Making the Future Secure with Java

Milton Smith

Sr. Principal Security PM

Email: milton.smith@oracle.com

Twitter: @spoofzu

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- **Role** – Java platform strategy, vision, features, internal, external communications
- **Background** – 20+ years of programming and specializing in security
- **Former Employer** – Yahoo! Lead security for the User Data Analytics property. Run enterprise triage program.

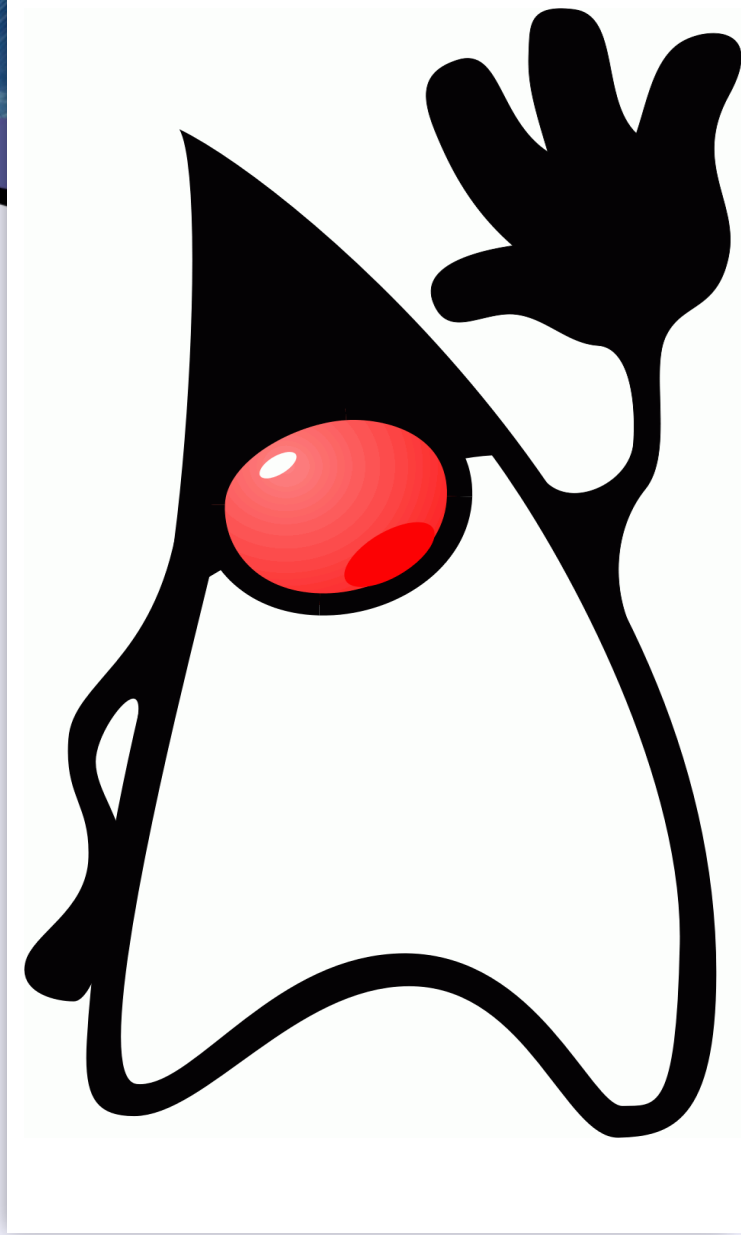
ORACLE®

Program Agenda

- Brief Java Primer
- Security Policies & Program
- Platform Remediation Progress
- Security Features Delivered
- Call to Action

Brief Java Primer

Java is useful in many different ways…



OWASP
The Open Web Application Security Project

What is Java?

An application platform, but what does that mean?

- **Specifications** – Java Community Process (JCP) drives rules defining Java
- **Implementations** – Transforming Java specifications into code like Java.exe, Javac.exe, utility libraries, etc.
- **Community Driven** – OpenJDK to drive open source implementation

Java SE

Java Card

Java FX

Java

Embedded

…and more

OWASP
The Open Web Application Security Project

Where is Java?

The Java ecosystem…

	Facts
Desktops	▪ Java deployed on 97 Percent desktops
Devices	▪ Java deployed on 80 percent of mobile platforms ▪ Java deployed on 125 million television sets
Community	▪ 1 billion Java downloads per year ▪ 9 million developers worldwide

OWASP
The Open Web Application Security Project

How Serious is Java Security?

Security is a top organization priority

Java 8: Secure the train (Apr 18, 2013) – Mark Reinhold, Java Chief Architect

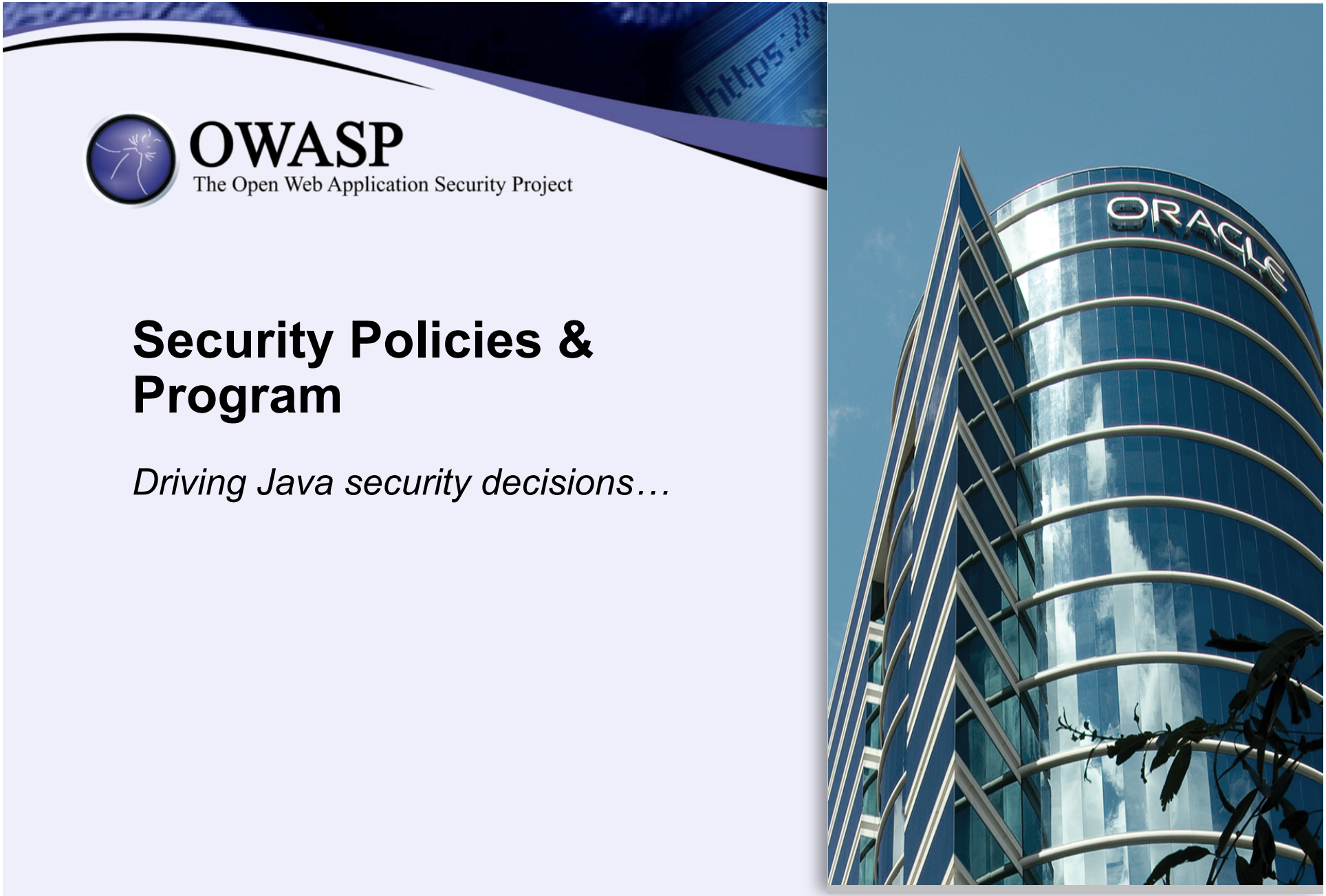
"...As a consequence of this renewed focus on security the Java 8 schedule, with a GA release in early September, is no longer achievable."

OWASP
The Open Web Application Security Project

What is Oracle Doing in Java Security?

Efforts are broad but the message is simple…

- **Defend Java applets** – limit ability of attackers to use malicious applets as a means of attack
- **Accelerate Remediation** – accelerate production of security fixes
- **New Security Features** – new security countermeasures to strengthen Java



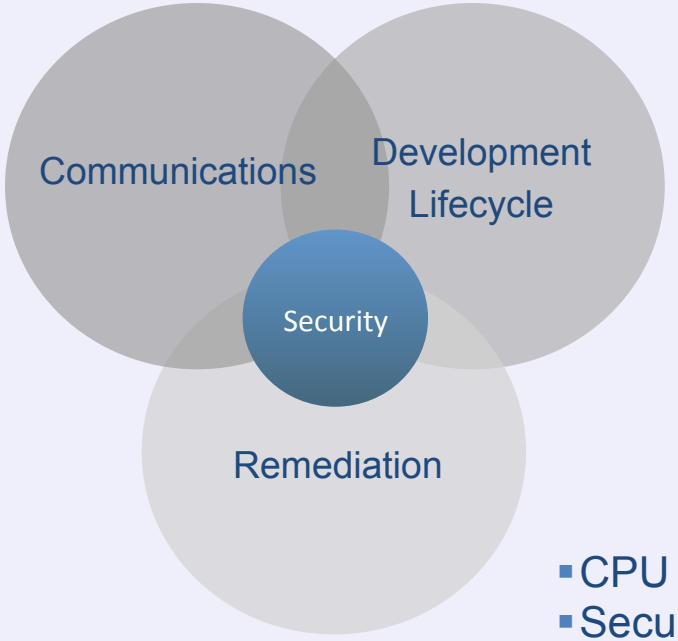
Security Policies & Program

Driving Java security decisions…

Security Policy

Larger areas of security policy at Oracle…

- SA/CPU RSS Feeds
- Security Blog
- eBlasts
- Java.com Security



- Architecture Review
- Peer Review
- Security Testing
- Post Mortems
- Anatomy of an Exploit

- CPU
- Security Alerts

OWASP
The Open Web Application Security Project

Security Policies – Communications

Different modes of security communication…

- Security Alerts (RSS feed)
- Critical Patch Update Advisories
- eBlasts
- Blogs (Security Assurance, Java PM)

OWASP
The Open Web Application Security Project

Security Policies – Communications (cont'd)

Why Oracle does not respond to published reports of alleged product vulnerabilities…

- 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.

OWASP
The Open Web Application Security Project

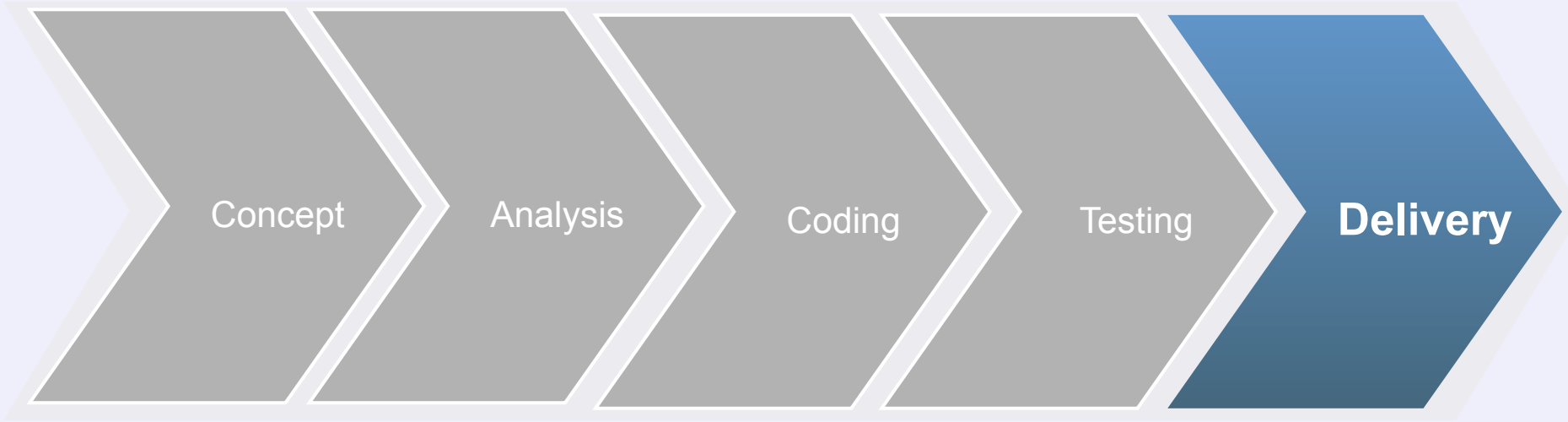
Security Policies – Communications (cont'd)

Why Oracle does not respond to published reports of alleged product vulnerabilities…

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

Security Throughout the Development Lifecycle

Non-specific lifecycle methodology



Risk Factors

- Less Scrutiny
- More Scrutiny

Project Review

- Architecture
- Compliance

Peer Review

- Manual
- Automated

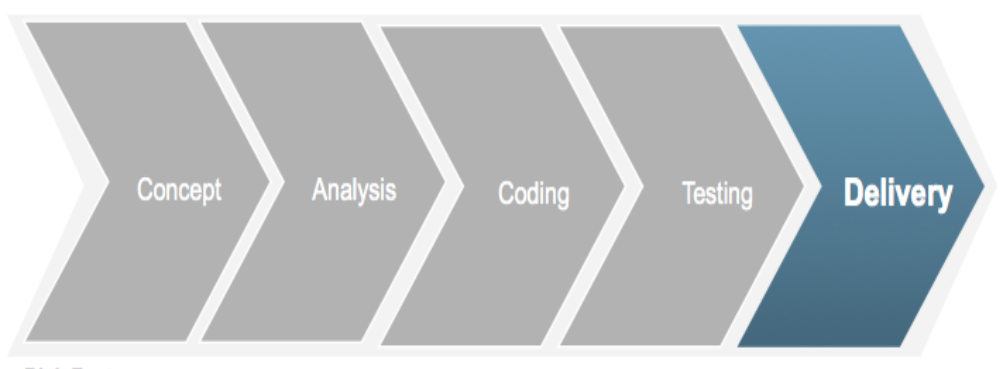
Security Tests

- Static Analysis
- Fuzzing

Java.com

OWASP
The Open Web Application Security Project

Outside the Development Lifecycle



Throughout Development Cycle

- GPS
- Ethical Hacking
- Security Training
- Tech Talks

…and more.

OWASP
The Open Web Application Security Project

Security Policies - Remediation

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

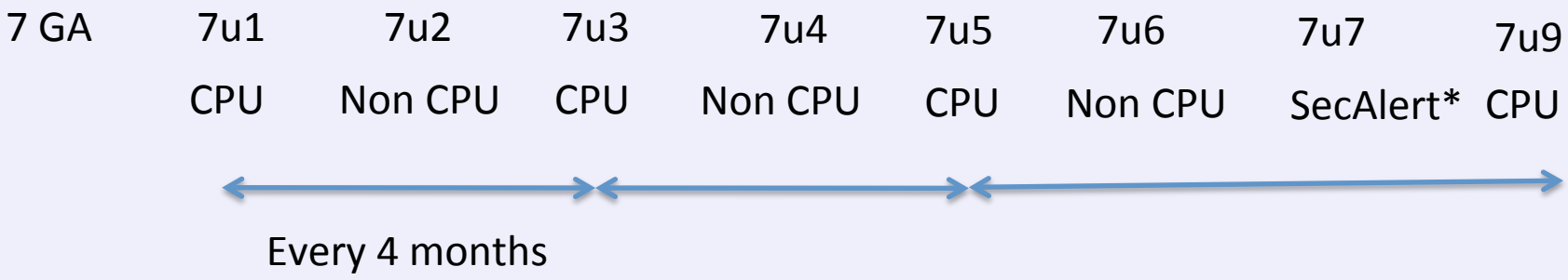
OWASP
The Open Web Application Security Project

Security Policies - Remediation

- Critical Patch Updates (CPU) - Security patches
  - October, February, June for Java Platform Group
  - Java Platform Group Different from Oracle CPU

- Security Alerts (SA) – Emergency security patches
  - Avoid where not absolutely necessary.

Java Critical Patch Updates(CPU)



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 (but there have been changes)
- Security Alerts are released as necessary
- Based off the previous (non-CPU) release
- Released simultaneously on java.com and OTN
- Java moving to regular CPU cycle with other Oracle products, Oct 2013

OWASP
The Open Web Application Security Project

Platform Remediation Progress

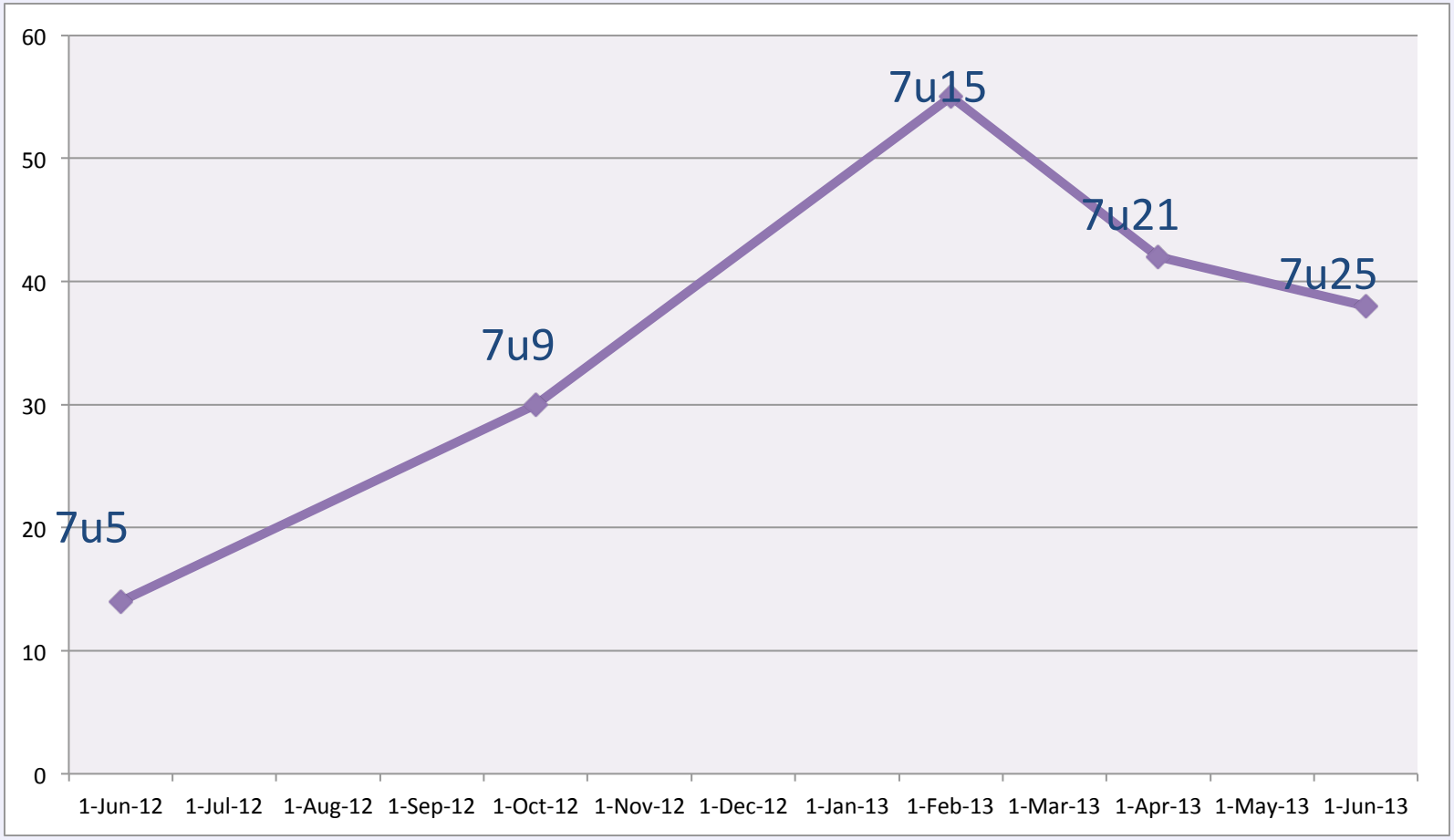
Accelerating progress against backlog…

OWASP
The Open Web Application Security Project

Remediation Highlights

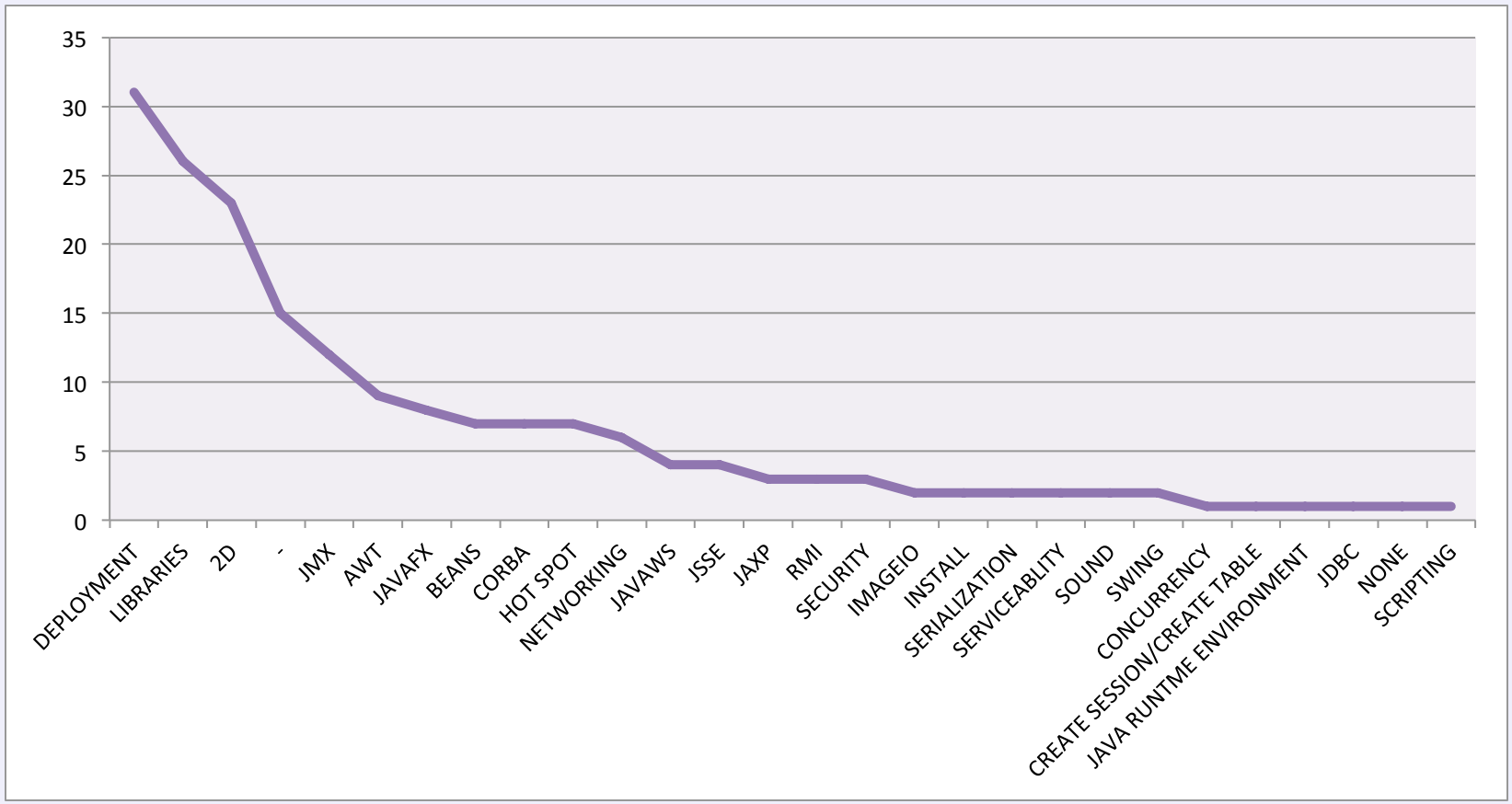
- **Java Applets Running in Browsers** – highest exploitation risk area
- **Other Areas of Java** – figures spotlight applets, we are concerned about all Java use cases, Server for example
- **Progress** – significant over last year

Remediated Vulnerabilities/ Month



OWASP
The Open Web Application Security Project

Remediated Vulnerabilities by Component Subtype



OWASP
The Open Web Application Security Project

Security Features Delivered

Security controls for today's challenges…

OWASP
The Open Web Application Security Project

Security Feature Highlights

Enable/Disable Java (DELIVERED JAVA 7 UPDATE 10)

- Feature within the Java Control Panel to enable or disable Java plugins

Hardcoded Best Before Date on JRE (DELIVERED JAVA 7 UPDATE 10)

- Java changes the way it operates if known to be vulnerable. For example, security dialogs communicate more risk for some activities

OWASP
The Open Web Application Security Project

Security Feature Highlights (cont'd)

Java Security Slider (DELIVERED JAVA 7 UPDATE 10)

- Adjust plugin security levels in accordance with end-user security risk preferences (or policies)

Signing for Sandboxed Applications (DELIVERED JAVA 7 UPDATE 21)

- Changing the security model to separate the notion of establishing identity of the signer and applet privileges. Previously, code-signing also granted applets privileges

OWASP
The Open Web Application Security Project

Security Feature Highlights (cont'd)

Server JRE (DELIVERED JAVA 7 UPDATE 21)

- Standard Java distribution without the plugin support.

Removed "Low" and "Custom" From Security Slider (DELIVERED JAVA 7 UDPATE 21)

- Low and Custom have been removed to reduce risk of desktop exploitation

OWASP
The Open Web Application Security Project

Security Feature Highlights (cont'd)

Dynamic Blacklisting (DELIVERED JAVA 7 UPDATE 21)

- Previously blacklisting was static to the Java release. Blacklisting is now updatable daily. Expanded scope of blacklisting includes: jars, code-signing certificates, and subsidiary CAs.

Lock JARs to Server (DELIVERED JAVA 7 UPDATE 25)

- Prevent applet code from being repurposed

Security Feature Highlights (cont'd)

Standardized Revocation Services (DELIVERED JAVA 7 UPDATE 25)

- Industry standard revocation services like CRL and OCSP are available in Java today.

Java Uninstaller (ONGOING)

- The goal of this effort is to cleanup old versions of Java that are no longer used. Old versions of Java can become a target for exploitation.

OWASP
The Open Web Application Security Project

Security Feature Highlights (cont'd)

Dynamic Rule Set (DRS) (EARLY ACCESS JAVA 7 UPDATE 40)

- DRS constrains enterprise desktop applets to authorized resources based upon system administrator defined policies

OWASP
The Open Web Application Security Project

Call to Action

Something we can all do…

OWASP
The Open Web Application Security Project

Vulnerability Reporting & Security Feature Suggestions

- Report Vulnerabilities
  - Support Customers: My Oracle Support
  - Others: secalert_us@oracle.com
- Suggest New Features
  - http://bugreport.sun.com/bugreport/

OWASP
The Open Web Application Security Project

Java Platform Support

- I provide the following as a service for those interested
- I'm in development, not sales. I do not receive a commission. ;o)

- 3 Options
  - Premier, 5 years from GA
  - Extended, Premier + 3 years
  - Sustaining, "as long as you own your Oracle products"

OWASP
The Open Web Application Security Project

Java Root Certificate Program

- Like web browsers, Java ships with root certificates
- Like web browsers, Java roots establish intrinsic "trust" for Java users
- Of course, the public is always free to include their own certificates or remove our defaults

OWASP
The Open Web Application Security Project

Securing Java

New Track for JavaOne Conference 2013 San Francisco

Challenge – many developers will never have the opportunity to attend a security conference

Answer – bring security education to developers

OWASP
The Open Web Application Security Project

Upcoming CPU's

- October 15, 2013 (transition to Oracle CPU schedule)
- January 14, 2014
- April 15, 2014
- July 15, 2014

OWASP
The Open Web Application Security Project

Help Us Keep You Secure

- To end users…
  - Keep your JRE's updated (auto-update on)
  - Practice defense-in-depth: harden OS, 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)
  - Review OWASP Top-10
  - Follow Secure Coding Guidelines for Java Language

OWASP
The Open Web Application Security Project

Help Us Keep You Secure (cont'd)

- Even more for developers…
  - Educate yourself
  - Attend JavaOne 2013 in San Francisco CA, USA
  - Alternatively review public media after conference concludes

OWASP
The Open Web Application Security Project

Additional References/Links

Security transparency, information available to the public…

- **Java 8: Secure the train** , Mark Reinhold, Java Chief Architect
- **Maintaining Security Worthiness of Java…** , Nandini Ramani, Java Engineering Leader
- **Security Fixing Policies** , Security policies available for public review
- **Oracle Security Vulnerability Disclosure Policies** , Information around vulnerability disclosure
- **Secure Coding Standards** , Security throughout development (SDLC) processes
- **Common Vulnerability Scoring System (CVSS)** , Vulnerability risk management

OWASP
The Open Web Application Security Project

Additional References/Links (cont'd)

Security transparency, information available to the public…

- **Critical Patch Update and Security Alerts**, Oracle's security patch and security hot fixes
- **Reporting Vulnerabilities**, Report vulnerabilities for any Oracle products(including Java)
- **Oracle Lifetime Support Policy**, Public literature on support for Fusion Middleware products (including Java)
- **Including Certificate Authority Root Certificates in Java**, Information around including digital root certificates in Java

OWASP
The Open Web Application Security Project

Additional References/Links (cont'd)

Security transparency, information available to the public…

- **Java Platform Group, Product Management Blog**, News about Java security features and plans
- **Oracle Security Assurance Blog**, News about Java Critical Patch Updates and Security Alerts
- **Secure Coding Guidelines for Java Language**, Secure coding practices for Java language

OWASP
The Open Web Application Security Project

Notice

"THE PRECEDING 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."

OWASP
The Open Web Application Security Project

Questions?