Software Component Transparency

Virtual Meeting | June 27, 2019

Healthcare Proof of Concept Update

Objective

This is a collaborative effort between healthcare delivery organizations (HDOs) and medical device manufacturers (MDMs) to employ a provisional SBOM format and exercise use cases for SBOM production and consumption.

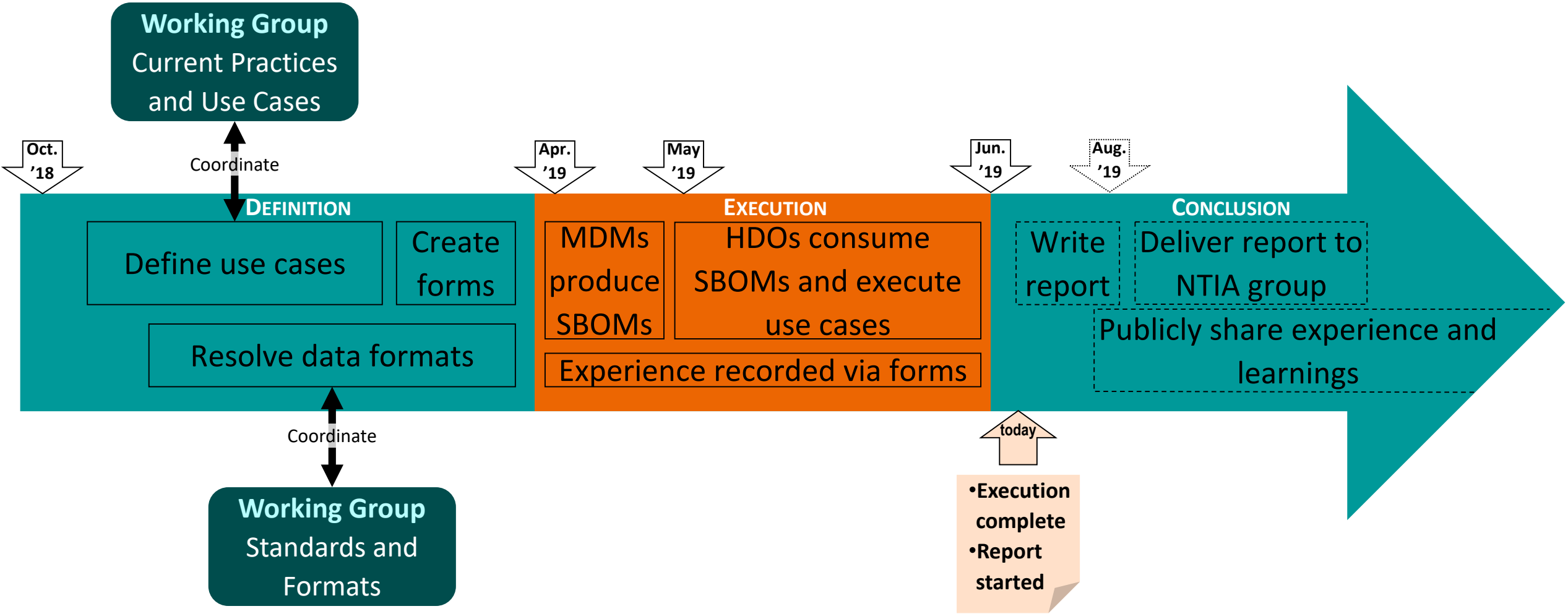
The goal is to demonstrate successful use of SBOMs and relate to the overall cross-sector effort to establish standardized formats and processes.

Scope

Item	In	Out	Comment
CBOM vs. SBOM (inclusion of hardware components)		✘	Minimum viable product, version 1, no clear line, let it be defined further outside the POC. Don't lose track of the issue. Parking lot.
Identifying a standard as the only acceptable format (canonization)		✘	No endorsement
Conforming to a standard (as opposed to defining a bespoke format)	✓		SWID and SPDX will both be used, but still not an endorsement
Inclusion of vulnerability information (front-end correlation)		✘	Gets stale, initiates long conversation, may need its own working group, could interfere with the execution of the POC, let's get the 1.0 version right and continue the conversation
Dependencies – level 1	✓		Best effort/optional*, may not contribute to POC
Dependencies – level n	✓		Best effort/optional*, may not contribute to POC, can explode complexity
Globally unique & immutable component identifiers (one and only one)		✘	Not in version 1.0, hard problem
Vendor name	✓		
Version down to build number (as far as provided)	✓		
Context ("yeah it's in here, but don't worry about it because…")	✓	✘	May not avoid further questions, worth a try to determine benefit Originally in scope, removed because of complexity
Delivery over the Internet (pull)	✓		Subscribe to information, manufacturers will not have the option to do so from their suppliers, at least for the POC
API for data access	✓	✘	Could be a reference architecture/model for adoption Originally in scope, removed as unessential to achieve goal, files shared via Box
Machine readable format	✓		

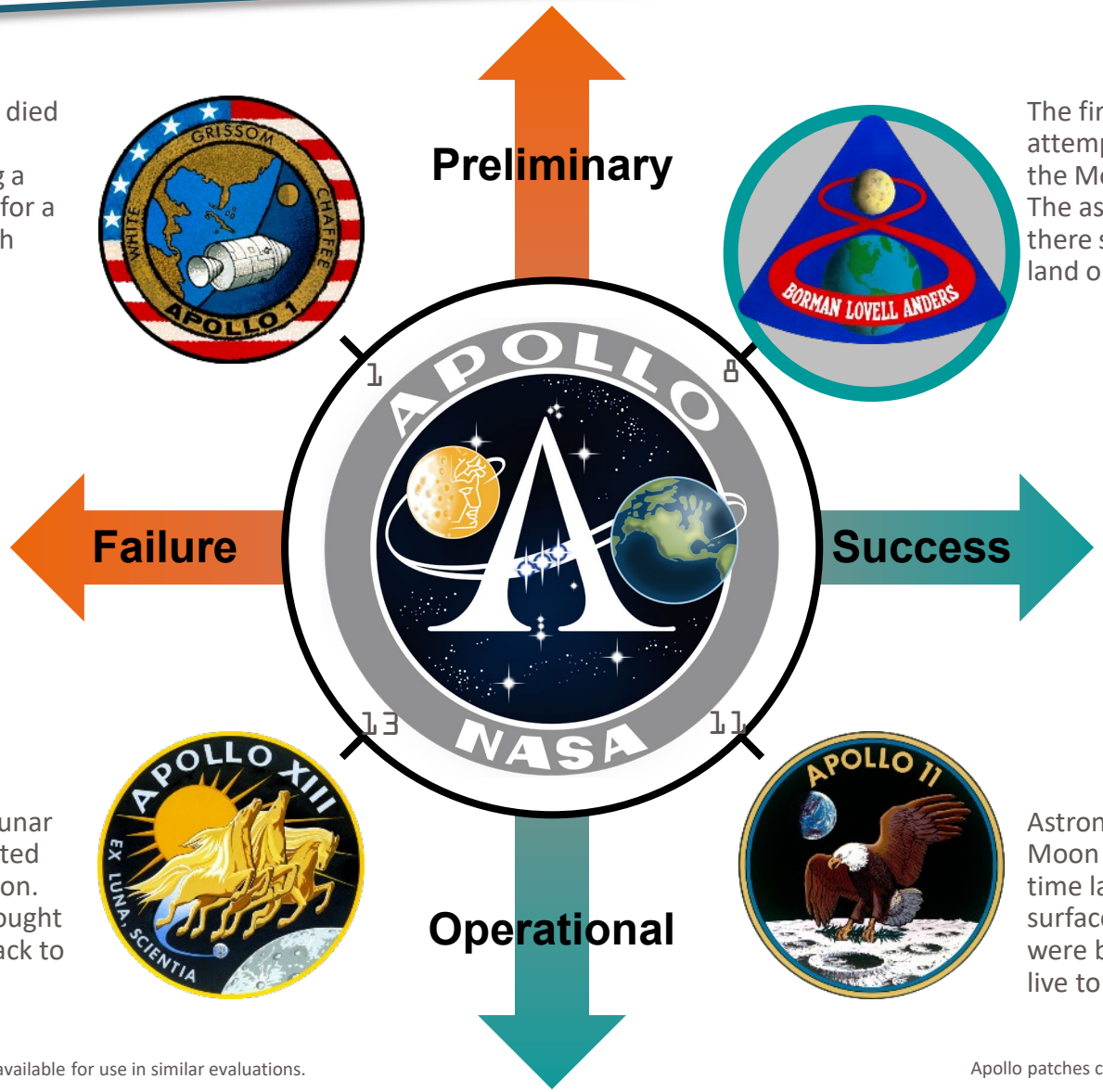
*Although not required for exercising the proof of concept, the final report should emphasize the importance of dependencies in the successful use of SBOMs.

Overview


Working Group
Current Practices and Use Cases
Coordinate
Oct. '18
Apr. '19
May '19
Jun. '19
Aug. '19
DEFINITION
Define use cases
Create forms
Resolve data formats
EXECUTION
MDMs produce SBOMs
HDOs consume SBOMs and execute use cases
Experience recorded via forms
CONCLUSION
Write report
Deliver report to NTIA group
Publicly share experience and learnings
today
•Execution complete
•Report started
Coordinate
Working Group
Standards and Formats

The Apollometer

“One small step for a working group, one giant leap for software security”



Three astronauts died tragically on the launchpad during a launch rehearsal for a planned low Earth orbital test.

The first planned attempt to shoot for the Moon succeeded. The astronauts made it there safely, but didn’t land on the surface.

The 3rd planned lunar landing was aborted due to an explosion. Heroic efforts brought the astronauts back to Earth safely.

Astronauts shot for the Moon and for the first time landed on the surface. The first steps were broadcast on TV live to the world.

Apollo patches courtesy of NASA: https://history.nasa.gov/apollo_patches.html

HDO Use Case Map

The following use cases were executed by the HDOs:

- Procurement
- Asset Management
  - General Asset Management
  - Risk Management
  - Vulnerability Management

Use Case Procurement

Note: This is a description of the use case activities with respect to use of SBOMs. HDOs did not necessarily execute all aspects during the Proof of Concept.

- A reduction of the number of questionnaires that have to be filled out as the SBOM can supplement the MDS2
Awareness regarding the presence of interfaced or system conflicts with the health IT system, etc.
- Awareness regarding the introduction of customized software into the IT system
- Clarity regarding end of life for software components in the device (e.g. device has windows 7 which is known to end of life in XX time, allows for questions at time of procurement regarding transition schedule, security coverage for devices that have components that will be end of life(e.g.Do you have a plan for covering security?), etc.)
- Informs asset management via identification of potential cybersecurity concerns
- Lifecycle management (understanding of current supported and unsupported software) for new devices and those already in the field
- Identifies unsupported software so HDOs can initiate alternative mitigations or control

Use Case Asset Management (General)

Note: This is a description of the use case activities with respect to use of SBOMs. HDOs did not necessarily execute all aspects during the Proof of Concept.

- Assisting HDOs in standardizing risk assessment for asset management
- Reduction of the number of questionnaires that have to be filled out as the SBOM can supplement the MDS2
- Asset inventory when SBOM changes/updates are communicated to HDOs
- Awareness regarding the presence of interfaced or system conflicts with the health IT system, etc.
- Awareness regarding the introduction of customized software into the IT system
- Actions that can be taken to protect the asset by providing sufficient details for each component

Use Case Asset Mgmt. / Risk Management

Note: This is a description of the use case activities with respect to use of SBOMs. HDOs did not necessarily execute all aspects during the Proof of Concept.

- Lifecycle management (understanding of current supported and unsupported software) for new devices and those already in the field
  - Identifies unsupported software so HDOs can initiate alternative mitigations or controls
- Monitoring of HDO inventory against new vulnerabilities as they emerge
- Assessment of a new product being added to the hospital network prior to integration (want to know how risky device is before adding to the network)
- Assessment of the level of risk associated with a particular vulnerability (SBOM allows you to get to the point of looking at what vulnerabilities still exist on a product and then can go look up CVE, etc. to enable risk assessment)

Use Case Asset Mgmt. / Vulnerability Mgmt.

Note: This is a description of the use case activities with respect to use of SBOMs. HDOs did not necessarily execute all aspects during the Proof of Concept.

- Monitoring of HDO inventory against new vulnerabilities as they emerge
- Assessment of a new product being added to the hospital network prior to integration (want to know how risky device is before adding to the network)
- Assessment of the level of risk associated with a particular vulnerability (SBOM allows you to get to the point of looking at what vulnerabilities still exist on product and then can go look up CVE, etc. to enable risk assessment

Participant Experience from Execution

Note: This is raw experience sampling, not the complete results nor the findings of the working group. The findings will be in the working group's formal report.

MDM experience: SBOM generation

Formats: for all MDMs but one, SWID and SPDX generated, slight preference for SWID (perceived as less error-prone)
Preparation challenges: list completeness, patch level determination, dependency relationships
Source data: some MDMs have central repository of components for all products, some don't
Generation method: various: manual, semi-automated (no automated tooling – to be developed)
Data issues: Product identification provided by readme – meta info that should be in the SBOM
Future looking: Anticipated complexity maintaining multiple version/configuration, but not covered in POC, anticipating trouble with HDOs connecting to different MDM/supplier portals

HDO experience: SBOM ingestion and use

CMDB: ServiceNow or N/A
Format appetite: SPDX more human readable, SWID preferred programmatically (easier ingest)
Data challenges: correlation to CVEs (SBOMs should use valid CPE names), data needed to be cleaned
Use Case Procurement:
- System not in place to leverage SBOM in procurement
- SBOMs allowed for identification of vulnerabilities
- End-of-Life components were identified and managed via added localized programmable firewall
- Information about customized software wasn't able to be processed
- Lack of trust in the completeness of the information provided
- Missing granular patch information (e.g., for OS)

HDO experience continued:

Use Case Asset Management (general):
- Digestion into CMDB not possible, tooling being developed
- Some risk management insights revealed, others are pending more sophisticated tooling
- In some cases, SBOM provided information that could be used to protect the asset
- SBOMs were useable in EoL planning, but in many cases this is still to be proven out

Use Case Asset Mgmt./Risk Management:
- Some risk management solutions not compatible with SBOM without future 3rd- party tools
- ISO 9001 – SBOM was leveraged by providing insight into risks
- Monitoring of devices against new vulnerabilities successful, and for others possible in theory

[Note: PoC did not include updating SBOMs over time]

Use Case Asset Mgmt./Vulnerability Management:
- Naming convention problem interfered
- Risk evaluation possible via associated CVSS score
- Some proactive mitigations possible because of SBOM info

Wishes: CPE names, version information, patch level (at the instance), retroactive SBOMs for EoL devices

Report

Purpose

The report will describe the Proof of Concept: how it was set up, what was exercised during execution, deriving findings from the recorded experience of the participants, and any conclusions that may be drawn.

Status

- Writing assignments accepted by group authors
- Initial analysis started
- Target completion: end of July
- Target review by working group: start of August
- Target availability to other working groups: August

Outline

I. Acknowledgements
II. Executive Summary
III. Background
IV. Purpose and Objectives
V. Scope
VI. Definitions
VII. Use Case Descriptions
VIII. Overview of Execution
IX. Overview of Findings
X. Conclusions (+ recommendations?)
XI. Appendices (if needed)