OWASP
Open Web Application Security Project

Managing Open Source Library Risks

-Dhanashree C. Kulkarni

About the speaker

- Application security Analyst with Paycor Inc.
- In addition to Pentesting Web and mobile applications, her focus areas include working with development teams to help build security in the SDLC.
- Formerly worked as a Security consultant and Team lead with Security services providing companies in Telecom and Healthcare domains.

Agenda

- Introduction: Risks associated with Open Source
- Risk Areas
  - Open Vulnerabilities
  - Legal Compliance
- Managing Open source components in codebase
- Challenges faced and effective solutions

Agenda

- Introduction: Risks associated with Open Source
- Risk Areas
  - Open Vulnerabilities
  - Legal Compliance
- Managing Open source components in codebase
- Challenges faced and effective solutions

Introduction: Risks associated with Open Source

- Open source components have become the backbone of modern applications, comprising of more than 60% of the entire code base

- Though it reduces the development time and efforts, it has its share of shortcomings
  - The code may have **open vulnerabilities** against it, which can be used to break into the application
  - The license under which the code/library is release may have **legal implications** on the company

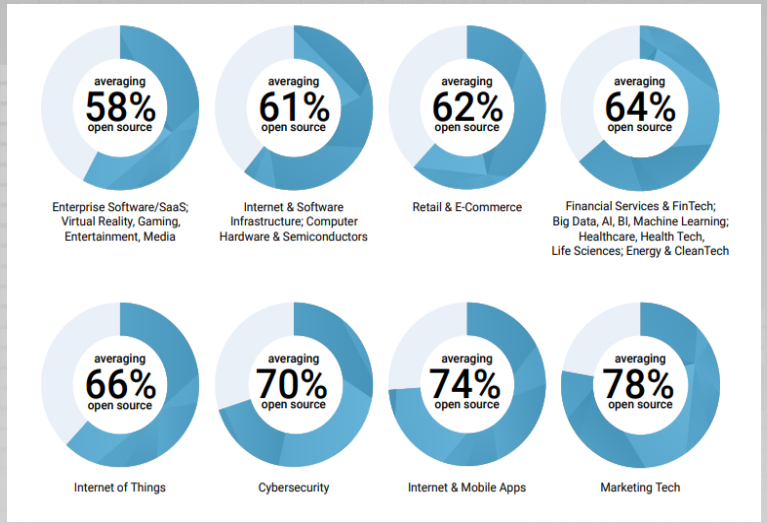


Image source: 2019 Open Source Security and Risk Analysis (OSSRA) Report

As per the OSSRA report, 60 % of the code they audited, contained at least one open source vulnerability and 68 % contained components with license conflicts.

Agenda

- Introduction: Risks associated with Open Source
- Risk Areas
  - Open Vulnerabilities
  - Legal Compliance
- Managing Open source components in codebase
- Challenges faced and effective solutions

Risk Areas : Open Vulnerabilities

Equifax Breach

- Attackers had exploited a vulnerability in the **Apache Struts2** open source component
- Personally identifiable information of around 147.9 million people was compromised
- The company failed to patch the vulnerable open source component in their web application, in time.

Drupal - Drupalgeddon

- The vulnerability potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being compromised

Image source: https://www.devopsdigest.com/breaches-caused-by-open-source-components-growing

Risk Areas : Open Vulnerabilities

Kubernetes

- Kubernetes, the de facto standard in Linux container orchestration had a privilege escalation vulnerability in 2018
- The vulnerability allowed any user to gain full admin access on any node being run in that cluster
- In addition to stealing sensitive data and installing malware, the flaw also had the ability to bring down production applications and services behind the firewall.

Node.js Event-Stream Hack

- The vulnerability due to a compromised event-stream package.
- The package had been injected with a malicious code, which could be used to capture user's private keys.

Last year, npm released and auditing tool to scan for know vulnerabilities against the package.

Risk Areas : Open Vulnerabilities

Why does Open source software need extra maintenance efforts?

- Open source has a **pull support model,** making the users responsible for keeping track of vulnerabilities, fixes, and updates for the open source they use.
- Difficult for the organization to track the open source components used in the application by the developers
- The average age of vulnerabilities identified by the OSSRA report in 2018 was 6.6 years

Agenda

- Introduction: Risks associated with Open Source
- Risk Areas
  - Open Vulnerabilities
  - Legal Compliance
- Managing Open source components in codebase
- Challenges faced and effective solutions

Risk Areas: Legal Compliance

- With the exponential growth of Open source components usage across all industries, Open source licensing issues should concern every organization.
- Patent trolls are becoming more common with companies acquiring patents, solely to file lawsuits against other companies and drive revenue through litigation.
- As a current trend, not only bigger brands, but more and more small companies are being targeted by trolls.

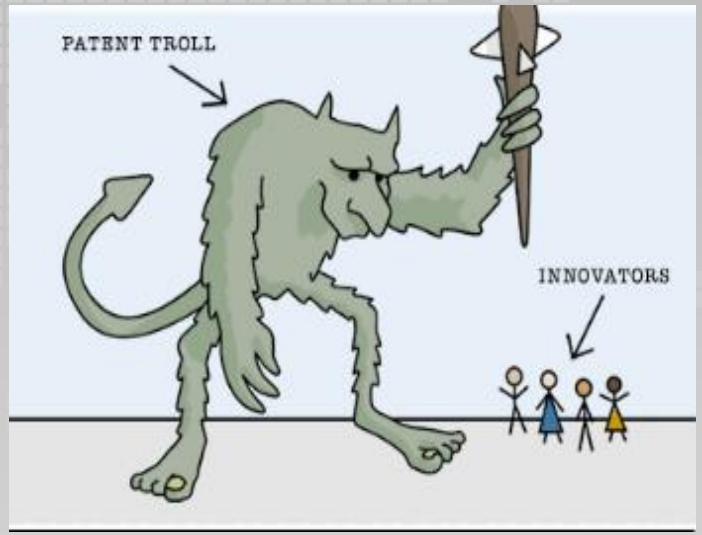


Image source: wh.gov/patenttrolls

Open Source License Types

Permissive	Semi-permissive	Restrictive
NON-COPY LEFT		COPY LEFT
Low Risk	Medium Risk	High Risk, Conditional licenses
Licensed works, modifications and larger works may be distributed under different terms and without source code.	Some of the licensed works need to be distributed under same license, however larger works may be distributed under different terms	Modifications must be released under same license so that the derived work remains open and free the same way as the original work(strong copyleft licenses even need the source code to be released, some licenses need the author's to be given credit in the license)
Do not place restrictions on later development or modification of original software	Do not place many restrictions on later development or modification of the original software*	Strong copyleft licenses do place restrictions on modification or later development of original software. Weak copyleft licenses like LGPL do not place restrictions to release their software as open source.
Can be combined with proprietary software	Can be combined with proprietary software*	Only weak Copyleft can be combined with proprietary software*

***NOTE: Accepting the use of a semi-permissive/restrictive license should be on a case by case basis**

Litigations against Open source licenses: BusyBox

- BusyBox Litigation - BusyBox is a software suite that provides several Unix utilities in a single executable file, which is licensed under GPL v2
- A series of lawsuits have been filed against companies for violating the GPL in relation to BusyBox software
- Companies like Verizon, VMware had been accused of using the BusyBox software without complying to the GPL requirements.
- Though none of the companies modified the code, the companies were charged for violating the requirements to release the source code, or to include attribution.

Litigations against Open source licenses: Artifex

- Another case involved Ghostscript, a PDF interpreter developed by Artifex Software that can be obtained under dual-licensing model
- Hancom, a Korean public company began integrating Ghostscript code into its proprietary office productivity products
- The company was charged for refusing to release the source code for free distribution or to purchase a commercial license
- Based on the terms of open source software license, Hancom was sued, both for copyright infringement and for breach of contract

Agenda

- Introduction: Risks associated with Open Source
- Risk Areas
  - Open Vulnerabilities
  - Legal Compliance
- Managing Open source components in codebase
- Challenges faced and effective solutions

Managing Open source components in codebase

- Create and Enforce Open source Risk Policies and processes
- Developer education
- Scanning code binaries for open vulnerabilities and incompatible licenses, using a scanner is a good option as it would be tedious to manually check the entire code base.

Open source Licenses: Acceptable Use Policy

License Name	Allow	Deny	Conditional Allow/Deny
Low Risk License/Permissive			
Apache 1.0	x		
Apache 2.0	x		
Artistic 1.0	x		
Artistic 2.0	x		
MIT	x		
Unlicense	x		
BSD Zero Clause license	x		
FreeBSD (2 clause)/FreeBSD	x		
FreeBSD (3 clause) ("New"/"Revised" license)			x
FreeBSD (4 clause)			x
Intel			x
ISC (Internet Systems Consortium)			x
JSON	x		
Ruby	x		
Boost Software License 1.0	x		
W3C	x		
WTFPL	x		

License Name	Allow	Deny	Conditional Allow/Deny
Medium Risk/Semi permissive			
Mozilla Public License 1.0	x		
Mozilla Public License 2.0	x		
Eclipse Public License 1.0		x	
Eclipse Public License 2.0			x
Common Public 1.0		x	
CC BY 2.5			x
CC BY 3.0			x
CC BY NC 3.0		x	
CC BY SA 1.0			x
CC0	x		
Common Development and Distribution License version 1.0, 1.1 (CDDL-1.0, 1.1) -Actually the Sun public license (SPL 2.0)			x
Microsoft Public license (MS-PL)	x		

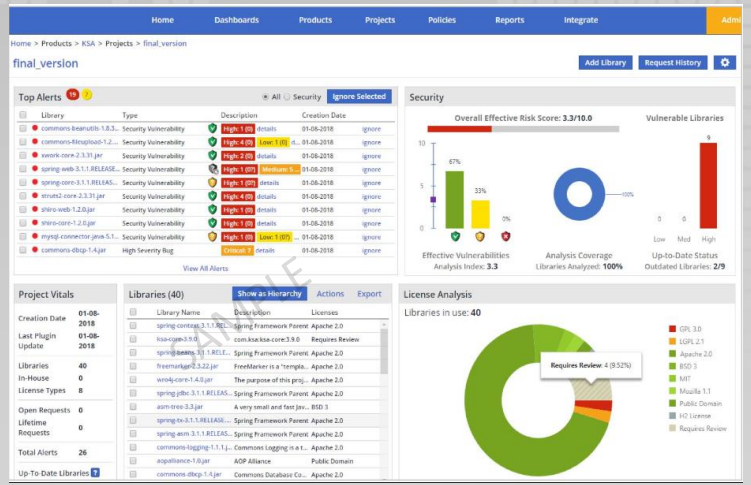
License Name	Allow	Deny	Conditional Allow/Deny
High Risk/Restrictibe or CopyLeft			
Microsoft Restrictive License (MS-RL)			x
GNU GPL v2.0		x	
GNU GPL v3.0		x	
GNU GPL with classpath exception			x
European Union Public License 1.1		x	
Affero GPL (AGPL)			X
Lesser GPL (LGPL) 2.0			X
Lesser GPL (LGPL) 2.1			X
Lesser GPL (LGPL) 3.0			X
OpenSource License 3.0		x	

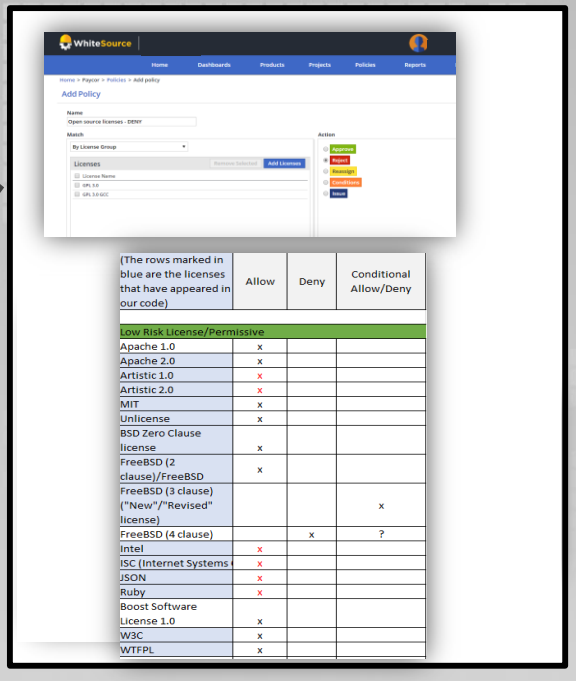
DISCLAIMER: Please consult your legal team pertaining to permissibility of various license types for your organization.

Whitesource: Configuration

Load the project in Whitesource

Build the latest code base





(The rows marked in blue are the licenses that have appeared in our code)	Allow	Deny	Conditional Allow/Deny
Low Risk License/Permissive			
Apache 1.0	x		
Apache 2.0	x		
Artistic 1.0	x		
Artistic 2.0	x		
MIT	x		
Unlicense	x		
BSD Zero Clause license	x		
FreeBSD (2 clause)/FreeBSD	x		
FreeBSD (3 clause) ("New"/"Revised" license)			x
FreeBSD (4 clause)		x	?
Intel	x		
ISC (Internet Systems	x		
JSON	x		
Ruby	x		
Boost Software License 1.0	x		
W3C	x		
WTFPL	x		

Agenda

- Introduction: Risks associated with Open Source
- Risk Areas
  - Open Vulnerabilities
  - Legal Compliance
- Managing Open source components in codebase
- Challenges faced and effective solutions

Challenges faced and effective solutions

Challenge: Implementing Software Composition Analysis (SCA) tool across 30+ development teams

Solution:

- Risk based prioritization
- Leaning on Security Champions group
- Tracking and metrics – to track implementation progress with management.

  Progress is measured in adoption across teams first, and then compliance to policy/standards once that has been implemented

Thank You

References

- https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-19.pdf
- https://tldrlegal.com/
- https://opensource.org/licenses
- http://www.bswd.com/CNSV-1304-Saper(IP-SIG).pdf
- https://resources.whitesourcesoftware.com/recommended/open-source-licenses-explained
- https://resources.whitesourcesoftware.com/blog-whitesource/guest-post-open-source-lawsuits-have-crossed-the-watershed
- https://resources.whitesourcesoftware.com/blog-whitesource/top-3-open-source-risks-and-how-to-beat-them-a-quick-guide
- https://www.eweek.com/security/node.js-event-stream-hack-exposes-supply-chain-security-risks