Framing

NTIA Software Supply Chain Transparency

Éamonn Ó Muirí
https://flic.kr/p/46dsiz
http://creativecommons.org/licenses/by/2.0/legalcode
Framing Working Group

Managed with love and patience by co-chairs Michelle Jump and Art Manion

Meeting almost weekly since July 2018

- Fridays at 1400 EDT
- https://lists.sei.cmu.edu/mailman/listinfo/ntia-sbom-framing

Framing concepts that apply to the entire multi-stakeholder process

Michelle Jump
MedSec LLC
Global Regulatory Advisor - Medical Device Cybersecurity
MichelleJump@medsec.com

Art Manion
Software Engineering Institute
CERT Coordination Center
Principle Engineer “/” Technical Manager
amanion@cert.org
Agenda

1. Phase 1 summary
2. Activity update
3. Next steps
4. Requests
Phase 1: What is an SBOM?

*Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)*

https://tinyurl.com/y7s8ab3t

“An SBOM is effectively a nested inventory, a list of ingredients that make up software components.”

Partial Table of Contents

- 2 What is an SBOM?
  - 2.2 Baseline Component Information
  - 2.4 Component Relationships
- 4 SBOM Processes
  - 4.1 SBOM Creation: How
  - 4.2 SBOM Creation: When
  - 4.3 SBOM Exchange
  - 4.4 Network Rules
  - 4.6 Applications of SBOMs
Phase 2: Beyond the basics

Started November 2019

Several Ongoing Projects

Additional Planned Work
Ongoing Activity

• Collaboration between Health Care Proof-of-Concept and Framing WGs
  • Provide upstream SBOMs
  • Test Framing Phase 1 concepts

• Documents in progress
  • Software Identity Discussion and Guidance
  • Sharing and Exchanging SBOMs

• Other threads
  • Supplier identification
  • The acronym formerly known as “VEX”
Naming is Important and Hard

• Currently, there are no global authoritative sources to obtain the values for the Component Name in SBOM data
  • Two actors who compile SBOM might use two different values for the same component
  • Need to map from SBOM to other data sources (e.g. vuln databases)
• Multiple standards for naming and identity exist and are being deployed (SWID, PURL, SWHID, etc)
• Goal: minimize the problem space and support naming convergence
• Several actors to consider
  • Original component supplier
  • Secondary authorship
  • Downstream users of the data
Potential Guidance for Component Identifiers

• We propose a two-step approach

• Preferred case: Existing Supplier or Coordinate namespace
  • If there exists an established, well-defined namespace, the component data
    author should use that
  • Includes: package managers, commercial suppliers with clear communication

• Alternate case: use an established software identity standard
  • Do not create a new identifier. Please.
  • Built from an existing, well accepted naming schema, including, for example:
    • SWID tags
    • Package URL (purl)
    • Software Heritage IDs
### Advertisement and Discovery

<table>
<thead>
<tr>
<th>Aspects of Sharing</th>
<th>Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>How does the author let people know where an SBOM is?</td>
<td>File in a well-known location, extension or MIME type to indicate format</td>
</tr>
<tr>
<td>How does the downstream developer locate the SBOM?</td>
<td>Well-known URI</td>
</tr>
<tr>
<td>How does the end user retrieve the SBOM?</td>
<td>Network information, such as Manufacturer Usage Description (MUD)</td>
</tr>
<tr>
<td>What format is the SBOM in?</td>
<td>See: Formats and Tooling WG</td>
</tr>
<tr>
<td>What search mechanisms might there be?</td>
<td>#SBOM?</td>
</tr>
</tbody>
</table>
Advertisement and Discovery

“Here’s how to find my SBOM”

./.well-known/sbom

---

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTRIBUTING.md</td>
<td>Unbundle ext/xmlrpc</td>
<td>last month</td>
</tr>
<tr>
<td>EXTENSIONS</td>
<td>Unbundle ext/xmlrpc</td>
<td>last month</td>
</tr>
<tr>
<td>LICENSE</td>
<td>Update and fix remaining year ranges (2019)</td>
<td>17 months</td>
</tr>
<tr>
<td>NEWS</td>
<td>Move to alpha2 section</td>
<td>yesterday</td>
</tr>
<tr>
<td>README.REDIST.BINS</td>
<td>Unbundle ext/xmlrpc</td>
<td>last month</td>
</tr>
<tr>
<td>README.md</td>
<td>Add <code>pkg-config</code> to the build list</td>
<td>2 months</td>
</tr>
<tr>
<td>SBOM.spdx</td>
<td>Create SBOM.spdx</td>
<td>now</td>
</tr>
<tr>
<td>UPGADING</td>
<td>Add ldap_count_references()</td>
<td>7 hours</td>
</tr>
<tr>
<td>UPGRADEING.INTERNALS</td>
<td>[ci skip] (Hopefully clarify meaning)</td>
<td>4 hours</td>
</tr>
<tr>
<td>azure-pipelines.yml</td>
<td>Increase timeout on sanitizer job</td>
<td>6 days</td>
</tr>
<tr>
<td>build.conf</td>
<td>Remove build.mk usage</td>
<td>12 months</td>
</tr>
<tr>
<td>build.conf.bat</td>
<td>Fix #79146: cscript can fail to run on some syste...</td>
<td>5 months</td>
</tr>
</tbody>
</table>

---

Icon by User: Manco Capac, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=5057789
Map by The Opte Project., CC BY 2.5, https://commons.wikimedia.org/w/index.php?curid=1538544
## Access

<table>
<thead>
<tr>
<th>Aspects of Sharing</th>
<th>Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>How does one retrieve an SBOM?</td>
<td>For the downstream developer, perhaps ‘git clone’ and look in well known file or directory</td>
</tr>
<tr>
<td></td>
<td>For the end user, HTTP[S], CoAP[S], OpenC2, email (worst case?)</td>
</tr>
<tr>
<td>What access rights to people have?</td>
<td>Access controls might include:</td>
</tr>
<tr>
<td></td>
<td>• Git permissions</td>
</tr>
<tr>
<td></td>
<td>• HTTP authentication (web token or basic user)</td>
</tr>
<tr>
<td></td>
<td>• OpenC2 MQTT group membership</td>
</tr>
</tbody>
</table>
Open Questions

- Does the SBOM consist of a single file or multiple files?
  - If multiple objects, what is retrieved first and how are the other objects retrieved?
- What are the security considerations for an SBOM?
  - Is an SBOM signed?
    - If integral, already retrieved
    - If externalized, then the signature needs to be located and retrieved
- Do we understand search well enough?
Next Steps

• Continue working on identification and sharing papers
• Contribute to Health Care Proof-of-Concept
• Supplier identification? Registration?
  • Why? Because it helps with global component identification
• A proper RDF model?
• VEX? What VEX?
  • Widespread interest, but has been de-prioritized over underlying fundamentals
  • Framing expects to take up VEX, or perhaps a more generic inheritance feature that incudes transitive vulnerability
Requests

• Review draft documents, provide comments
• Interested in ongoing or upcoming work? Join us:
  • Fridays at 1400 EDT
  • Mailing list: https://lists.sei.cmu.edu/mailman/listinfo/ntia-sbom-framing
  • Google Drive: https://tinyurl.com/yc3gajzz

• Should we be aware of, coordinating with other efforts?
• Have we identified important gaps from Phase 1?