SOFTWARE COMPONENT TRANSPARENCY: HEALTHCARE PROOF OF CONCEPT REPORT

Drafted as part of a process convened by the National Telecommunications and Information Administration

October 1, 2019

Table of Contents

Executive Summary

A significant challenge to all industry verticals is securing devices and systems that incorporate software components from complex supply chains. In particular, purchasers and users of software are typically unable to ascertain the provenance of the components in software, and thus are unable to adequately understand the operational and cyber risks of the software. This document describes the software bill of materials (SBOM) proof of concept (PoC) led by medical device manufacturers (MDMs) and healthcare delivery organizations (HDOs), which examined the feasibility of SBOMs being generated by MDMs and utilized by HDOs as part of operational and risk management approaches to medical devices at their hospitals.

The PoC demonstrated that SBOMs can play a key role in how HDOs manage operational and cyber risks associated with medical devices. First, MDMs successfully generated SBOMs for medical devices utilizing standardized industry-agnostic formats, that were successfully ingested by the HDOs. Second, the participant HDOs were able to utilize the SBOMs provided from the manufacturers for identification of software vulnerabilities, including end-of-life components requiring mitigation, as well as utilize the information in the SBOM in conjunction with external vulnerability assessments such as risk scores and manufacturer disclosure statements for medical device security (MDS2) to identify risks in a manner previously not possible. The PoC also identified opportunities for enhancing SBOM formats, and opportunities and challenges for MDMs in generating SBOMs over time.

The participants in the SBOM PoC believe that the generation and consumption of SBOMs can play a role in securing the medical devices deployed by HDOs. The PoC provides a foundation for further research into the practical utilization of SBOMs, with the lessons not specific to healthcare. Rather, the conclusions and lessons of the PoC will prove valuable to multiple industries participating in the software transparency efforts spearheaded by the National Telecommunications and Information Administration (NTIA). Further, the PoC should inform the Food and Drug Administration's (FDA) consideration of the role SBOMs can play in securing the medical device ecosystem.

Background

The NTIA engaged stakeholders from across industry verticals to discuss software transparency in June 2018. The mission of the NTIA multi-stakeholder process on Software Component Transparency is to:

> "Explore how manufacturers and vendors can communicate useful and actionable information about the third-party and embedded software components that comprise modern software and IoT devices, and how this data can be used by enterprises to foster better security decisions and practices. . . . The goal of this process is to foster a market offering greater transparency to organizations, who can then integrate this data into their risk management approach."[1]

Fundamental to this effort is acknowledging that the complexity of the software supply chain contributes substantially to cybersecurity risk, as well as the costs of procuring and supporting of information systems and devices. Thus, supply chain transparency can reduce cybersecurity risks and overall costs by:

- Facilitating the identification of vulnerable software to reduce cybersecurity risk;
- Reducing unplanned downtime through the identification of software vulnerabilities and defects;
- Supporting more informed purchasing decisions and market differentiation of system and device manufacturers with strong software development programs; and

[1] https://www.ntia.doc.gov/files/ntia/publications/ntia_framing_wg_deliverable_0.1_06.25.pdf

- Identifying suspicious or counterfeit software components.

Purpose and Objectives

Coming out of the June 2018 NTIA face-face working session, various workgroups were convened to examine different aspects of software transparency, including the workgroup leading the SBOM PoC, which sought to demonstrate that MDMs and HDOs could successfully leverage SBOMs across several use cases, with a goal of demonstrating the value SBOMs would provide to reducing the risks associated with medical devices. As the FDA has articulated, "ensuring medical devices are safeguarded from cyber intrusions is a shared responsibility across the medical device ecosystem."[2]

The PoC participants recognized the need for the PoC to align with existing standards utilized for SBOM generation, and, for the evaluative use cases align with those found in other industry verticals. To this end, high-level objectives of the PoC included:

- MDM generation and publication of SBOMs for actual medical devices in use at participant HDOs;
- HDO consumption of the SBOMs across use cases reflective of current acquisition and management of medical devices;
- Evaluation of the SPDX and SWID as SBOM formats to identify opportunities for enhancement and potential obstacles to real world utilization of these standards; and
- Opportunities for future evaluative efforts, with an eye towards SBOMs being a component of collaborative efforts to secure the medical device ecosystem.

Scope

Before beginning to plan the proof of concept in detail, the participants defined what was in scope for the proof of concept and what was out of scope. By doing this, the participants were able to identify the aspects important to demonstrate the proof of concept, and others that would be resolved by future work, if at all. In two cases items that were originally in scope later were changed to be out of scope either because it would mean resolving issues that were not easily addressable in a reasonable period or because they were subsequently identified as unnecessary to complete the proof of concept.

In Scope

The following items were considered in scope for the PoC:

- Conforming to a standard format – Rather than creating a new format to be used by the participants, it required less work and was expected to be more compatible with existing tooling, to use already-established format(s). Both SWID and SPDX were used, even though in both cases the specific use of those formats needed to be resolved to convey the intended information in the SBOM.
- Component dependencies – Providing dependency information, especially past the first hop, was considered a difficult problem for MDMs to resolve. For the proof of concept, this would be provided on a "best effort" basis by the MDMs, which would represent the real world.
- Component supplier name – This was identified as an essential element to be included in the SBOM and should be provided by MDMs if it could be determined.

[2] https://www.fda.gov/NewsEvents/Newsroom/FDAVoices/ucm624749.htm

- Component version number – Providing version numbers in as great a level of detail as possible was considered to be essential, up to and including the build number. It was left to the MDM to determine what level of detail was available in each case.
- Delivery over the internet by HDO pull – To model the real-world use of SBOMs the HDOs would pull the data from a repository as required. Ultimately a cloud file share was used for this purpose, although API access was originally proposed.

Out of Scope

The following items were considered out of scope for the PoC:

- Inclusion of hardware in the BOM – This would have made the BOM a cybersecurity BOM, or CBOM (as coined by the FDA), instead of an SBOM. Including hardware would have presented some difficult problems in identifying and specifying hardware —immaterial to completing the proof of concept.
- Identifying a single standard format – The goal was to identify one or more formats that could be used to transport the information to the HDO rather than blessing any one particular format. As long as the data was successfully generated and consumed, the format used for transport was not important to resolve.
- Inclusion of vulnerability information in the SBOM – While vulnerability management was a clear HDO use case from the start, it was felt that providing information about vulnerabilities in the generated SBOM would not reflect how this information would be provided in the future. It was important that the HDOs be able to identify the vulnerabilities associated with the components at any time after the SBOM was delivered, which modeled the anticipated real world SBOM use.
- Globally unique component identifiers – While this was seen as critical to the widespread use of SBOMs, resolving how to do this was a genuinely hard problem — one that was already taken up by other working groups — that could explode the proof of concept.
- Component context – Providing a method to convey to the SBOM consumer that, although the component may be included in the medical device, it wasn't being used in a way that presented any cybersecurity vulnerability, was originally in scope, but it was quickly realized that providing this information in the SBOM was challenging both conceptually and in representing that information in the formats used. Ultimately it wasn't necessary to completing the proof of concept.
- Programmatic access to the SBOM data – Providing a mechanism (e.g., an API) that would allow HDOs to pull the SBOM directly from some repository maintained by the MDM was originally in scope but was dropped because it wasn't essential to the proof of concept and would add complexity both for the MDM and the HDO.

Use Case Descriptions

This section lists all the activities identified by the group that apply for the use cases. Not all activities were exercised in the PoC.

Procurement

Activity	PoC Status
Identifies unsupported or vulnerable software so HDOs can initiate alternative mitigations or controls	Exercised
Informs asset management via identification of potential cybersecurity concerns	Exercised
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.)	Partially exercised (unsupported end-of-life software was not automatically identified, but manual analysis was performed)
Lifecycle management (understanding of current supported and unsupported software) for new devices and those already in the field	Partially exercised (unsupported end-of-life software was not automatically identified, but manual analysis was performed)
A reduction of the number of questionnaires that have to be filled out as the SBOM can supplement the MDS2	Not exercised
Awareness regarding the introduction of customized software into the IT system	Not exercised (custom software was not easily identified)
Awareness regarding the presence of interfaced or system conflicts with the health IT system, etc.	Not exercised

Asset Management

Activity	PoC Status
Actions that can be taken to protect the asset by providing sufficient details for each component	Exercised
Assisting HDOs in standardizing risk assessment for asset management	Exercised
Providing insight into end of life and aid in end of life planning for software and devices	Partially exercised (unsupported end-of-life software was not automatically identified, but manual analysis was performed)
Asset inventory when SBOM changes/updates are communicated to HDOs	Not exercised
Awareness regarding the introduction of customized software into the IT system	Not exercised (custom software was not easily identified)
Awareness regarding the presence of interfaced or system conflicts with the health IT system, etc.	Not exercised
Reduction of the number of questionnaires that have to be filled out as the SBOM can supplement the MDS2	Not exercised

Risk Management

Activity	PoC Status
Assessment of a new product being added to the hospital network prior to integration (determining potential risk of a device before adding it to the network)	Exercised
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)	Exercised
Monitoring of HDO inventory against new vulnerabilities as they emerge	Exercised
Identifies unsupported or vulnerable software so HDOs can initiate alternative mitigations or controls	Partially exercised (Unsupported End-of-life software was not automatically identified, but manual analysis was performed)
Lifecycle management (understanding of current supported and unsupported software) for new devices and those already in the field	Partially exercised (Unsupported end-of-life software was not automatically identified, but manual analysis was performed)

Vulnerability Management

Activity	PoC Status
Assessment of a new product being added to the hospital network prior to integration (determining potential risk of a device before adding it to the network)	Exercised
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)	Exercised
Identifying unsupported software so you can initiate alternative mitigations or controls	Exercised
Monitoring of HDO inventory against new vulnerabilities as they emerge	Exercised
Lifecycle management (understanding of current supported and unsupported software) for new devices and those already in the field	Partially exercised (unsupported end-of-life software was not automatically identified, but manual analysis was performed)
Assisting HDOs with proactive security activities such as supplemental network scanning and supplemental organizational penetration testing	Not exercised

Overview of PoC Execution

The PoC execution use-case activities were designed to capture the valuable components of the SBOM creation and integration processes to evaluate the execution, intakes efforts, and opportunities for developing future standard practices. A working group of MDM and HDO organizations focused on how to properly scope and execute this PoC to clearly understand how well their SBOM development tools

and integration processes fit relative to their functional requirements, challenges, and to identify key opportunities for further developments in support of SBOM industry best practices.

High-level description of participant roles and responsibilities

NTIA – Provide input on PoC objectives and requirements to synthesize the outcomes with associated SBOM working groups.

HDO - Provide input on PoC objectives and requirements and feedback on their SBOM integration processes fit relative to their functional requirements. Also aid in development of the use case definitions and draft final report

MDM - Provide input on PoC objectives and requirements and feedback on their SBOM creation process, development tools, and integration processes. Also aid in development of the use case definitions and draft final report.

Workgroup contributors: Provide input on PoC objectives and requirements, aid in development of the use case definitions, and draft final report.

PoC High-Level Activities

Key Activities	Primary Contributors
• Weekly meetings over 12 months	HDO, MDM, NTIA, WG Contributors
• Held three face-to-face associated SBOM working groups meetings.	HDO, MDM, NTIA, WG Contributors
• Develop PoC scope, objectives and requirements	HDO, MDM, NTIA, WG Contributors
• Continuously align PoC objectives and requirements to synthesize the outcomes with associated SBOM working groups.	HDO, MDM, NTIA, WG Contributors
• Produce MDM specific install base list	HDO
• Align HDO install base with SBOM creation	MDM
• Define SBOM integration use cases and processes review scope relative to their functional requirements.	HDO
• Creation of SBOM (SWID and SPDX)	MDM
• Implement PoC SBOM use cases to their functional requirements.	HDO
• Develop MDM SBOM use case questionnaire to align outcomes.	MDM
• Develop HDO SBOM use case questionnaire to align outcomes.	HDO
• Develop and finalize the PoC Use Case report	HDO, MDM, NTIA, WG Contributors

Methodology Section for the PoC

The execution methodology framework for this PoC focused on the premise that the participating MDM's have the knowledge and ability to create a SBOM for one or more of their products within the HDO's assets inventory. Secondly that HDO's have the knowledge, processes, and platforms to intake an SBOM. From this premise, two primary working groups formed to execute a SBOM creation use case and a SBOM intake use case. The outcomes of these use cases are captured from the working groups in the form of feedback questionnaires.

Execution Methodology and Framework

- Working groups
- MDM creation working group
- HDO SBOM intake working group
- SBOM PoC working group

SBOM Creation MDM Use Case

The SBOM MDM creation use case working group was tasked to create SBOMs using their established processes and deliver those SBOMs to the HDO's for intake. Each MDM worked separately to create their SBOMs. MDM's shared experiences and focused on creating like SBOMs (format and content).

SBOM Intake HDO Use Case

The HDO SBOM Intake Use Case working group was tasked to simulate the ingestion, processing, and analysis of the SBOM. Each HDO exercised this simulation utilizing their configuration management databases (CMDB), security information and event management (SIEM) systems, vulnerability scanners, and custom-developed software tools. HDO's shared experiences, successes, challenges, and lessons learned.

SBOM PoC Working Group

The SBOM PoC working group was task to develop and report on the PoC by establishing and describing the approach, objectives, concerns, conditions, settings, establish guidelines and outcomes.

Overview of PoC Findings

SBOM Generation

The initial scope was defined by the HDOs providing an inventory of existing biomedical devices by manufacturer. This information was then provided to the respective MDMs. A small number (1 to 2) of the devices in the inventory were then selected by the MDMs for the purposes of executing the PoC. The generation of the SBOM differed slightly between the MDMs but predominantly relied on a combination of both manual and semi-automated processes, often leveraging common scripting languages and/or existing software composition analysis tools to support the generation. Throughout the creation of the SBOM, a collaborative and iterative approach was utilized by the MDMs with the intention of aligning the file format prior to delivery to the HDOs. The lack of a standard naming convention for attributes such as "software identity name" and "supplier name" resulted in the MDMs relying on commonsense or reasonable names for the components. Despite these challenges, the MDMs were successful in the generation and did not deviate from the PoC timeline.

For this proof-of-concept, the MDM participants generated medical device SBOMs containing the following information:

1. Author, composed of:
   - *Created By*
   - *When Created*
   - *Creator Comments*
2. SBOM Document Name
3. List of SBOM Components, composed of the following information for each included component:

- *Component Name*
- *Version*
- *Component Supplier*
- *Identifier*
- *Download Location*
- *Files Analyzed*
- *License*
- *Copyright Text*

Both manual and automated approaches were used to generate the SBOM. Some MDMs did not have the internal systems available to automate the generation of the SBOM, although all MDMs had internal processes to capture the data. When generating a medical device SBOM, information may have to be collected from multiple sources. The open source and COTS components integrated into the proprietary applications built by the MDM can be retrieved through the software build and associated documentation. However, the components included as part of the hardware platform, such as the operating system and database, may have to be obtained through other sources, such as device specifications. Thus, complete automation for the generation of a medical device SBOM may have to account for multiple data sources. When MDMs used automation, they first used a manual process to gather information and then leveraged automated to format the data based on the content specifications.

Currently, there are no authoritative sources to obtain the values for the *Component Name*, *Version*, and *Supplier*. For the PoC, the MDMs took a best-effort approach for defining these values. Thus, the MDMs may have different values in their medical device SBOM for the same component. In the production version of an SBOM, it will be important for authors to have a clear and consistent mechanism for identifying this information.

The Package URL (purl) syntax was used for the component identifier, which was based on a combination of the *Component Name* and *Version* using the following purl construct:

> pkg: commonname/<component name@<component version

It is possible to improve this definition by including the optional “namespace” in the construct, and using the *Component Supplier* name as follows:

> pkg: commonname/<component supplier name/<component name@<component version

Using this syntax should result in a unique and consistent identifier for the components.

The *Download Location*, *Files Analyzed*, *License*, and *Copyright Text* elements were optional for the PoC. MDMs noted that the values for these fields were not readily available in the SPDX database, and were only provided if time permitted to locate the information.

For the PoC, no MDM provided dependency information. This is challenging information to extract and complicated to retrieve. The MDMs were uncertain if dependency information is required for HDO risk management.

The SBOM format used for the PoC did not support providing the identification information for the medical device the SBOM described. Therefore, MDMs provided this through additional documentation included with the SBOM file. An observation from the PoC was that the same information used to define an SBOM component could also be included in the SBOM to clearly identify the medical device. Essentially, this could be applied to any SBOM to provide SBOM authors with the information they need when creating an SBOM component list.

MDMs provided their SBOM in an SPDX and/or SWID format. It was necessary for the working group to agree on a specification for each format based on the SBOM content selected for the PoC. The variability and flexibility of the two formats required establishing a constrained specification for consistency across the SBOMs.

For the PoC, it was not necessary to manage versions of an SBOM or to manage multiple versions of a medical device and associated SBOMs. These are important considerations that should be addressed throughout the medical device lifecycle. During a discussion of this topic, it was determined that MDMs would need to have different SBOM versions for each medical device version because one or more proprietary, COTS, or open source components would have changed.

SBOM Consumption

Both the HDOs and MDMs identified medical device SBOM cybersecurity benefits throughout the biomedical device procurement process, within general asset management, as part of routine enterprise risk management activities, and as a supplemental component to existing vulnerability management practices. The generation, distribution, ingestion, processing, and analysis of the SBOM was conceptualized and executed with respect to these use cases, leveraging configuration management databases (CMDB), security information and event management (SIEM) systems, vulnerability scanners, and custom-developed software tools. Although the SBOM was successfully generated in both SWID and SPDX machine-readable formats, the following use case findings largely represent the ingestion and analysis of the SWID file format. Throughout the PoC, successes, challenges, and lessons learned were documented and reported to all working groups and participants in the NTIA Software Component Transparency effort.

The primary challenge in all of the use cases was the lack of a standard universal resource identifiers (URIs) for the SBOM attributes. Manual mappings had to be performed, which increased the overall subjectivity of the exercise and ultimately resulted in varying levels of correlation success across the HDOs. Additionally, there was no authoritative “software end-of-life database”, nor was custom software easily identifiable without manual intervention or the creation of custom queries. As such, these attributes did not factor into the overall risk profile of the device created during the PoC. Similarly, although specific software name and version information was denoted, patch status (i.e. listing of operating system KBs installed) was absent, which would need to be identified using alternate methods. Lastly, the completeness of the information provided in the SBOM was accepted “as is” during the PoC; however, the HDOs unanimously noticed the absence of a defined audit or validation process to confirm the accuracy and completeness of the information provided.

Procurement Use Cases

Once generated, files were shared using an online collaboration tool; however, future distribution channels may include device-initiated API delivery, web accessible customer portals, or the SBOM being included as a separate file on the device. The SBOM was not imported directly into any procurement tools; however, the ingestion and subsequent correlation and analysis of the SBOM was able to be performed quickly through the usage of either a SIEM or a custom script. Leveraging these supplemental technologies, it is the expectation of the HDOs that this SBOM analysis step would not materially impede procurement activities.

Post-ingestion, this data was correlated with existing National Vulnerability Database (NVD) data using the aforementioned analysis tools to identify known vulnerabilities in the software components contained within the device. This known vulnerability information was used to supplement existing data and documentation (i.e., self-assessment questionnaires, manufacturer disclosure statement for medical device security (MDS2)) to develop a comprehensive risk profile. Identification of known vulnerable components was quickly performed by all of HDOs. Ideally, end-of-life software was to be identified during this analysis, but the HDOs were unable to locate a comprehensive end-of-life database to

correlate with the parsed SBOM data. Consensus amongst the HDOs was that custom queries could reasonably be used to identify known end-of-life components across SBOMs; however, this data would need to be collected from multiple sources or generated manually and validated. Due to the PoC timelines, the analysis of end-of-life components was largely deemed out of scope.

It was determined that the rapid identification of devices with known vulnerable components during procurement would likely support the identification of appropriate compensating controls prior to implementation. For example, a compensatory control such as network isolation could be judiciously proposed towards the beginning of the procurement lifecycle, resulting in more focused architecture, design, and roadmap discussions between the HDOs and the MDMs.

Areas for improvement were quickly recognized throughout the procurement use case and included the accompaniment of an XML Schema Definition (XSD) file alongside the SBOM to assist in parsing the data, as well as including part type in the SBOM file, the latter of which currently exists as part of the Common Platform Enumeration (CPE) database.

Asset Management Use Cases

Asset Management Use Case Findings – General

The HDOs explored the usage of their respective CMDBs as an ingestion point for the SBOM; however, it was determined that the current implementation of these systems was not configured to adequately import or map the parsed SBOM data. Customization could be performed or tooling could be developed to support this, but this was not explored further due to the time limitations of the PoC. Subsequent to this conclusion, the HDOs did engage with their corresponding CMDB vendors and were successful in generating vendor interest into this exercise.

Asset Management Use Case Findings – Risk Management

Similar to the procurement use case, the SBOM was not consumed directly into any dedicated risk management tools. Nevertheless, it is reasonable to acknowledge that governance, risk, and compliance solutions can accept post-analysis SBOM data for ongoing risk management purposes. It is the expectation of the group that this data could be retrieved using either batch import or via API, after which it can be correlated to specific configuration items (CI) or risk registries.

Ongoing monitoring of devices against newly discovered vulnerabilities is practical in concept; however, due to the timeline of the PoC, the HDOs did not cover the long-term risk management of the devices. The frequency of NVD updates supports this concept, as vulnerability information is routinely updated no less than daily. The HDOs leveraged the Common Vulnerability Scoring System (CVSS), which provides end users with both principal characteristics of the vulnerability as well as a quantitative, numerical score to represent impact (none, low, medium, high, and critical).

An identified limitation of the SBOM is configuration vulnerabilities, as these cannot reasonably be represented on the SBOM files. Configuration risks would likely be identified through device testing or manually, but could be recognized and tracked alongside the SBOM data on a risk management platform. Although initially identified in the procurement use case, the lack of a standard naming convention was persistent and impacted the risk management use case, as well.

Asset Management Use Case Findings – Vulnerability Management

The Vulnerability Management (VM) use case yielded findings that were consistent with general asset management, procurement, and risk management; however, this use case highlighted the potential for some unique testing and exploitation scenarios. Although existing enterprise vulnerability management practices across the HDOs were largely unaffected by the introduction of the SBOM, the Vulnerability Management teams noted that access to this data provided visibility into some unique attack vectors

which could be used for research, demonstration, and offensive security purposes. Additionally, the SBOM risk profile information can be combined with existing vulnerability scan results to provide a more holistic view of the attack surface of the device, as well as highlight lesser known vulnerabilities throughout the dependent components.

PoC Observations

The POC participants made the following observations in relation to the use of the SBOMs utilizing the SWID and SPDX formats. The observations are generalized, and intended to inform the broader stakeholder communities' efforts as to the general use of SBOMs, enhancements to existing standard formats, and to inform future usage in the healthcare setting.

Strengths	**Weaknesses**
• The HDOs were successful in accessing, importing/ingesting, and parsing the SBOM data into systems that were able to query the SBOM data independently and correlate the data with external resources to perform both quantitative and qualitative analysis. • MDM's produced both SWID and SPDX formats • HDO's and MDM's identified SBOM cybersecurity benefits throughout the procurement process, asset management, risk management, and vulnerability management practices.	• Conforming to a standard format • Medical devices from different MDMs may have different values in their medical device SBOM • CMDB does not have import or map the SBOM data tool • Currently, there are no authoritative sources to obtain the values for the Component Name, Version, and Supplier • Dependency information challenging one to extract and complicated to retrieve • Limitation of the SBOM configuration vulnerabilities • Patch status
Opportunities	**Threats**
• Inclusion of hardware in the bill of materials • Identifying a single standard format • Inclusion of vulnerability information in the SBOM • Globally unique component identifiers • Component context • Programmatic access to the SBOM data • Analysis of end-of-life components • Accompaniment of an XML Schema Definition (XSD) file alongside the SBOM to assist in parsing the data • Distribution channels, API delivery, web accessible customer portals, file on the device	• Lack of a standard universal resource identifiers (URIs) for the SBOM attributes • Absence of a defined audit or validation process to confirm the accuracy and completeness of the SBOM information provided

Conclusion

The Healthcare SBOM PoC demonstrated that software bills of material can be successfully produced by medical device manufacturers, as well as consumed by healthcare delivery organizations. The information contained in the SBOMs produced for the PoC provided software transparency that previously was not available to the HDOs, and improved their overall risk management and operational approaches. The PoC also demonstrated that industry-agnostic standard formats can be leveraged by the healthcare vertical, and industry-specific formats are unnecessary. Additionally, the PoC's findings should inform the cross-industry efforts to improve software transparency spearheaded by the National Telecommunications and Information Administration.

Participants in the PoC have discussed a second proof of concept, one which would involve additional MDM and HDO participants, as well as incorporating lessons learned during this initial effort. This second proof of concept could also include participation by non-MDM and HDO third-parties, with the recognition that an ecosystem will ultimately be required to support the on-going development, publication, consumption and maintenance of SBOMs.

Acknowledgements

The following individuals constitute the membership of the WG who were responsible for development of the Healthcare Proof of Concept (PoC). WG leadership and those medical device manufacturers and healthcare delivery organizations that directly participated in the PoC are highlighted.

- Working Group Co-Chair, Jennings R. Aske, Senior Vice President & Chief Information Security Officer, NewYork-Presbyterian
- Working Group Co-Chair, Jim Jacobson, Chief Product and Solution Security Officer, Siemens Healthineers

PoC Participants:

- Jonathan Bagnall, Sr. Manager, Product Security & Services Office, Philips
- Michael Dittamo, Information Security Risk Manager, NewYork-Presbyterian
- Les Gray, Director of Product Cybersecurity, Abbott
- Edwin Heierman, Senior Product Cybersecurity Architect, Abbott
- Kevin McDonald, formerly Director of Clinical Information Security, Mayo Clinic
- Michael C. McNeil, Head of Product Security & Services Office, Philips
- Amusan Odutola, Senior Cybersecurity Analyst, Mayo Clinic
- Perumal Poopathy, Product & Solution Security Expert, Siemens Healthineers
- Mike Powers, Clinical Engineering Supervisor, Christiana Care
- Harbakshish Singh, Program Manager for Medical Device Security, Cedars-Sinai Health System
- Timothy Walsh, Principal Information Security Analyst, Mayo Clinic

Working Group Contributors:

- Seth Carmody, Cybersecurity Project Manager, Center for Devices and Radiological Health (CDRH) at US Food and Drug Administration
- Chris Clark, Principal Security Engineer, Synopsys
- Jim Covington, Head of Global Security and Privacy at Capsule Technologies, Qualcomm
- Anita Finnegan, Founder & CEO, Nova Leah
- Allan Friedman, Director of Cybersecurity Initiatives at US Dept. Commerce, NTIA
- Robert Haack, Senior Manager Product Security and Data Privacy, Karl Storz
- Zack Hornberger, Director of Cybersecurity & Informatics, Medical Imaging Technology Association
- Joseph Jacques, Principal Engineer, Boston Scientific
- Robert Jarrin, formerly Senior Director of Wireless Health Public Policy, Qualcomm
- Michelle Jump, Vice President of Cyber Program Initiatives, Nova Leah
- Kent Landfield, Chief Standards and Technology Strategist, McAfee

- Joern Lubadel, Director of Marketing, Healthcare IT Solutions, B. Braun USA
- Art Manion, Senior Vulnerability Analyst, CERT/CC
- Aftin Ross, Senior Project Manager, CDRH at US Food and Drug Administration
- Dana-Megan Rossi, Assoc. Director for Product Security Policy, Strategy & Incident Response, Becton Dickinson
- Zach Rothstein, Vice President, Technology and Regulatory Affairs, AdvaMed
- Brian Scarpelli, Senior Policy Council, Actonline
- Eirene Shipkowitz-Smith, Business Information Security Officer, Baxter
- Nick Sikorski, Manager, Deloitte Cyber
- Kate Stewart, Sr. Director of Strategic Projects, Linux Foundation
- Craig Spiezle, Owner, Agelight
- Andrew Suter, Sr. Manager/Principal Security Response Analyst, BlackBerry
- Betty Tsao, Director IT Medical SW & Medical Device Security, Varian
- Chad Waters, Senior Cybersecurity Engineer/Senior Project Officer, ECRI Institute
- Ashley Woyak, formerly Business Information Security Officer, Baxter Healthcare Corporation
- Beau Woods, Cyber Safety Advocate, I Am the Cavalry
- Kenneth Zalevsky, Director of Informatics Research, Bayer

The Working group would also like to thank all of the individuals and organizations within the NTIA SBOM WG's that provided feedback along the way which helped to inform the POC activities.

A special thank you goes to Aftin Ross, Senior Project Manager, CDRH at US Food and Drug Administration, who led the working group in the development of this report.

Definitions

Application Program Interface (API): the set of public functions provided by an executable application component for use by other executable application components (*IEC 61970-301, ed. 5.0 I* (*2013-12*)).

Attack Vector: the path or means by which an attacker or malicious program can gain access to a computer-based system (*IEC 62645, ed. 1.0* (*2014-08*)).

Asset Management: the process of identifying and protecting hardware and software devices that could be used by attackers as a platform from which to extend compromise of the network to be mitigated. (adapted from definition of "software asset management", *NISTIR 8011 Vol. 1*).

Configuration Management Database (CMDB): a database that contains all relevant information about activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. (adapted from definition of "configuration management", *NIST SP 800-53 Rev. 4*).

Commercial Off the Shelf (COTS): software and hardware that already exists and is available from commercial sources (*NIST SP 800-161*).

Compensating Control: the management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in *NIST Special Publication 800-53*, that provide equivalent or comparable protection for an information system (*NIST SP 800-37 Rev. 1*).

Common Platform Enumeration (CPE): a security content automation protocol specification that provides a standard naming convention for operating systems, hardware, and applications for the purpose of providing consistent, easily parsed names that can be shared by multiple parties and solutions to refer to the same specific platform type (*NIST SP 800-128*).

Common Vulnerabilities and Exposures (CVE): a nomenclature and dictionary of security-related software flaws. (*CNSSI 4009-2015* (*NIST SP 800-126 Rev. 2*)).

Common Vulnerability Scoring System (CVSS): a system for measuring the relative severity of software flaw vulnerabilities. (CNSSI 4009-2015 (NIST SP 800-126 Rev. 2))

Component: unit of software defined by a supplier at the time the component is built, packaged, or delivered (NTIA Framing Group Report). A product is a component. So is a library. So is a single file. So is a collection of other components, like an operating system, office suite, database system, car, an ECU in a car, a medical imaging device, or an installation package like an ".rpm" file. In SPDX terms package, file, and snippet map to "component." In SWID terms … source is not excluded, but is not the primary focus. Also referred to as: Software Component.

Dependency: relationship between two elements in which a change to one element (e.g., the server) may affect or supply information needed by the other element (e.g., the client) (*ISO/IEC 14776-414, ed. 1.0* (*2009-06*)).

Supplier: entity that creates, defines, and identifies components and produces associated SBOMs (NTIA Framing Group Report). A supplier may also be known as a manufacturer, vendor, developer, integrator, maintainer, or provider. Ideally, all suppliers are also authors of SBOMs for the suppliers' components.

End of Life (End-of-life): discontinuance of production by the original manufacturer. End-of-life should not be confused with 'time to wear out' or 'end of use' (*IEC 62402, ed. 1.0*).

Exploit: is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or other (adapted from https://en.wikipedia.org/wiki/Exploit_(computer_security)).

Extensible Markup Language (XML): a flexible text format designed to describe data for electronic publishing. (*NISTIR 7250*).

Harm: injury or damage to the health of people, or damage to property or the environment (*IEC Guide 51:2014, 3.1*).

Hazard: potential source of harm (IEC Guide 51:2014).

Health Delivery Organization (HDO): an organization, or group of related organizations, that are involved with the delivery of healthcare services (custom definition).

Hop: the transfer of software or software components from one entity to another along the software supply chain (custom definition).

Manufacturer Disclosure Statement for Medical Device Security (MDS2): a form intended to assist professionals responsible for executing security risk assessments in their management of medical device security capabilities (*MDS2-2013*).

Mapping: set of values having defined correspondence with the quantities or values of another set (*IEC 61800-7-301, ed. 2.0*).

Medical Device Manufacturer (MDM): manufacturer of medical devices (*IEC 80001-2-3, ed. 1.0*).

National Vulnerability Database (NVD): the U.S. Government repository of standards-based vulnerability management data, enabling automation of vulnerability management, security measurement, and compliance (e.g., FISMA). (*CNSSI 4009-2015* (http://nvd.nist.gov))

Open Source: source code available to the general public with relaxed or non-existent copyright restrictions (*IEC 62279, ed. 2.0* (*2015-06*))

Procurement: process of obtaining services, supplies, and equipment (*IEC 62647-23, ed. 1.0*)

Persistent Uniform Resource Locator (PURL): web addresses or Uniform Resource Locators (URLs) that act as permanent identifiers (https://www.ifla.org/best-practice-for-national-bibliographic-agencies-in-a-digital-age/node/8790).

Risk: risk combination of the probability of occurrence of harm and the severity of that harm Note 1 to entry: The probability of occurrence includes the exposure to a hazardous situation and the possibility to avoid or limit the harm. (*ISO/IEC Guide 51:2014, 3.9*)

Risk Assessment: overall process comprising a risk analysis and a risk evaluation (*IEC 80001-2-1, ed. 1.0* (*2012-07*))

Risk Management: systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, and controlling risk. (*IEC 62304, ed. 1.0, amd. 1*)

Software Bill of Materials (SBOM): list of one or more identified components and other associated information (NTIA Framing Group Report). The SBOM for a single component with no dependencies is just the list of that one component. “Software” can be interpreted as “software system,” thus hardware (true hardware, not firmware) and very low-level software (like CPU microcode) can be included. Hardware is not excluded, but not the primary focus.

Security Information and Event Management (SIEM): the ability to gather security data from information system components and present that data as actionable information. (adapted from the definition of the term “Security Information and Event Management (SIEM) Tool”, *NIST SP 800-128*)

Software Identity Name: the unique name or identifier of a software package or software component (Custom definition)

Software Package Data Exchange (SPDX): an open standard for communicating software bill of material information (including components, license, copyrights, and security references) (https://spdx.org/)

Software Identification Tags (SWID tags): a set of structured data elements containing authoritative identification information about a software component. (*CNSSI 4009-2015* (*ISO/IEC 19770-2:2009*)

Total Product Lifecycle: activities occurring during a period of time that starts when software is conceived and ends when the software is permanently decommissioned (*IEC 61508-4, ed. 2.0* (*2010-04*))

Uniform Resource Identifier (URI): web standard syntax and semantic for identifying (referencing) resources (things, such as files, documents, images). (*IEC 61970-552, ed. 1.0*)

Unsupportable Software: software that is no longer receiving updates or patches from its original creator. (custom definition)

Version Number: identification number assigned to a version (*IEC 62507-1, ed. 1.0*)

Vulnerable Software: software that has one or more vulnerabilities. (custom definition)

Vulnerability: flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy (*IEC 62443-3-1, ed. 1.0* (*2009-07*))

Vulnerability Management: an ISCM capability that identifies vulnerabilities (Common Vulnerabilities and Exposures (CVEs)) on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network. (*NISTIR 8011 Vol. 1*)

XML Schema Definition (XSD): offers facilities for describing the structure and constraining the contents of XML documents, including those which exploit the XML Namespace facility. (https://www.w3.org/TR/xmlschema11-1/)