Open Source Software: the Intersection of IP and Security

Greg Kelton, Managing Director EMEA, Palamida Inc.

PALAMIDA™

1995

F22 software (avionics only)
~1.7M LOC

2009

F22 software (avionics only)
~1.7M LOC

"It takes dozens of microprocessors running 100 million lines of code to get a premium car out of the driveway"

(IEEE Spectrum February 2009 Image: General Motors)

New Ways of Composing Services

Cloud Computing … a style of computing in which massively scalable IT-related capabilities are provided "as a service" using Internet technologies to multiple external customers.

Definition: Gartner Group

Smarter Devices

PALAMIDA™

The point is…

More and Better… Software

In... Less Time

And with…

Smaller Budgets

Today's Reality…

A software development organization cannot be competitive without widespread use of open source

Gartner OSS Predictions

- By 2016, OSS will be included in mission-critical software portfolios within 99% of Global 2000 enterprises, up from 75% in 2010.
- By 2014, 50% of Global 2000 organizations will experience technology, cost and security challenges through lack of open-source governance.
- By 2015, OSS will be used and adopted to help enable over 60% of platform-as-a-service (PaaS) services.
- By 2014, 30% of applications running on proprietary versions of Unix will be migrated to OSS-based Linux on x86.
- By 2014, those organizations with effective, open-source community participation will consistently deliver high returns from their open-source investments.
- By 2013, up to 50% of Global 2000 non-IT enterprises will contribute to at least one OSS project.
- By 2016, 50% of leading non-IT organizations will use OSS as a business strategy to gain competitive advantage.

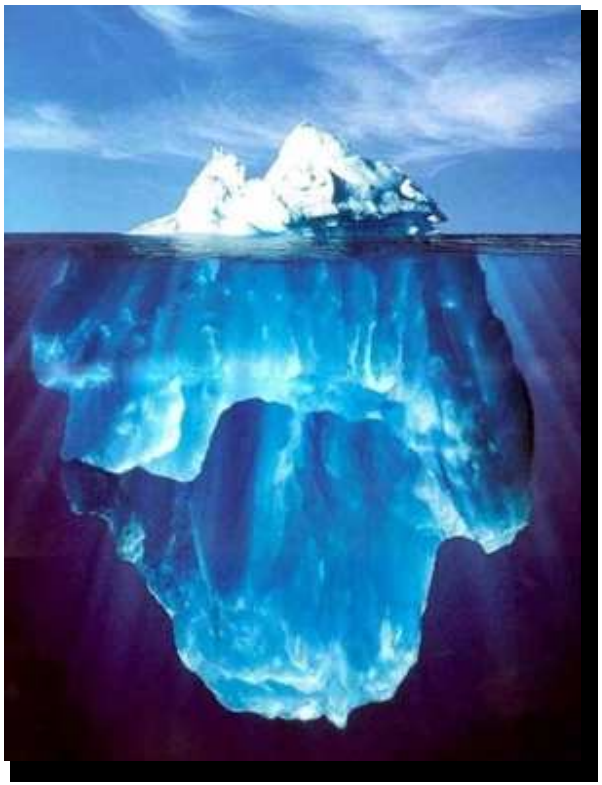
Predicts 2011: Open-Source Software, the Power Behind the Throne
23 November 2010
ID:G00209180

Typical Software Project Metrics

- 2.9 GB
- 87,863 Files
- 8,535,345 LOC
- Copyright holders – ~350
- Binaries/Archives/JARS – 1207

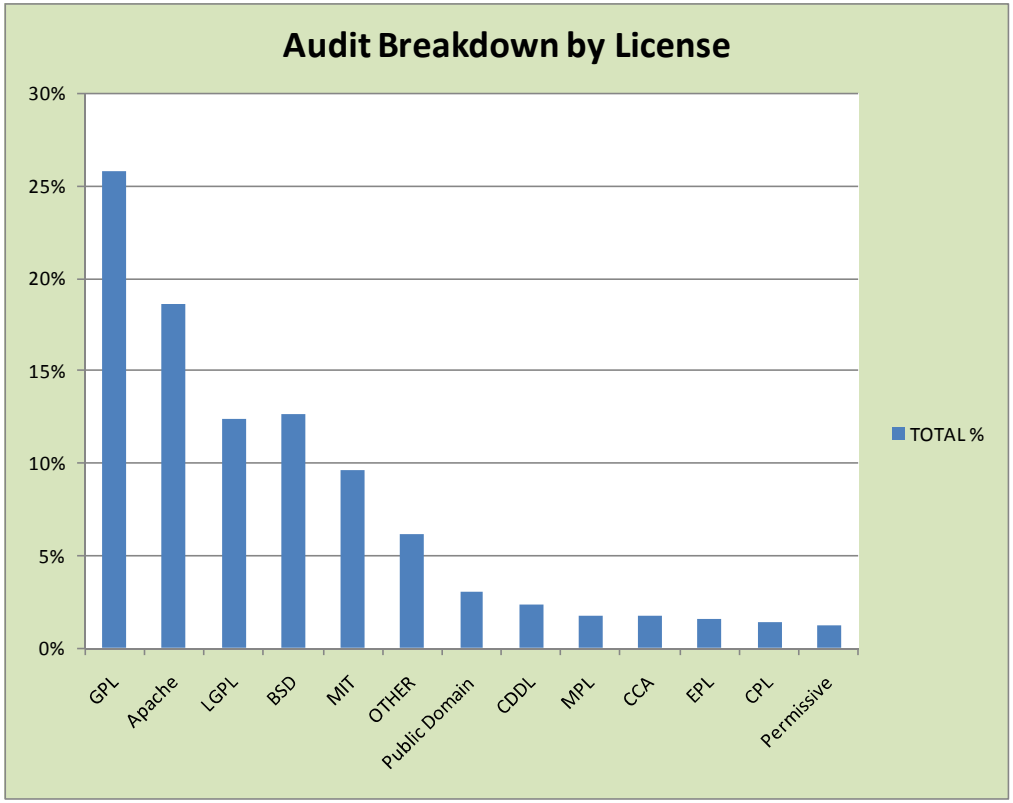
What is This Software Project Trying To Tell You?

There is probably a lot of content that you don't know about



Audit Example	
Size	15.9GB 59.1M LOC
Documented OS components	303
Undocumented OS components	535
Total #	838
% LOC from Open Source	60-65%

With license terms that may be problematic



Source: 2010 Year to Date Audit Engagements Performed by Palamida Professional Services

Open Source is not somehow "different"

Plaintiffs would be happy to settle this matter with Best Buy and Phoebe Micro if they either (i) ceased all distribution of BusyBox or (ii) committed to distribute BusyBox in compliance with the free and open source license terms under which Plaintiffs offer BusyBox to the world. Plaintiffs have patiently worked with Best Buy and Phoebe Micro to bring their products into compliance with the license, but unfortunately have now concluded that those efforts are destined to fail because neither Best Buy nor Phoebe Micro has the capacity and desire to meet either of Plaintiffs' demands for settlement. As such, Plaintiffs are forced to protect their interests in BusyBox by now respectfully moving for a preliminary injunction, pursuant to Rule 65, enjoining and restraining defendants Best Buy and Phoebe Micro from any further copying, distribution, or use of their copyrighted software BusyBox.

PLAINTIFFS'
MEMORANDUM OF LAW
IN SUPPORT OF THEIR
MOTION FOR
PRELIMINARY INJUNCTION
AGAINST DEFENDANTS
BEST BUY, CO., INC. AND
PHOEBE MICRO, INC.

SOFTWARE
FREEDOM CONSERVANCY, INC. and
ERIK ANDERSEN,

Filed 1/31/11

Software IP is a potent competitive weapon

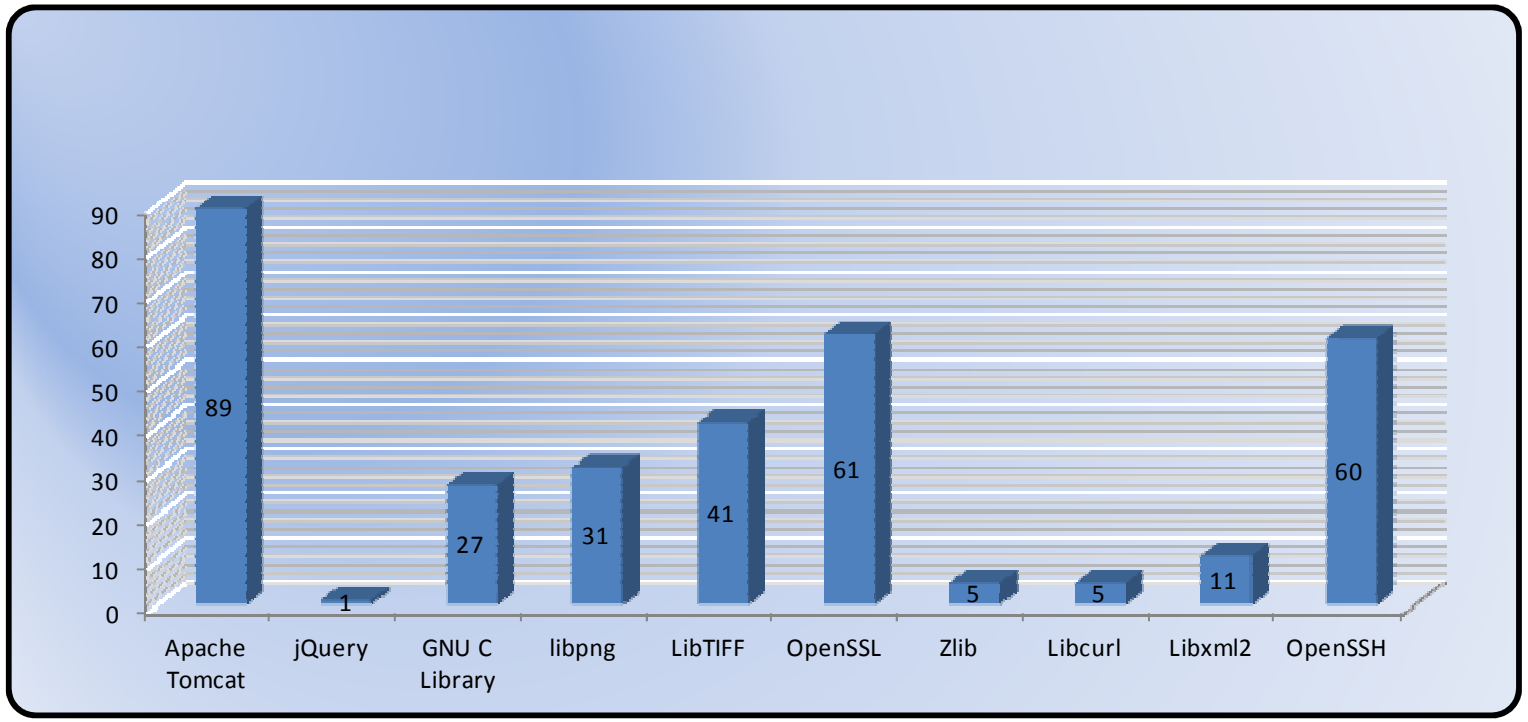
Love, Larry: Here Is the Oracle Statement and Final Complaint Versus Google

by Kara Swisher
Posted on August 12, 2010 at 6:46 PM PT

This afternoon, the database software giant said it was suing Google (GOOG), alleging patent and copyright infringement of Java-related intellectual property in the development of Android mobile operating system software.

http://kara.allthingsd.com/20100812/love-larry-here-is-the-oracle-statement-and-final-complaint-versus-google/

And Open Source Is Not Immune to Vulnerabilities



Vulnerabilities in Popular Open Source Projects Source: National Vulnerability Database

Oh No, Kernel.org was Hacked

by Susan Linton - Aug. 31, 2011

A notice appeared on www.kernel.org today informing visitors that the servers housing the Linux kernel source code had been hacked earlier this month. The breach was discovered yesterday and maintainers believe the source code itself is unaffected.

Source: ostatic.com

August 2011

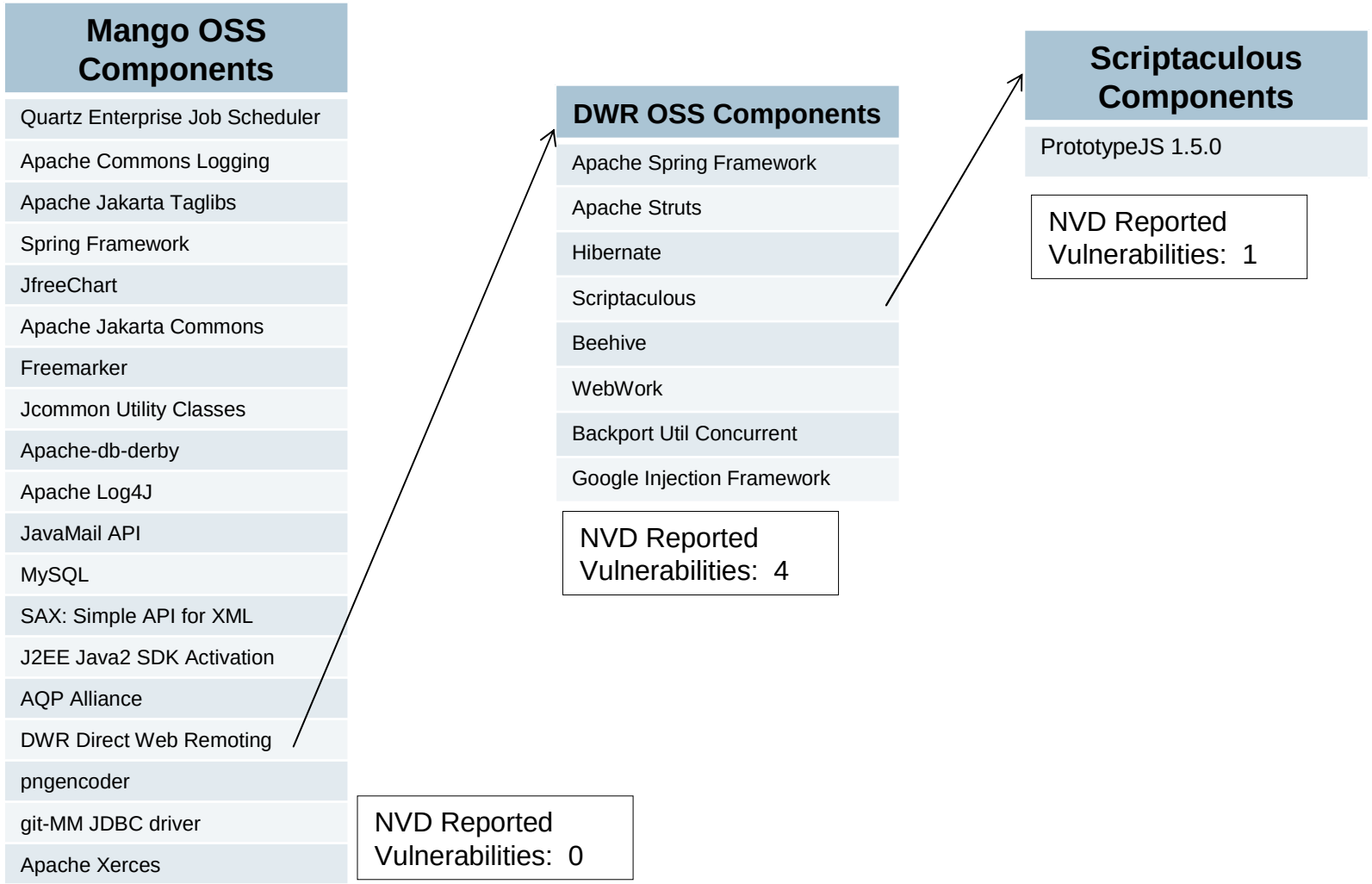
‘Devastating’ Apache bug leaves servers exposed

Devs race to fix weakness disclosed in 2007

Attack code dubbed “Apache Killer” that exploits the vulnerability in the way Apache handles HTTP-based range requests was published Friday on the Full-disclosure mailing list. By sending servers running versions 1.3 and 2 of Apache multiple GET requests containing overlapping byte ranges, an attacker can consume all memory on a target system.

The Register®

August 14, 2011



Risk is Risk

And you can’t mitigate risk you don’t know you have

PALAMIDA™

PALAMIDA™

What to Do Tomorrow

- Set up an OSRB or equivalent
- Establish your policy for use of externally sourced software
- Don’t stop at IP, include security
- Audit any software acquired via M&A
- Evaluate compliance alternatives, and get started

Open Source Review Board

- Comprised of Legal, Development and Security
- Review and Approve Policy for externally sourced software
- Establish the scope of information required and retained (the request form)
- Case-by-case use decisions
- Review and approve the policy for compliance with obligations
- Reports to CFO, GC, VP engineering or others periodically on compliance status

Policy

What is the name and version of this software component?

Where is it used?

What is the license?

Is this component in a software product that ships to customers?

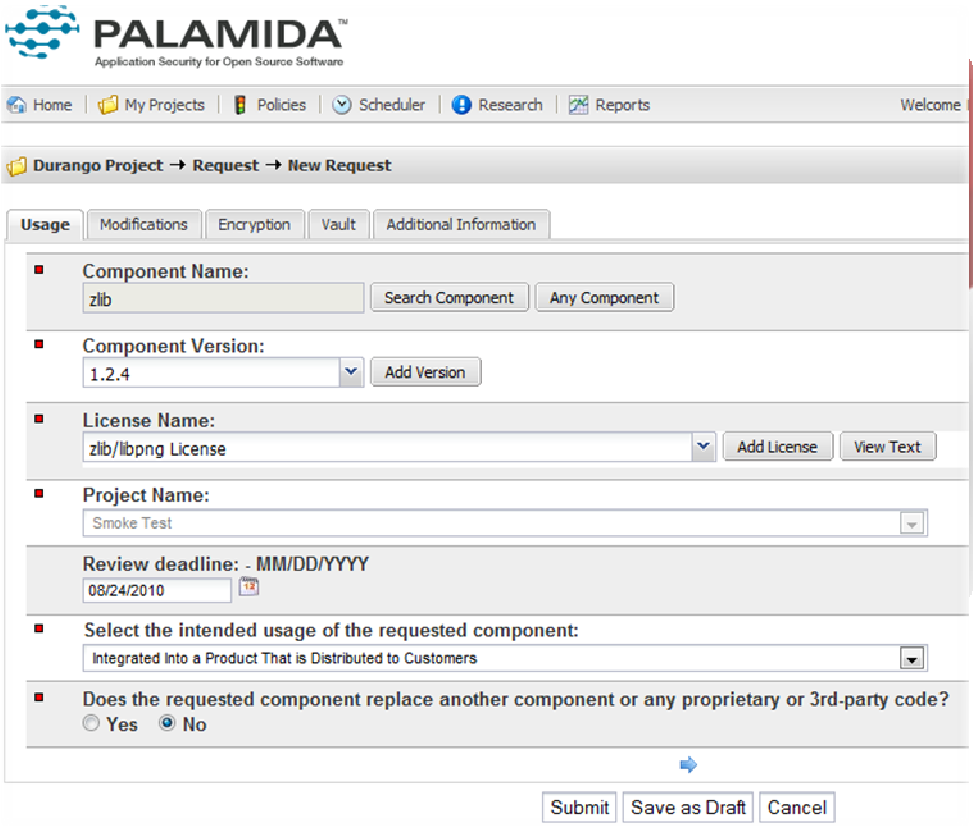
Does this component contain known vulnerabilities?

Have we modified this component?

When was the last time we checked this software for version and vulnerability?

Does this component contain encryption?

Have we added this component to the notices file?



Mergers and Acquisitions (and outsourced development)

- Make code audit a contract item
- Don’t rely on reps regarding code content – typically 3-5x more found than disclosed
- Use outside firms to maintain an “arms-length” relationship
- Factor in remediation costs
- Don’t integrate the code with yours until you are confident of origin

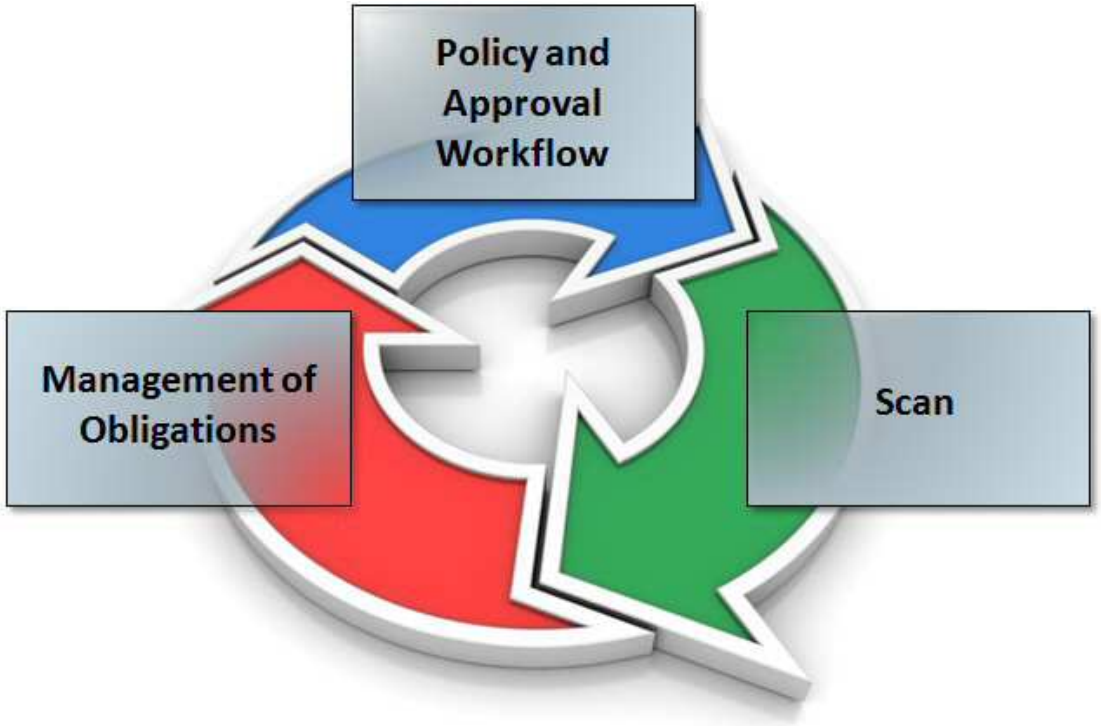
What Acquiring Firms Are Concerned About Today

- GPL and other Viral Licenses (esp v3.0)
- Affero GPL
- Commercial Content and Libraries
- Restrictions on commercial use or field of use (e.g. no Military use)
- Cryptography
- Code with Unknown Licenses
- % of undisclosed content

Evaluate Compliance Alternatives, and Get Started

- In-house process
- External Professional Services – periodic reports
- In-house system
  - Owned by development
  - Used by development, legal and security
  - System of record for policy and content
- The first pass is the most time-consuming – consider a outside audit to populate the internal system

Evaluate Compliance Alternatives, and Get Started



Open Source Software: the Intersection of IP and Security

Greg Kelton, Managing Director EMEA, Palamida Inc.
gkelton@palamida.com

PALAMIDA™