU

Planned

7 GA	7u1 CPU	7u2 Non CPU	7u3 CPU	7u4 Non CPU	7u5 CPU	7u6 Non CPU	7u7 SecAlert*	7u9 CPU

Every 4 months

Rules for Java CPUs

- Main release for security vulnerabilities
- Covers all families (7, 6, 5.0, 1.4.2)
- CPU release triggers Auto-update
- Dates published 12 months in advance
- Security Alerts are released as necessary
- Based off the previous (non-CPU) release
- Released simultaneously on java.com and OTN

JavaOne™ ORACLE

Securing Platforms vs. Securing Applications

- Different tools for securing platforms and applications
  - Platform development often precedes tool features
- Platforms support a wider range of use cases
- Different techniques for securing platforms and applications

JavaOne™ ORACLE®

Ongoing Security Improvements

JavaOne™ ORACLE®

Theme, Preventing Drive-By Exploitation

- Defense against phishing attacks
- “Best used before” date for JRE security
  - Largest number of exploits are against out-of-date software

JavaOne™ ORACLE®

Theme, Preventing Drive-By Exploitation

- Easier to disable Java in Browser (Applet/JNLP)
- Encourage users to uninstall older JREs
  - First step, as an applet
  - Next step, component of the installer

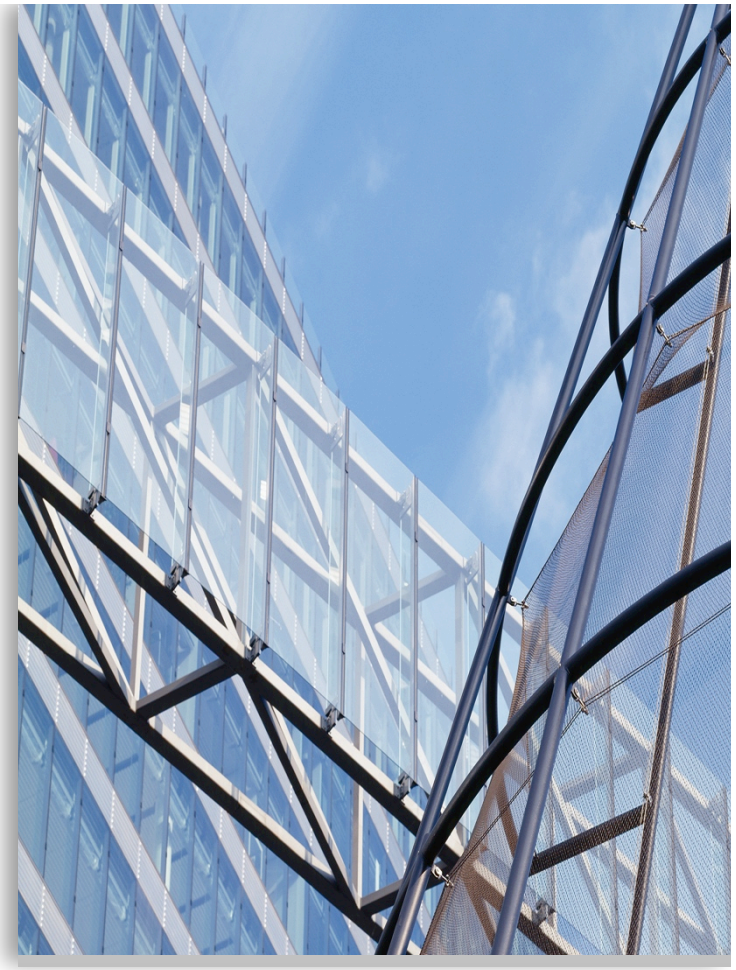
JavaOne™ ORACLE®

Theme, JRE Security Hardening

- Configurable IT security policy
- More frequent security feeds (blacklists, security baseline updates)

JavaOne™ ORACLE®

Call to Action



JavaOne™ ORACLE®

Vulnerability Reporting & Security Feature Suggestions

- Report Vulnerabilities
  - Support Customers: My Oracle Support
  - Others: secalert_us@oracle.com

  Policy:

  http://www.oracle.com/us/support/assurance/reporting/index.html

- Suggest New Features
  - http://bugreport.sun.com/bugreport/

JavaOne™ ORACLE®

Upcoming CPU's

- October 16, 2012 - (7u9, 6u37)
- February 19, 2013 - (7u11, 6u39)
- June 18, 2013 - (7u13, 6u41)

- CPUs
  http://www.oracle.com/technetwork/topics/security/alerts-086861.html

JavaOne™ ORACLE®

Help Us Keep You Secure

- To end users…
  - Keep your JRE's updated (auto-update on)
  - Practice defense-in-depth: virus scanner, firewall
- To developers…
  - Support current JRE's so end users can upgrade
  - Sign your applications (use timestamp)
  - Validate untrusted data (input/output validation)
  - Follow Open Web Application Security Project, https://www.owasp.org/
  - CON4786 - "Secure Coding Guidelines for the Java Programming Language" Wednesday, Oct 3, 3:00 PM - 4:00 PM - Hilton San Francisco - Yosemite A/B/C

JavaOne™ ORACLE®

JavaOne ORACLE


JavaOne™