WG3 Status Report
15th NEAOSS Promotion Forum

Study on Standardization and Certification
Working Group of NEA OSS Promotion Forum

Cheju, Korea, 2016-11-16
Table of Contents

- Introduction
- FOSS Supply Chain Risk Management
- FOSS Governance
- Technology requirement of mobile terminal browser
- OPENTHOS
- Survey of OSS in Big Data Platform
- Work Plan
Introduction - Role of WG3

NEAOSS Forum formed

“WG3: Standardization and Certification Study” in order to study

Open Source Software standardization and certification in July 2004
NEAOSS WG3

- Co-chairmen (CJK)
  - Miao Zongli
  - Koutarou Noyama
  - Keundong Kim
- Secretariat: Kan Zhang

- SWG1 (IME-SPI)

- SWG2 (Web)
  - FWTF
  - OMATF

- OSS Maturity Assessment
  - SPDX
  - OSMAAM
  - OSS Governance F/W

- Note: All activities/decisions are per NEAOSS WG3 directives

Dismissed at 2009

Find new work item for WG3
Recent Meeting Activities

1. **Beijing**
   - 2016.5.17
   - Evaluation Methodology of Government R&D Project
   - FOSS Supply Chain Risk Management
   - Open Source Software Hub

2. **Tokyo**
   - 2016.7.21
   - Survey of OSS in Big Data Platform and Data Analysis Result
   - FOSS Supply Chain Risk Management
   - Standard Status of Smart terminal

3. **Beijing**
   - 2016.10.19
   - Introduction of the OpenTHOS
   - FOSS Governance Guide
   - OASIS (Open Adoption Support Information System)

4. **Cheju**
   - 2016.11.15
   - Preparation for 15th NEA OSS Promotion Forum
   - WG3 Work Plan in 2017
WG3 Documents Server

- Totally:
  - WG3 Meeting: 38
  - WG3 Documents: 276

[Files and folders related to WG3 documents]
FOSS Supply Chain Risk Management

Background

- “By 2016, Open Source Software will be included in mission-critical applications within 99% of Global 2000 enterprises.” Gartner, Inc.
- “78% of companies run on open source software.” 2015 the future of open source

**Open Source Vulnerabilities Reported Per Year**

Reference: Black Duck Software knowledgebase, NVD, VulnDB
# FOSS Supply Chain Risk Management

<table>
<thead>
<tr>
<th>Component</th>
<th>Heartbleed</th>
<th>Shellshock</th>
<th>Freak</th>
<th>Ghost</th>
<th>Venom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found by</td>
<td>Riku, Antti, Matti, Mehta</td>
<td>Chazelas</td>
<td>Beurdouche</td>
<td>Qualys researchers</td>
<td>Geffner</td>
</tr>
</tbody>
</table>

Component: OpenSSL, Bash, OpenSSL, GNU C library, QEMU.
FOSS Supply Chain Risk Management

- **Why Legal Teams Care about Open Source Security?**
  - Open source risk management is not limited to license compliance.
  - Legal teams are increasingly aware of security obligations & risks.

- **Internal/External Reporting**
  - Executive management, Directors, Regulatory Agencies

- **Litigation Risks**
  - Lawsuits from customer/patient/financial data loss

- **Regulatory Penalties**
  - HIPAA, PCI, SOX

- **Loss of company IP/secrets**

- **Damage to company reputation from high-visibility breaches**
FOSS Supply Chain Risk Management

- Four factors that make open Source different
  1. Used everywhere
  2. Easy access to code
  3. Vulnerabilities are public
  4. Exploits readily available

- The Road to Secure Open Source Use
# FOSS Supply Chain Risk Management

## License Risk

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>5</td>
</tr>
<tr>
<td>Medium</td>
<td>11</td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
</tr>
<tr>
<td>None</td>
<td>22</td>
</tr>
</tbody>
</table>

## Security Risk

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>2</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
</tr>
<tr>
<td>None</td>
<td>34</td>
</tr>
</tbody>
</table>

## Operational Risk

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>18</td>
</tr>
<tr>
<td>Medium</td>
<td>14</td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
</tr>
<tr>
<td>None</td>
<td>3</td>
</tr>
</tbody>
</table>

## Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
<th>License</th>
<th>Security Risk</th>
<th>Operational Risk</th>
<th>Match Type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANTLR</td>
<td>2.7.7</td>
<td>BSD 3-clause &quot;New&quot; or &quot;Revised&quot; License</td>
<td></td>
<td></td>
<td>Automatic</td>
<td>Used</td>
</tr>
<tr>
<td>Apache Commons FileUpload</td>
<td>1.2.2</td>
<td>Apache License 2.0</td>
<td></td>
<td></td>
<td>Automatic</td>
<td>Used</td>
</tr>
<tr>
<td>Apache Commons Lang</td>
<td>3.1</td>
<td>Apache License 2.0</td>
<td></td>
<td></td>
<td>Automatic</td>
<td>Used</td>
</tr>
<tr>
<td>Apache Struts</td>
<td>2.3.7</td>
<td>Apache License 2.0</td>
<td></td>
<td></td>
<td>Automatic</td>
<td>Used</td>
</tr>
<tr>
<td>ASM</td>
<td>3.3</td>
<td>BSD 3-clause &quot;New&quot; or &quot;Revised&quot; License</td>
<td></td>
<td></td>
<td>Automatic</td>
<td>Used</td>
</tr>
<tr>
<td>ASM Commons</td>
<td>3.3</td>
<td>BSD 3-clause &quot;New&quot; or &quot;Revised&quot; License</td>
<td></td>
<td></td>
<td>Automatic</td>
<td>Used</td>
</tr>
</tbody>
</table>
## Security Risks

### 15 Vulnerabilities in Apache Struts 2.3.7

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Published</th>
<th>Base Score</th>
<th>Exploitability</th>
<th>Impact</th>
<th>Status</th>
<th>Target date</th>
<th>Actual date</th>
</tr>
</thead>
<tbody>
<tr>
<td>VulnDB 103918</td>
<td>Mar 3, 2014</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>Needs review</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>VulnDB 95405</td>
<td>Jul 18, 2013</td>
<td>6.8</td>
<td>8.6</td>
<td>6.4</td>
<td>Needs review</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>VulnDB 95406</td>
<td>Jul 18, 2013</td>
<td>4.3</td>
<td>8.6</td>
<td>2.9</td>
<td>Remediation Required</td>
<td>in 7 days</td>
<td>Never</td>
</tr>
<tr>
<td>NVD CVE-2013-1965</td>
<td>Jul 11, 2013</td>
<td>9.3</td>
<td>8.6</td>
<td>10</td>
<td>Remediation Required</td>
<td>19 days ago</td>
<td>Never</td>
</tr>
<tr>
<td>NVD CVE-2013-1966</td>
<td>Jul 11, 2013</td>
<td>9.3</td>
<td>8.6</td>
<td>10</td>
<td>Remediation Required</td>
<td>Never</td>
<td>Never</td>
</tr>
<tr>
<td>NVD CVE-2013-2115</td>
<td>Jul 11, 2013</td>
<td>9.3</td>
<td>8.6</td>
<td>10</td>
<td>Remediation Required</td>
<td>25 days ago</td>
<td>Never</td>
</tr>
<tr>
<td>NVD CVE-2013-2134</td>
<td>Jul 17, 2013</td>
<td>9.3</td>
<td>8.6</td>
<td>10</td>
<td>Remediation Required</td>
<td>19 days ago</td>
<td>Never</td>
</tr>
</tbody>
</table>

### Description

Apache Struts 2 before 2.3.14.3 allows remote attackers to execute arbitrary OGNL code via a request with a crafted action name that is not properly handled during wildcard matching, a different vulnerability than CVE-2013-2135.

**View full record**

### Base Score Metrics

**Description**

*AV*: NETWORK  
*AC*: MEDIUM  
*Au*: NONE  
*l*: COMPLETI

**Published on**: Jul 17, 2013  
**Updated on**: May 5, 2014

**Status**: Remediation Required

**Remediation**

*Target date*: Jul 23, 2015  
*Actual date*:  
*Reviewed by*: demo1  
*Updated by*: demo1  
*Updated on*: Jul 13, 2015

**Needs fixing**
## FOSS Supply Chain Risk Management

<table>
<thead>
<tr>
<th>Classification</th>
<th>Standard Development Organisation</th>
<th>Standard</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Origins (sources) of supply chains</td>
<td>ISO SC27</td>
<td>ISO/IEC 27036: Guidelines for Security of Outsourcing</td>
<td>These are generic documents and not specific to SCI</td>
</tr>
</tbody>
</table>
| 2 Delivery and governance of the Supply Chain       | NASPO (North American Security Products Organization)  
NIST                                           |                                        | Nothing specific to SCI                          |
| 3 Processing and configuration                      | ISO SC31                         | RFID supply chain applications            | Nothing specific to SCI                          |
|                                                    | iNEMI Supply Chain study group    | Risk Modelling pilot                     |                                                   |
|                                                    | HDPUG Supply Chain study group:   | Data Exchange pilot                       |                                                   |
| 4 Integrity techniques                              | JTC1-SC27                        | N10656: Update to ISO 27002: Security Techniques  
Open Trusted Technology Framework | Nothing specific to SCI              |
|                                                    | Safecode                         |                                        |                                                   |
|                                                    | Open Group                       |                                        |                                                   |
| 5 Verification and checks                           | ISO TC247                        | Fraud Controls and Countermeasures        | Nothing specific to SCI                          |
|                                                    |                                  | SEMI T20: Traceability (semiconductor industry) |                                                   |
WG3 has finished **FOSS SCRM standard guideline**

- The requirements of OSS supply management
- The governance for OSS SCRM
- OSS profiling for SCRM
- The guide of compliance for SCRM
- SPDX Specification
- The application of SPDX for SCRM

We have supplied service for more than 1000 enterprises.
FOSS Governance

Definition

- Open-source governance (also known as open politics) is a political philosophy which advocates the application of the philosophies of the open-source and open-content movements to democratic principles to enable any interested citizen to add to the creation of policy, as with a wiki document. ([https://en.wikipedia.org/wiki/Open-source_governance](https://en.wikipedia.org/wiki/Open-source_governance))

- Open source governance is the way an organization controls the use of open source software within their products and services, supply chains and business management activities, and the associated business and legal processes. ([blackduck](https://blackduck.com))
FOSS Governance

- **Purpose**
  - This guide provides a control framework and procedures for companies using open source, designed to help the accountability and compliance of enterprise open source.

- **Scope**
FOSS Governance

- Structure of FOSS Governance framework

- 3 Non sequential activities
- 5 Phases of FOSS Adoption
- 18 Sequential activities
## FOSS Governance

### Four standards in Korea

<table>
<thead>
<tr>
<th>No.</th>
<th>Name of the Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTAK.KO-11.0110</td>
<td>Open Source Software Categorization &amp; Profile</td>
</tr>
<tr>
<td>TTAK.KO-11.0133/R1</td>
<td>Open Source Software Maturity and Applicability Assessment Model(OSMAAM)</td>
</tr>
<tr>
<td>TTAK.KO-11.0182</td>
<td>TTAK.KO-11.0182 Open source software package data exchange specification(SPDX)</td>
</tr>
<tr>
<td>TTAK.KO-11.0176</td>
<td>The Governance framework for Open Source Software</td>
</tr>
</tbody>
</table>
FOSS Governance

Applying the Standard to the Structure of FOSS Governance framework

- TTAK.KO-11.0182
  Open source software package data exchange specification (SPDX)

- TTAK.KO-11.0110
  Open Source Software Categorization & Profile

- TTAK.KO-11.0133/R1
  Open Source Software Maturity and Applicability Assessment Model (OSMAAM)
FOSS Governance

Future Work Overview

- The Competency management method for open source software engineers
- Establish policy
- Acquisition
- Adoption
- Operation and Maintenance

- Continuously improve
- Compliance
- Education
- Monitoring

- Diagnosis or consulting
  - Create policy
  - Build Organization

- Requirements Analysis
  - Research
  - Analysis

- Contract
- Design
- Development
- Packaging
- Test
- Deployment

- Installation
- Operation
- Maintenance
- Community

- Technical Support

Open Source Organization Maturity Diagnostic Model.

The open source projects monitoring method of enterprises in Japan. Ex) FUJITSU big data FOSS projects monitoring method

The open source community management techniques of enterprises in China. Ex) HUAWEI, ALIBABA ...
Technology requirement of mobile terminal browser

- **Background**
  - PC: interactive terminal = 2:3 (2007)
  - PC: smart terminal = 1:10 (Now)
  - Smart terminal will reach 33 billion in 2020 ≈ 4.3 / person

- **Purpose**
  - This standard applies to the design, development and test of mobile terminal browser
Technology requirement of mobile terminal browser

Scope

Run-time System Requirements
- Network
- Platform
- Memory
- Screen
- Keyboard
- Input Method
- ...

Protocol Requirements
- Makeup Language
- Transfer Protocol
- Security Protocol
- Image Format
- Audio and Video Format
- Cache
- ...

Function Requirements
- Display
- Operation
- Network
- Address Bar Function
- Download Function
- Upload Function
- Bookmark Function
- Security Function
- Cache Function
- ...

Software Design Requirements
- Design Rules
- Analytical Page Requirements
- Performance Requirements
- Core Requirements
- Cache Requirements
- ...

Technology requirement of mobile terminal browser

- Standard Status

New Project -> Draft -> Publicity -> Verify -> Final Version

- Technology requirement of mobile terminal browser
OPENTHOS

- Background
- Problem
- What
- How
- Purpose
OPENTHOS

- **Purpose**
  - High performance OS
  - Android ecosystem
    - Developers
    - User
  - High Security
  - Cross-platform
OPENTHOS

- **Characters**
  - Multi-Windows Mngt
  - Phone & Pad supported
  - Mouse & Touch supported
  - Print supported
  - High performance
    - 60 frames/second
    - Low delay
  - Low hardware requirement
  - Unitive user information
    - Real-time backup
    - Synchronization between devices
    - High security
    - High reliability
  - OPENThos Cloud
OPENTHOS

Community

- Committers
  - Tinghua
  - Tongfangpc
  - emindsoft
  - ...

Status

- IOS version available
  - Download: 700 in August
- Source Code
  - https://github.com/openthos
- 2016.12 - release on Tongfang PC
Survey of OSS in Big Data Platform

Structure

Data Source
- Web Data
- Sales Data, etc.
- Structured Data (RDB)
- Sensor Data
- Unstructured Data
- System Log
- Sound File
- Images

Data Collector
- Crawler
  - Apache ManifoldCF
  - Apache Nutch
- Data Loading
  - Apache Sqoop
  - Talend
- Data Collecting
  - Apache Flume
  - Apache Kafka
  - Fluentd
- CEP
  - Apache S4
  - Apache Spark
  - Streaming
  - Apache Storm
  - Esper
  - Drools
  - Fusion
  - Jubatus

Data Store
- Data Store/File System
  - Apache Hadoop
  - HDFS
  - Ceph
  - GlusterFS
  - Lustre
- Security/Authentication
  - MIT Kerberos
  - OpenLDAP
- Cache / Scale Out
  - Apache Cassandra
  - Apache Hbase
  - Infinispan

Parallel/Distributed Processing
- Data Analysis
  - Apache Hadoop
  - YARN
  - Apache Hadoop
  - Apache Mesos
  - Apache Spark
  - Apache Tez

Query Engine
- Security/Authentication
  - Apache Drill
  - Apache Hive
  - Apache Spark SQL
  - Impala

Data Loading
- Apache Sqoop

Cache / Scale Out
- In-memory DB/Distributed KVS
  - Apache Cassandra
  - MongoDB
  - Redis
  - Riak

Machine Learning
- Mlib
- Jubatus

Deep Learning
- Caffe
- Chainer
- CNTK
- Deeplearning4j
- DSSTNE
- PredictionIO

Statistic Analysis
- R

Full Text Search
- ElasticSearch

BI/BA Tools
- Pentaho
- JasperReports
- SAS
- MicroStorategy

In-memory DB
- VoltDB

DWH/Martless
- MySQL
- PostgreSQL
- * No famous OSS

System Operation Control / Monitoring
- Hinemos
- Zabbix
Survey of OSS in Big Data Platform

- **Survey Category**

  **Developers’ Activity**
  How active are developers?
  - Number of committers
  - top committer
  - Mailing list Numbers
  - Ratio of active days

  **Users’ Activity**
  How popular is the software?
  - Books in Amazon
  - Stars in GitHub
  - Mailing list Mails
  - Followers on Twitter

  **Quality of Software**
  Can we use the software without defects?
  - Bug resolution rate
  - Blocker/Critical Bug resolution rate
  - Vulnerabilities
  - Duplications
Survey of OSS in Big Data Platform

Survey Result

Number of committers (monthly)

Apache Spark is rapidly increasing from 2014

Average number of committers in month

- Over 100 committers make some commits to Apache Spark
  - 2013: 27.8 → 2014: 72.1 → 2015: 114.7

![Graph showing commit activity for various OSS projects over time with Apache Spark and Talend highlighted.]

- Apache Spark
- Talend
Survey of OSS in Big Data Platform

Survey Result

Commits (x-axis) and Critical bug fix rate (y-axis)

Vulnerabilities (2006 – 2016)

- Totally there are small number of vulnerabilities
  - JasperReports had the largest number of vulnerabilities, but the number is 10
  - MongoDB
  - Pentaho
  - JasperReports

Not active development, High critical bug fix rate (need to watch)

Active development, High critical bug fix rate
Survey of OSS in Big Data Platform

Survey Summary

- We can build the Big Data Platform only with OSS
  - Enterprise supports are getting better
  - However, it is necessary to check the functions and quality of softwares

Survey Conclusion

- Apache Spark and the ecosystem are hot
- Developers for Elasticsearch may be hardworkers
- MongoDB and Ceph are going to be stable
Work Plan of WG3 in 2017

- OASIS (Open source Support Information System)
- Assessment Model of Open R&D project for Government
- Applying FOSS Supply-Chain Risk Management Guide
- OpenTHOS Project
- Promote the application of WG3 achievements in CJK.
Thank you very much!

谢谢
ありがとうございました
감사합니다