Software Bill of Materials

Transparency in the Software Supply Chain

Information Session for the Energy Community

January 26, 2021

Overview

- Background
  - The case for transparency
  - Why this is important
- What is an SBOM
  - Some of the work has already been done
  - A focus on the basics
- Why should we SBOM
  - Understanding the value
  - Use cases for the energy sector
- Some lessons from the other sectors' "proof of concept" exercises
- Next steps for the energy community

<u>Takeaways</u>:
**** SBOM will be an invaluable tool for managing cybersecurity and software supply chain risk.***
**** The energy and power community can safely experiment with this tool through a "proof of concept" exercise.***

Motivating Example #1

Amnesia:33 vulnerabilities impact millions of smart and industrial devices

Security researchers have identified 33 security flaws in four open-source TCP/IP stacks used across a wide range of smart products.

Motivating Example #1

Amnesia:33 vulnerabilities impact millions of smart and industrial devices

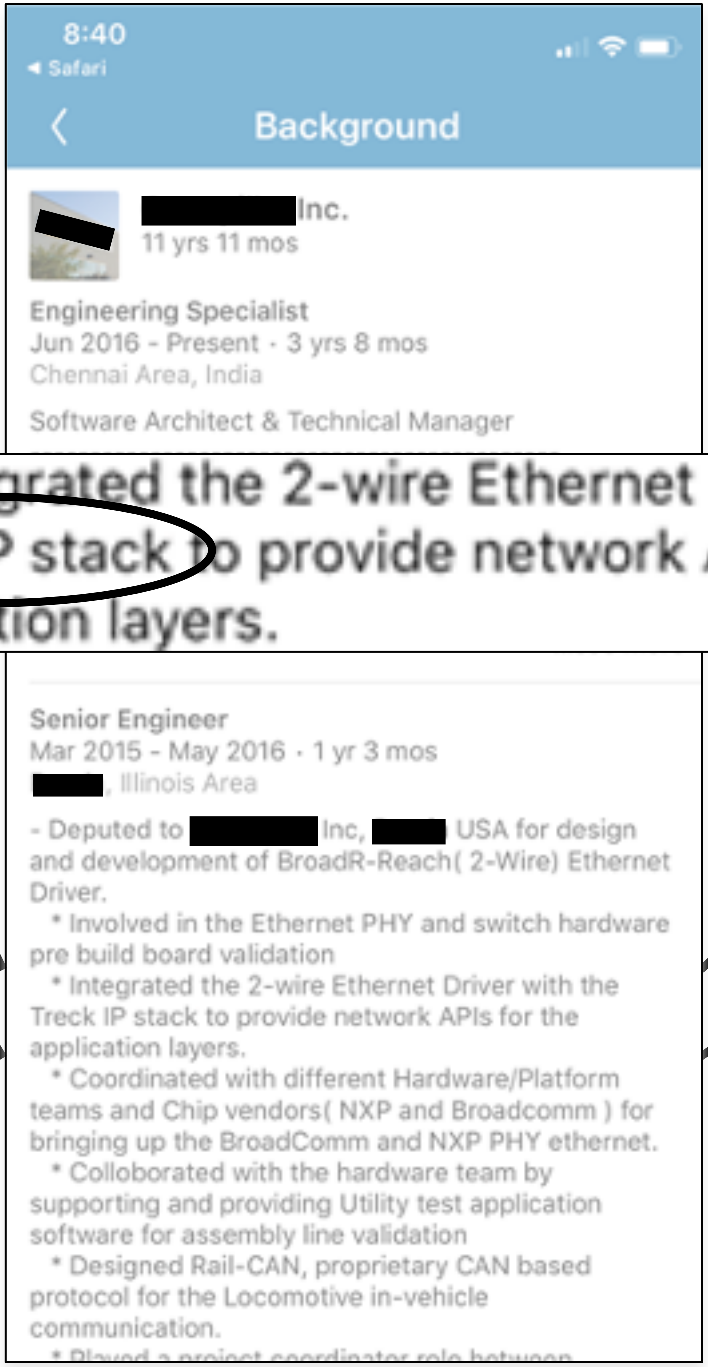
Security researchers have identified 33 security flaws in four open-source TCP/IP stacks used across a wide range of smart products.

Can any organization that makes or uses software easily answer:

Am I affected by $vulnerability ?

Motivating Example #2

Researchers at security firm JSOF were forced to scour LinkedIn to identify companies that might use the vulnerable Treck IP library to disclose Ripple20 risks.



8:40
◂ Safari

Background

[redacted] [redacted] Inc.
11 yrs 11 mos

Engineering Specialist
Jun 2016 - Present · 3 yrs 8 mos
Chennai Area, India

Software Architect & Technical Manager

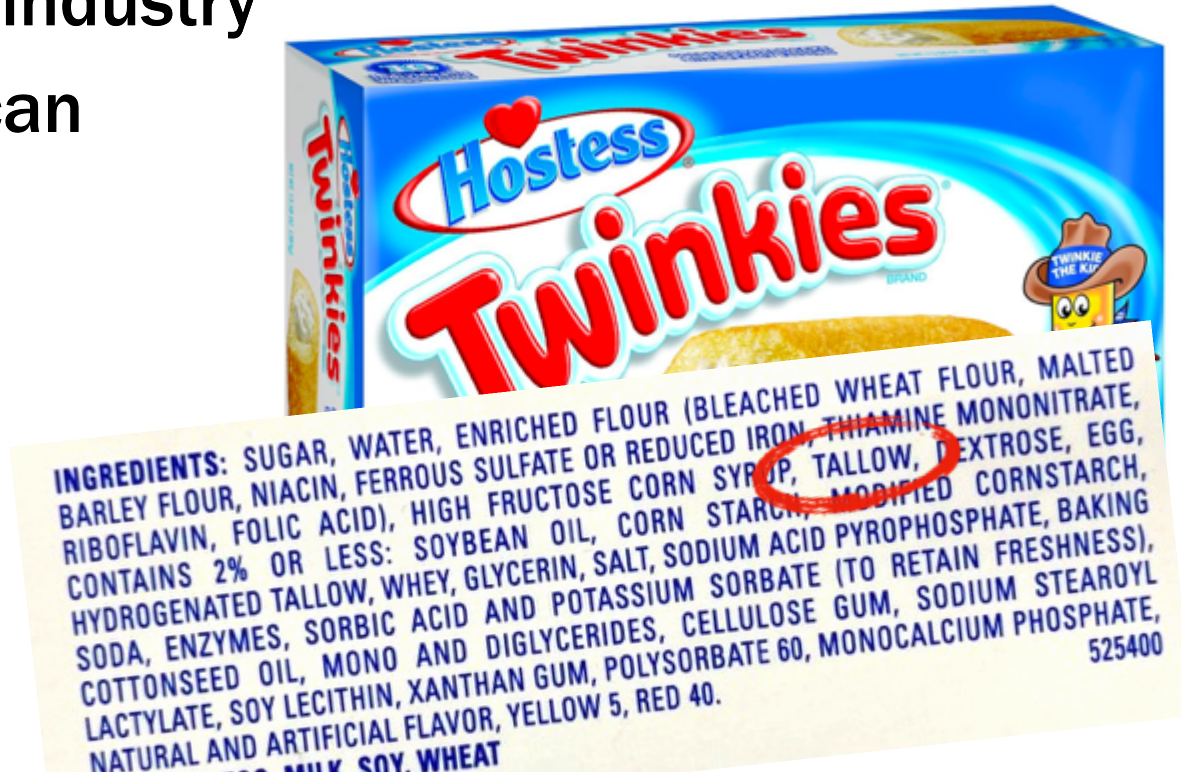
* Integrated the 2-wire Ethernet Driver with the Treck IP stack to provide network APIs for the application layers.

Senior Engineer
Mar 2015 - May 2016 · 1 yr 3 mos
[redacted], Illinois Area

- Deputed to [redacted] Inc, [redacted] USA for design and development of BroadR-Reach(2-Wire) Ethernet Driver.
 * Involved in the Ethernet PHY and switch hardware pre build board validation
 * Integrated the 2-wire Ethernet Driver with the Treck IP stack to provide network APIs for the application layers.
 * Coordinated with different Hardware/Platform teams and Chip vendors(NXP and Broadcomm) for bringing up the BroadComm and NXP PHY ethernet.
 * Colloborated with the hardware team by supporting and providing Utility test application software for assembly line validation
 * Designed Rail-CAN, proprietary CAN based protocol for the Locomotive in-vehicle communication.
 * Played a project coordinator role between

Transparency can help markets thrive

- Food ingredients and food labels
- Safety Data Sheets in the chemical industry
- Hardware Bills of Material (BOM) in industry
- Naming and tracking components can drive innovation (e.g. CVE)

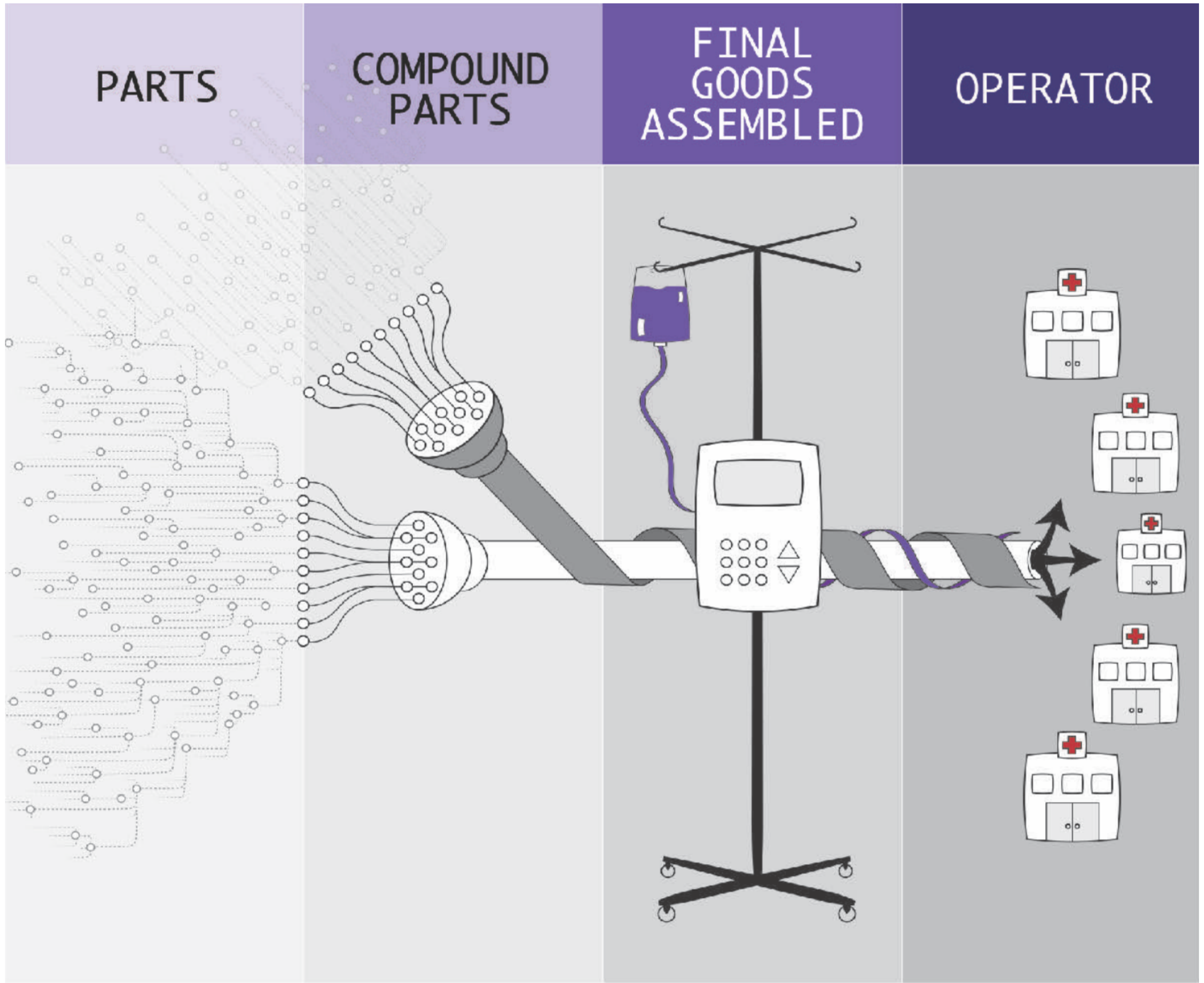


INGREDIENTS: SUGAR, WATER, ENRICHED FLOUR (BLEACHED WHEAT FLOUR, MALTED BARLEY FLOUR, NIACIN, FERROUS SULFATE OR REDUCED IRON, THIAMINE MONONITRATE, RIBOFLAVIN, FOLIC ACID), HIGH FRUCTOSE CORN SYRUP, TALLOW, DEXTROSE, EGG, CONTAINS 2% OR LESS: SOYBEAN OIL, CORN STARCH, MODIFIED CORNSTARCH, HYDROGENATED TALLOW, WHEY, GLYCERIN, SALT, SODIUM ACID PYROPHOSPHATE, BAKING SODA, ENZYMES, SORBIC ACID AND POTASSIUM SORBATE (TO RETAIN FRESHNESS), COTTONSEED OIL, MONO AND DIGLYCERIDES, CELLULOSE GUM, SODIUM STEAROYL LACTYLATE, SOY LECITHIN, XANTHAN GUM, POLYSORBATE 60, MONOCALCIUM PHOSPHATE, NATURAL AND ARTIFICIAL FLAVOR, YELLOW 5, RED 40.

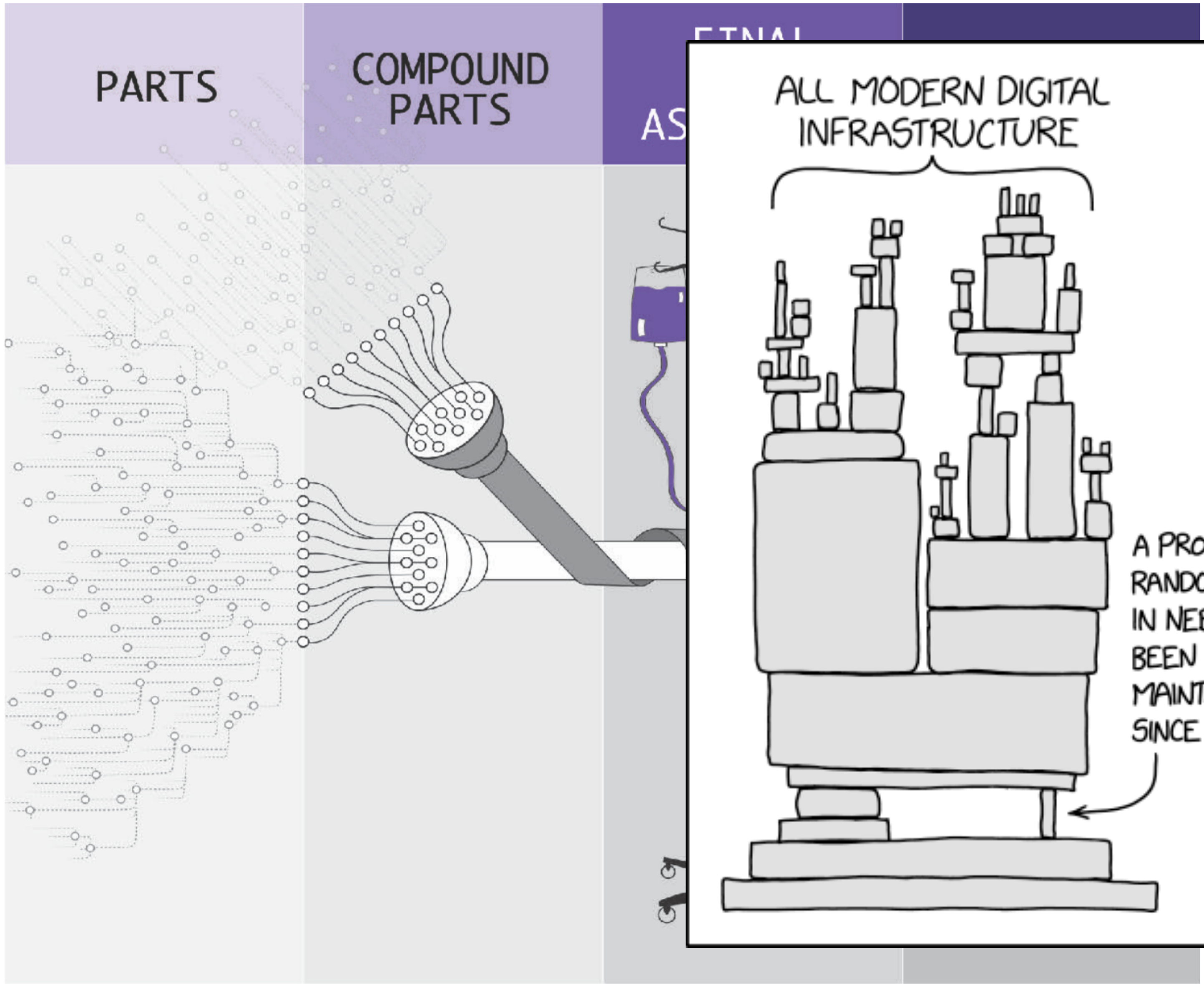
525400

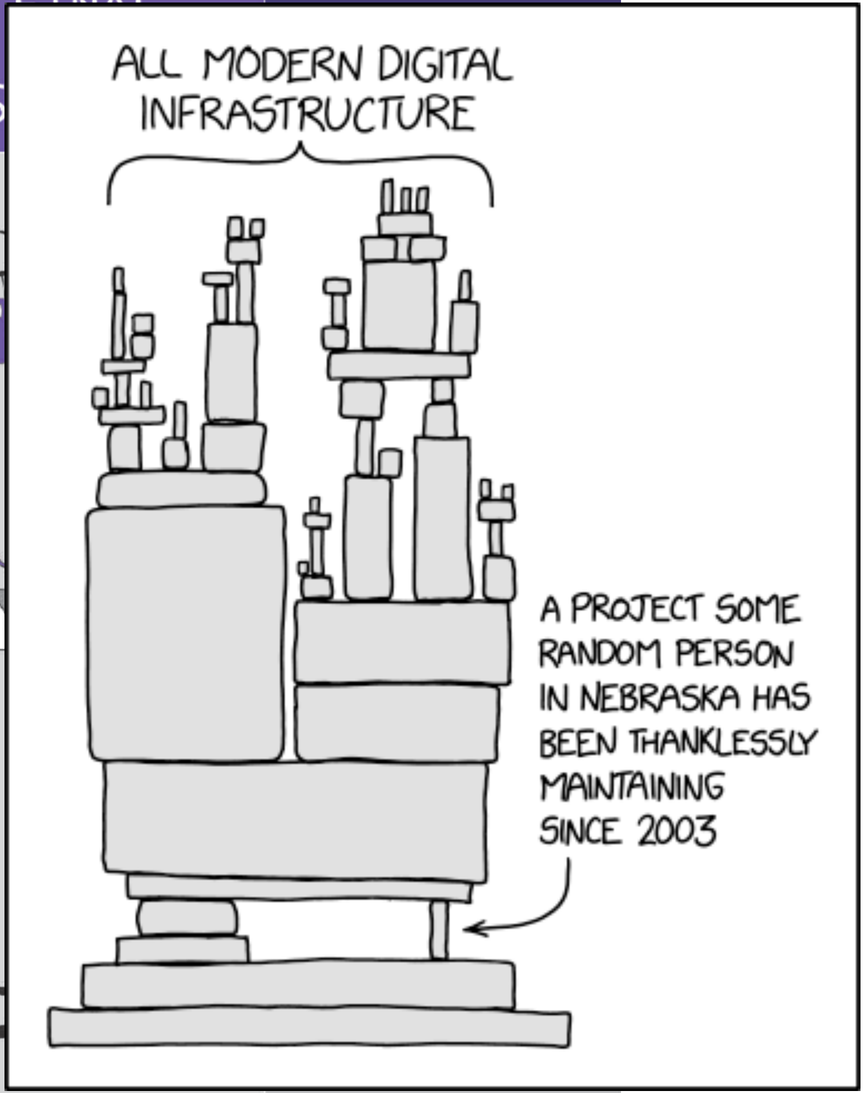
MILK, SOY, WHEAT

Software Supply Chain

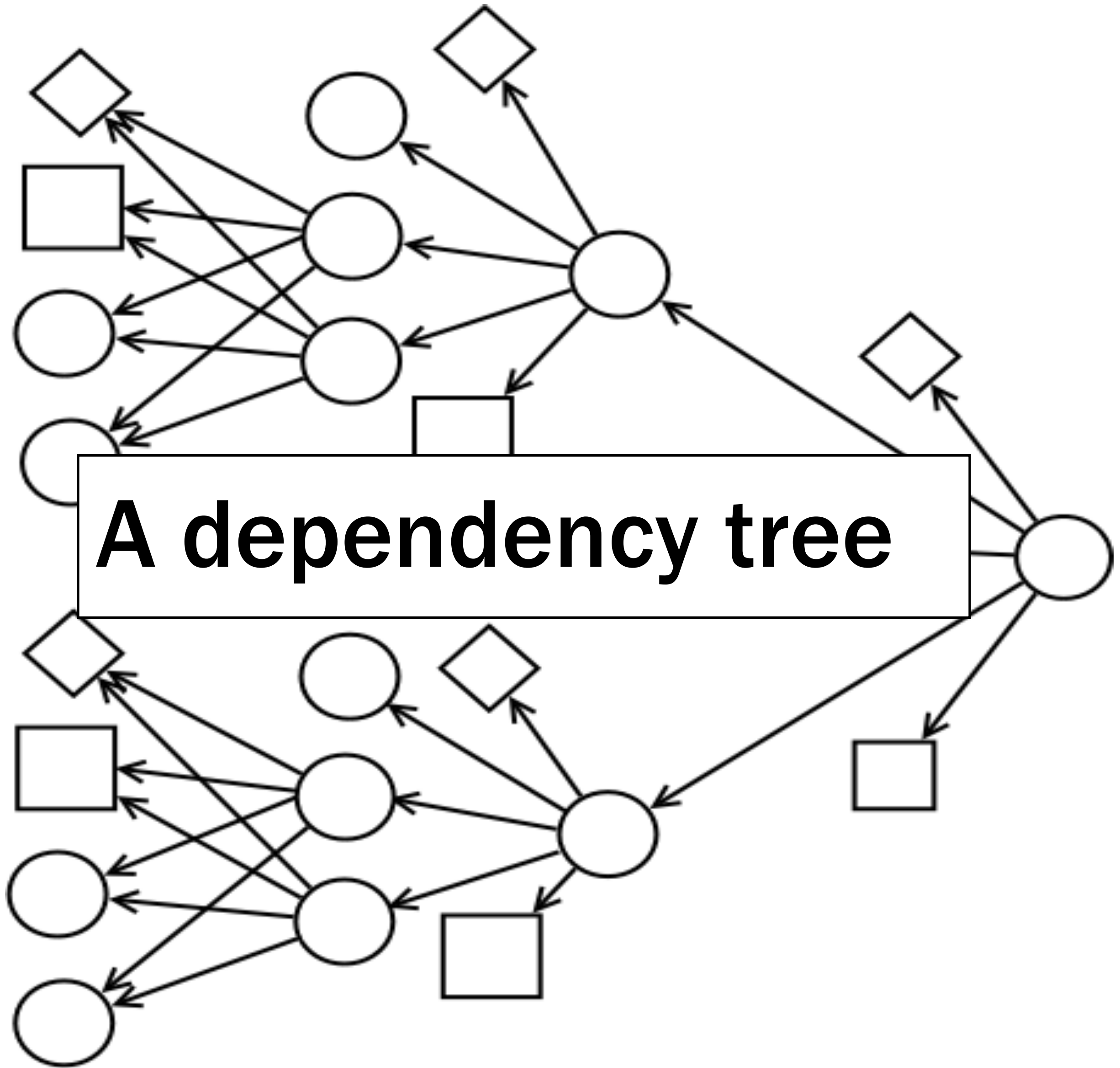


Software Supply Chain



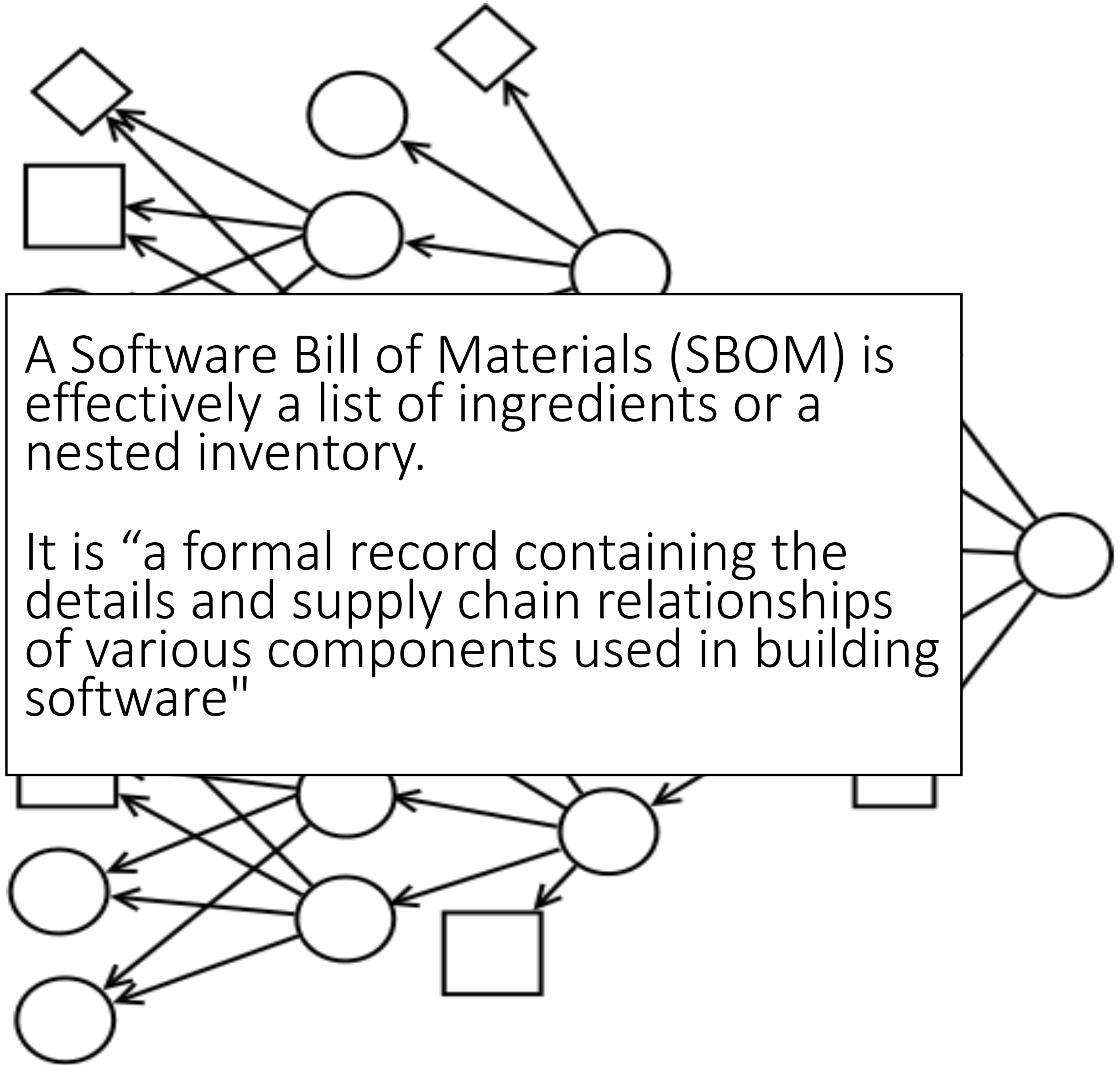

ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

What is an SBOM?



A dependency tree

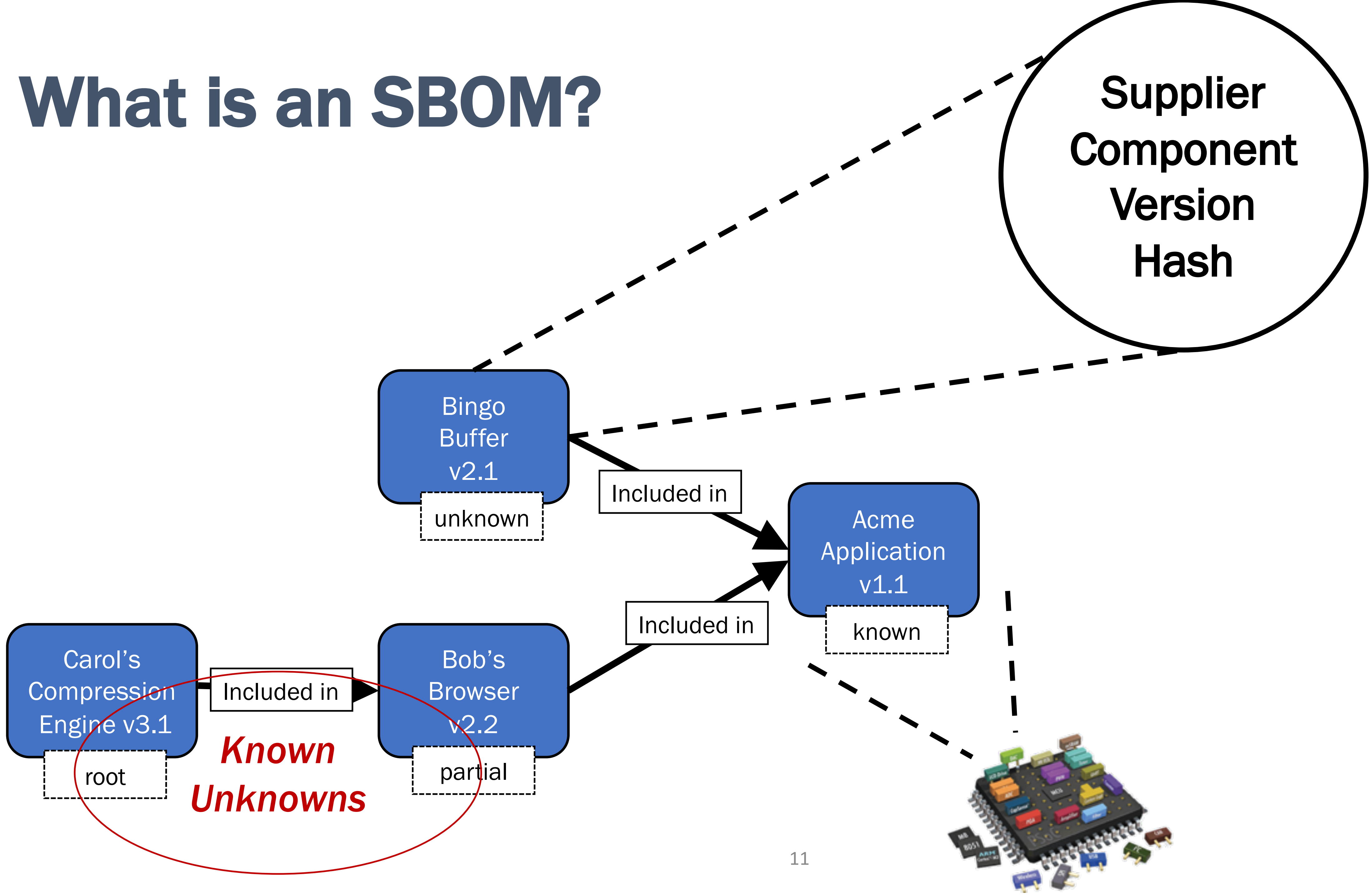
What is an SBOM?



A Software Bill of Materials (SBOM) is effectively a list of ingredients or a nested inventory.

It is “a formal record containing the details and supply chain relationships of various components used in building software"

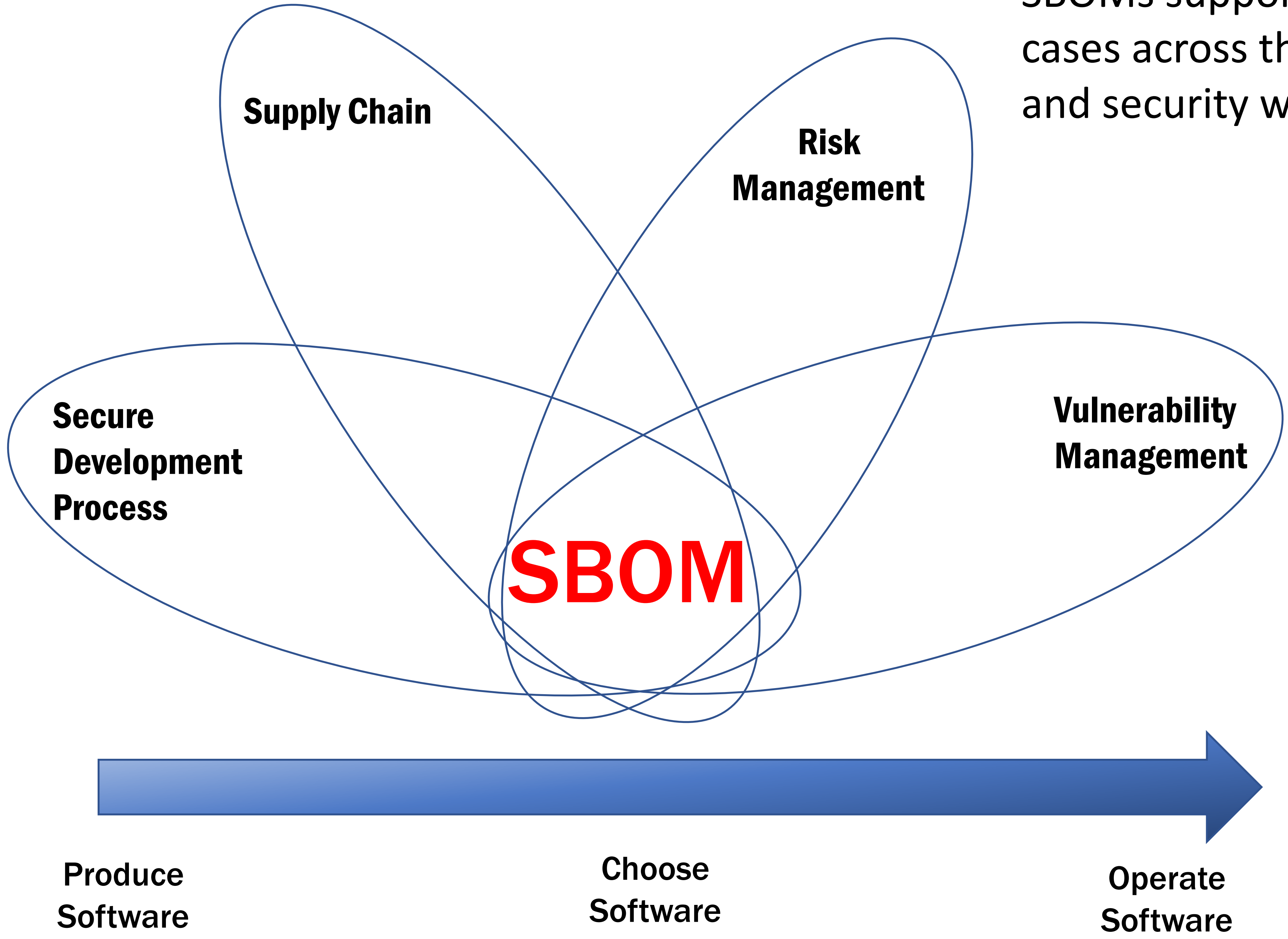
What is an SBOM?



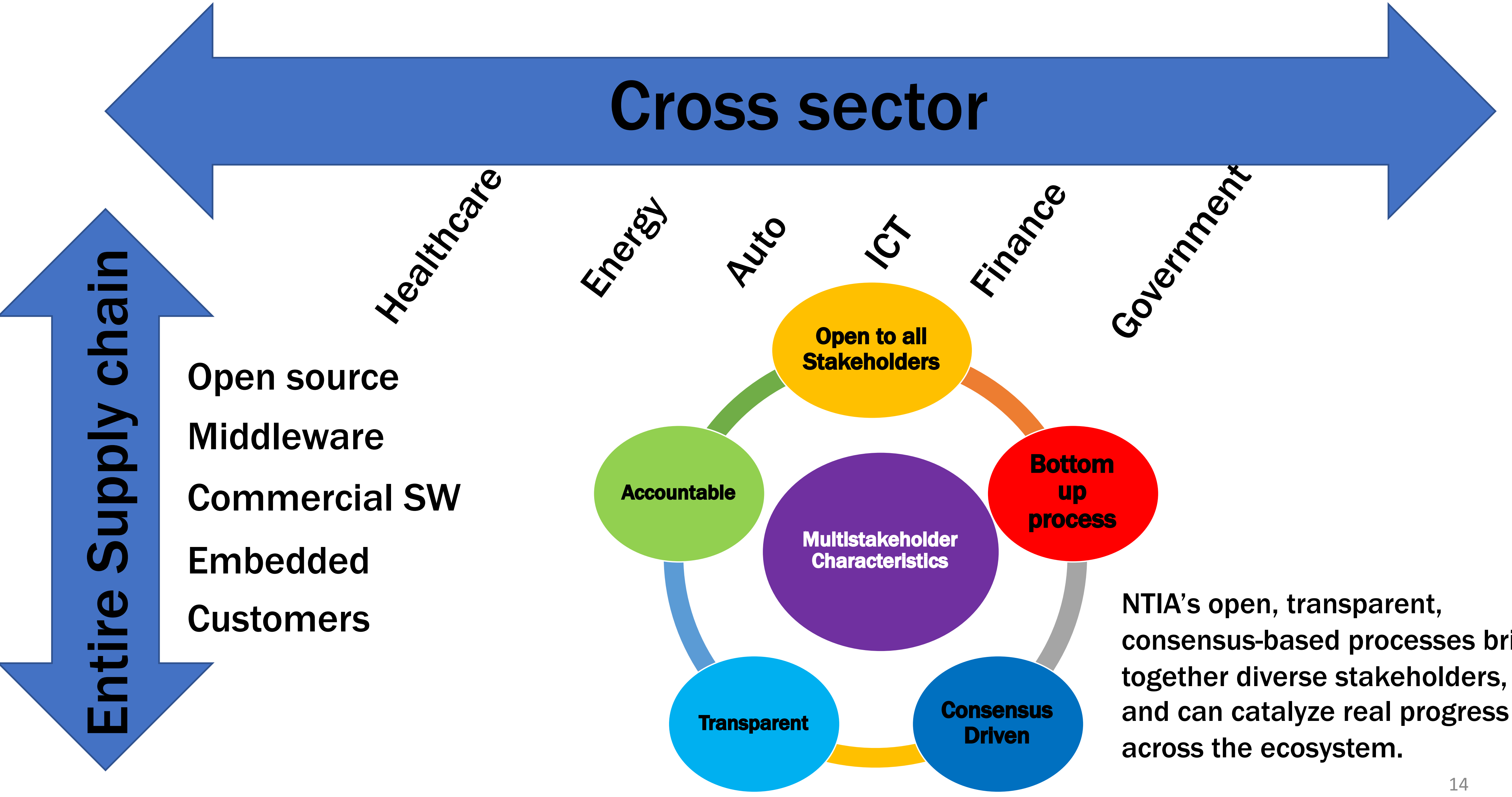
Why aren’t we doing this today?

- Licensing concerns and open source restrictions
- It’s a chicken-and-egg problem.
- It’s hard: benefits require machine readability for automation.
- It’s complex: involves integrating some technical and operational innovation.
- Success requires non-trivial adoption.

SBOMs support multiple use cases across the software and security world.



NTIA's Process on Software Component Transparency



NTIA's open, transparent, consensus-based processes bring together diverse stakeholders, and can catalyze real progress across the ecosystem.

What we're <u>not</u> doing

- Building out regulation
- Source code disclosure
- Standards development

- Solving all supply chain or assurance issues

Beyond talking

- From descriptive work to implementation
- Scalability, automation, and interoperability

The Future of SBOM

- Interest in the US and around the world
- SBOM in standards and guidance
- It is critical to establish a common set of practices and market expectations that is viable and reflects the needs of industry.

Summing up

- Software Bill of Materials is a technical and operational model of tracking software dependencies.
- SBOMs enable better software security and supply chain risk management
  - Vulnerability Management
  - Procurement
  - Dealing with emerging risks
- While we need cross-sector solutions, each community will need to understand its own unique implementation.
- Need continued industry leadership to guide investment, standards, and policy around the world.
- More information
  - Published documents: ntia.gov/SBOM
  - About the SBOM process: ntia.gov/SoftwareTransparency
  - Reach out to get involved: afriedman@ntia.gov

Next steps for the Energy Community

SBOM
Software Bill of Materials
ntia.gov/sbom #SBOM

- More detailed briefings in February / March
  - Highlight the global consensus on SBOM structure and implementation
  - Existing technical standards
  - How to experiment with SBOM: lessons from healthcare
- Initial conversations about potential structures of proof-of-concept exercise
- Search for initial participants

- Want to stay involved? Have more questions?

  afriedman@ntia.gov

Three formats to implement SBOM

SPDX is an open standard for communicating software bill of material information (including components, licenses, copyrights, and security references). The SPDX specification is developed by the SPDX workgroup, which is hosted by The Linux Foundation. The grass-roots effort includes representatives from more than 20 organizations—software, systems and tool vendors, foundations and systems integrators.

CycloneDX is a software bill of materials (SBOM) standard, purpose-built for software security contexts and supply chain component analysis. The specification is maintained by the CycloneDX Core working group, with origins in the OWASP community

SWID tags record unique information about an installed software application, including its name, edition, version, whether it is part of a bundle and more. SWID tags support software inventory and asset management initiatives. The structure of SWID tags is specified in international standard ISO/IEC 19770-2:2015.

- We have identified the common elements.
- A ‘multilingual’ ecosystem does not offer too many challenges
- Rather than pick a winner, we will build out guidance to support all formats with effective interoperability.

Implementing core SBOM fields

Field	SPDX	SWID	CycloneDX
Supplier	`(3.5) PackageSupplier:`	`<Entity> @role (softwareCreator/ publisher), @name`	`publisher`
Component	`(3.1) PackageName:`	`<softwareIdentity> @name`	`name`
Unique Identifier	`(3.2) SPDXID:`	`<softwareIdentity> @tagID`	`bom/serialNumber and component/bom-ref`
Version	`(3.3) PackageVersion:`	`<softwareIdentity> @version`	`version`
Component Hash	`(3.10) PackageChecksum:`	`<Payload>/../<File> @[hash-algorithm]:hash`	`hash`
Relationship	`(7.1) Relationship: CONTAINS`	`<Link>@rel, @href`	(Nested assembly/subassembly and/or dependency graphs)
SBOM Author	`(2.8) Creator:`	`<Entity> @role (tagCreator), @name`	`bom-descriptor: metadata/manufacture/ contact`