Framing

NTIA Software Supply Chain Transparency

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

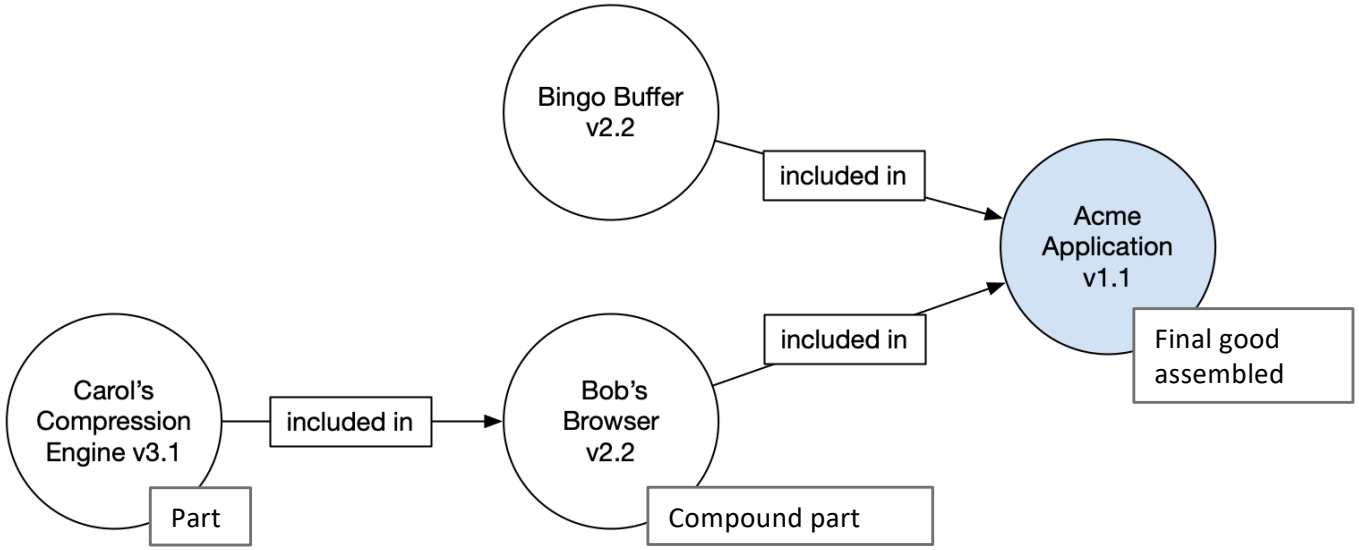
Phase 1: What is an SBOM?

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



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

Phase 2: Beyond the basics

Started November 2019

Several Ongoing Projects

Additional Planned Work

https://www.facebook.com/powerofpositivity/posts/10156301474602371
and Roy T. Bennet

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

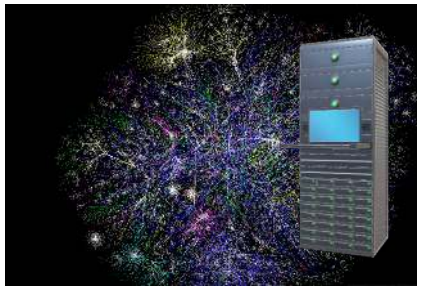
Advertisement and Discovery

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

Advertisement and Discovery

"Here's how to find my SBOM"

/.well-known/sbom



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

Access

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

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?