Web Access to SBOM Data

Proposal to Standardize SBOM access

Agenda

Context and Background

- Current state of SBOM standardization
- What's missing for ubiquitous access to SBOM data

Network Access and Protocols

- Overview of RFC 9472
- Discussion on what additional protocol work needed

Common Vocabulary

- Overview of SPDX SBOM Vocabulary
- Discussion on what additional vocabulary standardization is needed

Current State of SBOM Standardization

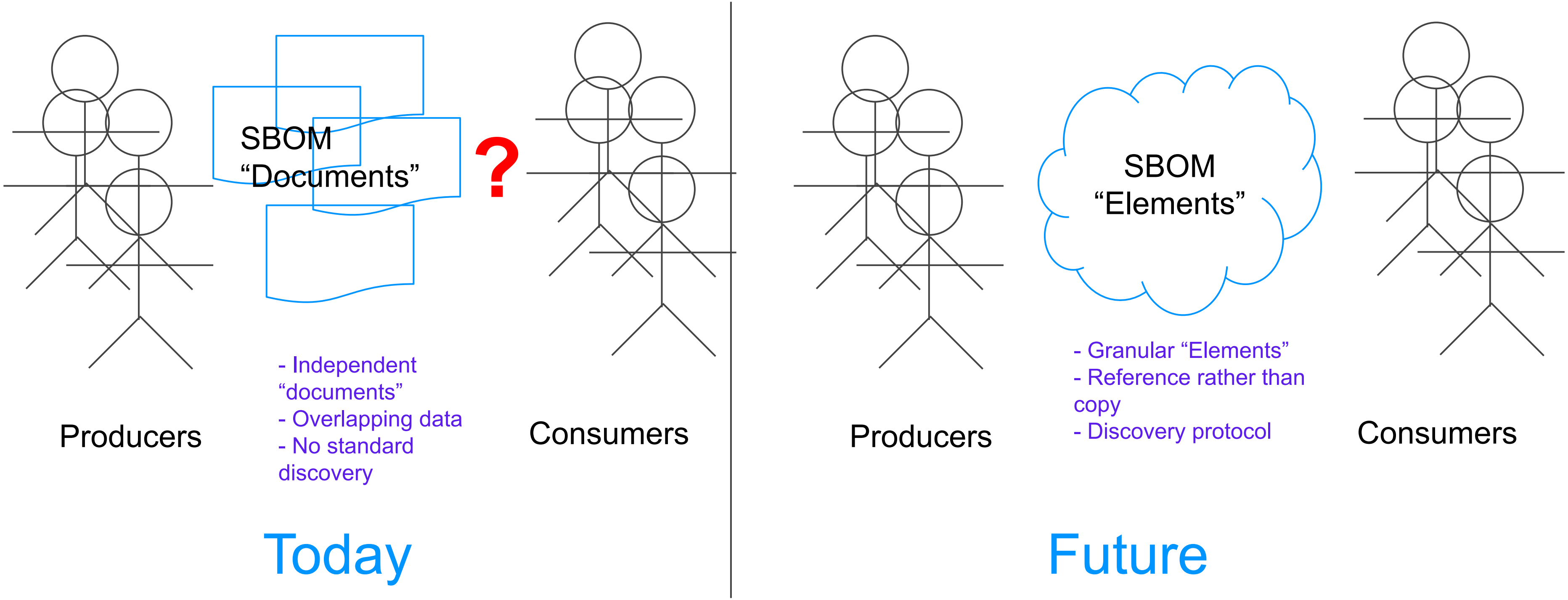
- CISA / NTIA refers to 3 different SBOM standard (SWID, SPDX, CycloneDX)
- Primarily focused on meta-data interchange
- Some collaboration between the SBOM standards to make sure we can interoperate on the most common use cases
- Efforts underway in OpenSSF SBOM Everywhere to have best practices for discovery of SBOM artifacts
- CISA Tooling workgroup clarifying how the field should be filled in

- however -

- No standard protocol for SBOM discovery and access (yet)
- Granularity of SBOM data access rather course

A Possible Future for SBOM’s

Open Easy Granular Access to SBOM Data



Producers

- Independent “documents”
- Overlapping data
- No standard discovery

Consumers

Today

Producers

- Granular “Elements”
- Reference rather than copy
- Discovery protocol

Consumers

Future

SPDX

A Possible Future for SBOMs

Problems Addressed in the Future Scenario

- Reference, not copy - reduces Element metadata inconsistencies
- Element metadata provided by the originator - not intermediate suppliers
- Only transfer what you need - more efficient SBOM communication

Protocols

SBOM Discovery

Protocols for SBOM Discovery

RFC 9472

- IETF RFC 9472
- The model consists mostly of a JSON object and can be associated with software or hardware
- Manufacturer Usage Descriptions (MUDs) YANG schema is an example how it can be applied to hardware (RFC 8520).
- Supports discovery of location of SBOMs and vulnerability information
- Format neutral - based on media type (SPDX, CDX, CSAF, CVRF, OpenVEX)
- 3 methods of SBOM communication - URL, from the device, from supplier

- However -

- May not be applicable to software in the middle of the software supply chain

SPDX

Question and Discussion

- Does it make sense to create a protocol for SBOM “Element” discovery similar to draft-ietf-opsawg-sbom-access-18?
  - Alternative is that each package management ecosystem and each commercial software provider has its own mechanism for SBOM and/or SBOM Element discovery
  - Another alternative is to have some kind of global registry

- If it does make sense, who’s interested and how do we get started?

SPDX

Common Vocabulary

Current SBOM RDF Vocabulary Specs

SPDX

- Everything in the SPDX SBOM specification supports linked data (JSON-LD, RDF)
- Decades of development and debate have gone into the spec
- First SPDX ontology introduced in 2010
- Current vocabulary covers the majority of SBOM use cases, however, is more “document centric”
    - OWL schema is available at https://github.com/spdx/spdx-spec/tree/development/v2.3.1/ontology
    - There are some known issues with the Ontology and schema
- SPDX 3.0 is under development - release candidate 1 is available
    - Model has been updated to be much more granular and “Element” base rather than “Document” based
    - In addition to the OWL schema, we are using SHACL for parser validations

SPDX

Questions and Discussion

- Should we have a common vocabulary for SBOM?
  - Is this a problem worth solving?
- Should we use a formal ontology language which supports linked data like OWL/RDF/SHACL?
  - W3C Standard
- Should we start with an existing Ontology (or two)?
- Who’s interested and what do we do next?

SPDX