31ST ANNUAL FIRST CONFERENCE

EDINBURGH
JUNE 16-21
2019

Software Bill of Materials:

Progress toward transparency of 3rd party code

Allan Friedman, U.S. Department of Commerce

Art Manion, CERT Coordination Center

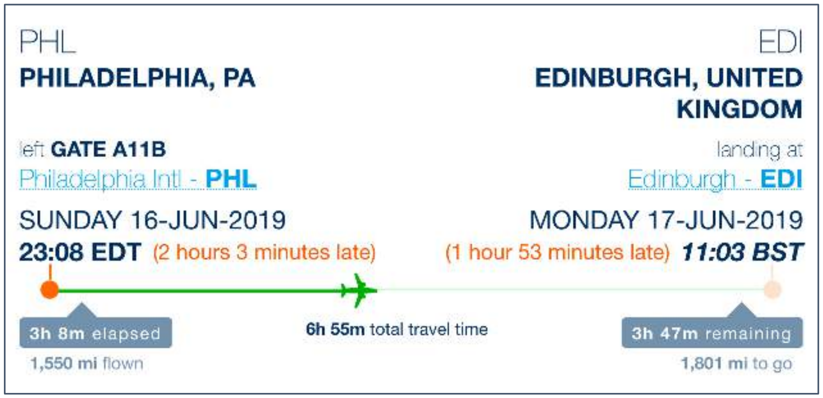
Art commutes by bike

- "Torn up grade crossing in bad weather at a low angle, what could possibly go wrong?"
- "Wow it takes longer to heal when you're over 40."

Where's Allan?

- "Flying in the morning of the talk should be fine."
- "My slides are mainly pictures, surely Art will know what I wanted to say."

AAL278 B752
ESTIMATED
PHL-EDI 10:53
EDI
PHL



PHL
PHILADELPHIA, PA

left **GATE A11B**
Philadelphia Intl - **PHL**

SUNDAY 16-JUN-2019
23:08 EDT (2 hours 3 minutes late)

EDI
EDINBURGH, UNITED KINGDOM

landing at
Edinburgh - **EDI**

MONDAY 17-JUN-2019
(1 hour 53 minutes late) ***11:03 BST***

3h 8m elapsed
1,550 mi flown

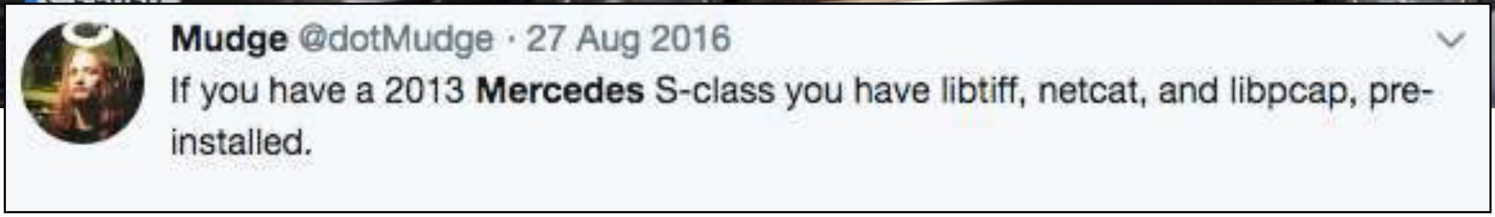
6h 55m total travel time

3h 47m remaining
1,801 mi to go

Paying attention vs Checking Email

- The case for transparency
- How transparency can help the software ecosystem
- Why aren’t we doing this already?
- What *is* a Software Bill of Materials?
- How do we do this?
- What next?

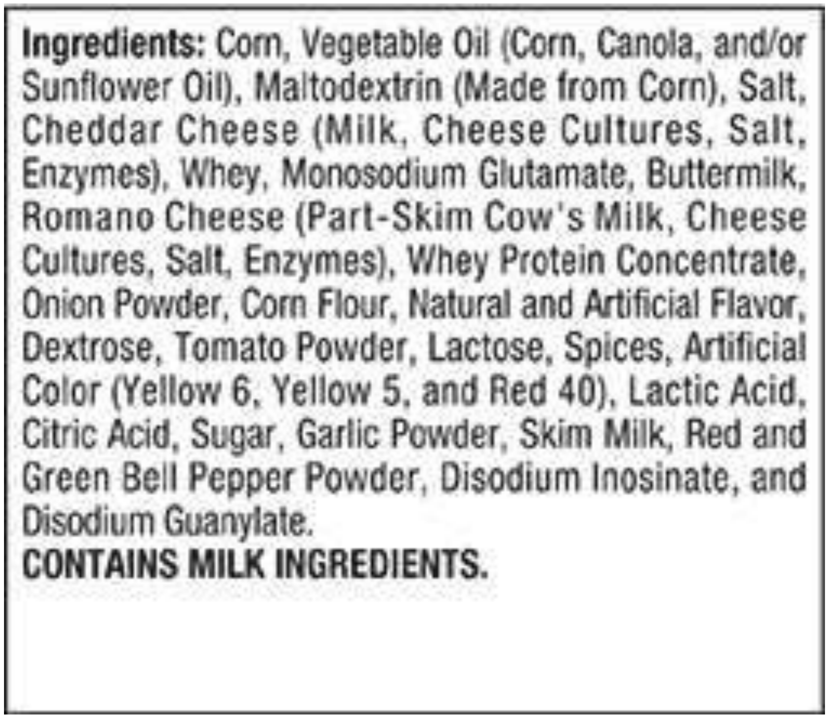
S E 5060



Mudge @dotMudge · 27 Aug 2016

If you have a 2013 **Mercedes** S-class you have libtiff, netcat, and libpcap, pre-installed.

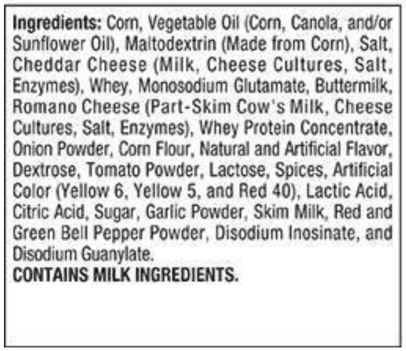
Analogies



Ingredients: Corn, Vegetable Oil (Corn, Canola, and/or Sunflower Oil), Maltodextrin (Made from Corn), Salt, Cheddar Cheese (Milk, Cheese Cultures, Salt, Enzymes), Whey, Monosodium Glutamate, Buttermilk, Romano Cheese (Part-Skim Cow's Milk, Cheese Cultures, Salt, Enzymes), Whey Protein Concentrate, Onion Powder, Corn Flour, Natural and Artificial Flavor, Dextrose, Tomato Powder, Lactose, Spices, Artificial Color (Yellow 6, Yellow 5, and Red 40), Lactic Acid, Citric Acid, Sugar, Garlic Powder, Skim Milk, Red and Green Bell Pepper Powder, Disodium Inosinate, and Disodium Guanylate.

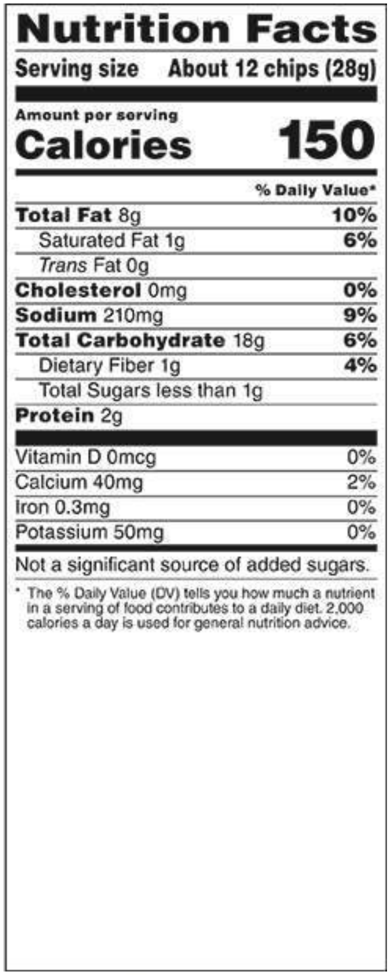
CONTAINS MILK INGREDIENTS.

Analogies



Ingredients: Corn, Vegetable Oil (Corn, Canola, and/or Sunflower Oil), Maltodextrin (Made from Corn), Salt, Cheddar Cheese (Milk, Cheese Cultures, Salt, Enzymes), Whey, Monosodium Glutamate, Buttermilk, Romano Cheese (Part-Skim Cow's Milk, Cheese Cultures, Salt, Enzymes), Whey Protein Concentrate, Onion Powder, Corn Flour, Natural and Artificial Flavor, Dextrose, Tomato Powder, Lactose, Spices, Artificial Color (Yellow 6, Yellow 5, and Red 40), Lactic Acid, Citric Acid, Sugar, Garlic Powder, Skim Milk, Red and Green Bell Pepper Powder, Disodium Inosinate, and Disodium Guanylate.

CONTAINS MILK INGREDIENTS.



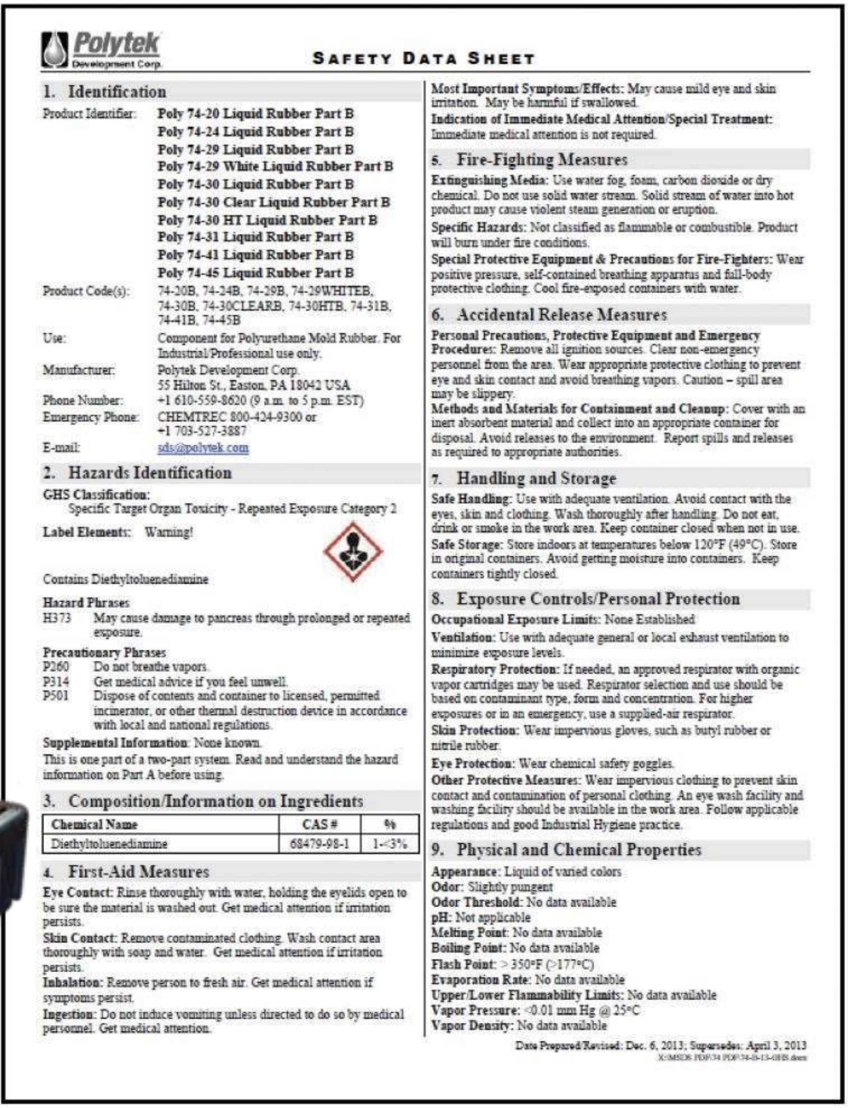
Nutrition Facts

Serving size	**About 12 chips (28g)**
Amount per serving **Calories**	**150**
	% Daily Value*
Total Fat 8g	**10%**
Saturated Fat 1g	**6%**
Trans Fat 0g	
Cholesterol 0mg	**0%**
Sodium 210mg	**9%**
Total Carbohydrate 18g	**6%**
Dietary Fiber 1g	**4%**
Total Sugars less than 1g	
Protein 2g	
Vitamin D 0mcg	0%
Calcium 40mg	2%
Iron 0.3mg	0%
Potassium 50mg	0%

Not a significant source of added sugars.

* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

Analogies (cont'd)



Polytek Development Corp.

SAFETY DATA SHEET

1. Identification

Product Identifier:	**Poly 74-20 Liquid Rubber Part B** **Poly 74-24 Liquid Rubber Part B** **Poly 74-29 Liquid Rubber Part B** **Poly 74-29 White Liquid Rubber Part B** **Poly 74-30 Liquid Rubber Part B** **Poly 74-30 Clear Liquid Rubber Part B** **Poly 74-30 HT Liquid Rubber Part B** **Poly 74-31 Liquid Rubber Part B** **Poly 74-41 Liquid Rubber Part B** **Poly 74-45 Liquid Rubber Part B**
Product Code(s):	74-20B, 74-24B, 74-29B, 74-29WHITEB, 74-30B, 74-30CLEARB, 74-30HTB, 74-31B, 74-41B, 74-45B
Use:	Component for Polyurethane Mold Rubber. For Industrial/Professional use only.
Manufacturer:	Polytek Development Corp. 55 Hilton St., Easton, PA 18042 USA
Phone Number:	+1 610-559-8620 (9 a.m. to 5 p.m. EST)
Emergency Phone:	CHEMTREC 800-424-9300 or +1 703-527-3887
E-mail:	sds@polytek.com

2. Hazards Identification

GHS Classification:
Specific Target Organ Toxicity - Repeated Exposure Category 2

Label Elements: Warning!

Contains Diethyltoluenediamine

Hazard Phrases

H373	May cause damage to pancreas through prolonged or repeated exposure.

Precautionary Phrases

P260	Do not breathe vapors.
P314	Get medical advice if you feel unwell.
P501	Dispose of contents and container to licensed, permitted incinerator, or other thermal destruction device in accordance with local and national regulations.

Supplemental Information: None known.

This is one part of a two-part system. Read and understand the hazard information on Part A before using.

3. Composition/Information on Ingredients

Chemical Name	CAS #	%
Diethyltoluenediamine	68479-98-1	1-<3%

4. First-Aid Measures

Eye Contact: Rinse thoroughly with water, holding the eyelids open to be sure the material is washed out. Get medical attention if irritation persists.

Skin Contact: Remove contaminated clothing. Wash contact area thoroughly with soap and water. Get medical attention if irritation persists.

Inhalation: Remove person to fresh air. Get medical attention if symptoms persist.

Ingestion: Do not induce vomiting unless directed to do so by medical personnel. Get medical attention.

Most Important Symptoms/Effects: May cause mild eye and skin irritation. May be harmful if swallowed.

Indication of Immediate Medical Attention/Special Treatment: Immediate medical attention is not required.

5. Fire-Fighting Measures

Extinguishing Media: Use water fog, foam, carbon dioxide or dry chemical. Do not use solid water stream. Solid stream of water into hot product may cause violent steam generation or eruption.

Specific Hazards: Not classified as flammable or combustible. Product will burn under fire conditions.

Special Protective Equipment & Precautions for Fire-Fighters: Wear positive pressure, self-contained breathing apparatus and full-body protective clothing. Cool fire-exposed containers with water.

6. Accidental Release Measures

Personal Precautions, Protective Equipment and Emergency Procedures: Remove all ignition sources. Clear non-emergency personnel from the area. Wear appropriate protective clothing to prevent eye and skin contact and avoid breathing vapors. Caution – spill area may be slippery.

Methods and Materials for Containment and Cleanup: Cover with an inert absorbent material and collect into an appropriate container for disposal. Avoid releases to the environment. Report spills and releases as required to appropriate authorities.

7. Handling and Storage

Safe Handling: Use with adequate ventilation. Avoid contact with the eyes, skin and clothing. Wash thoroughly after handling. Do not eat, drink or smoke in the work area. Keep container closed when not in use.

Safe Storage: Store indoors at temperatures below 120°F (49°C). Store in original containers. Avoid getting moisture into containers. Keep containers tightly closed.

8. Exposure Controls/Personal Protection

Occupational Exposure Limits: None Established

Ventilation: Use with adequate general or local exhaust ventilation to minimize exposure levels.

Respiratory Protection: If needed, an approved respirator with organic vapor cartridges may be used. Respirator selection and use should be based on contaminant type, form and concentration. For higher exposures or in an emergency, use a supplied-air respirator.

Skin Protection: Wear impervious gloves, such as butyl rubber or nitrile rubber.

Eye Protection: Wear chemical safety goggles.

Other Protective Measures: Wear impervious clothing to prevent skin contact and contamination of personal clothing. An eye wash facility and washing facility should be available in the work area. Follow applicable regulations and good Industrial Hygiene practice.

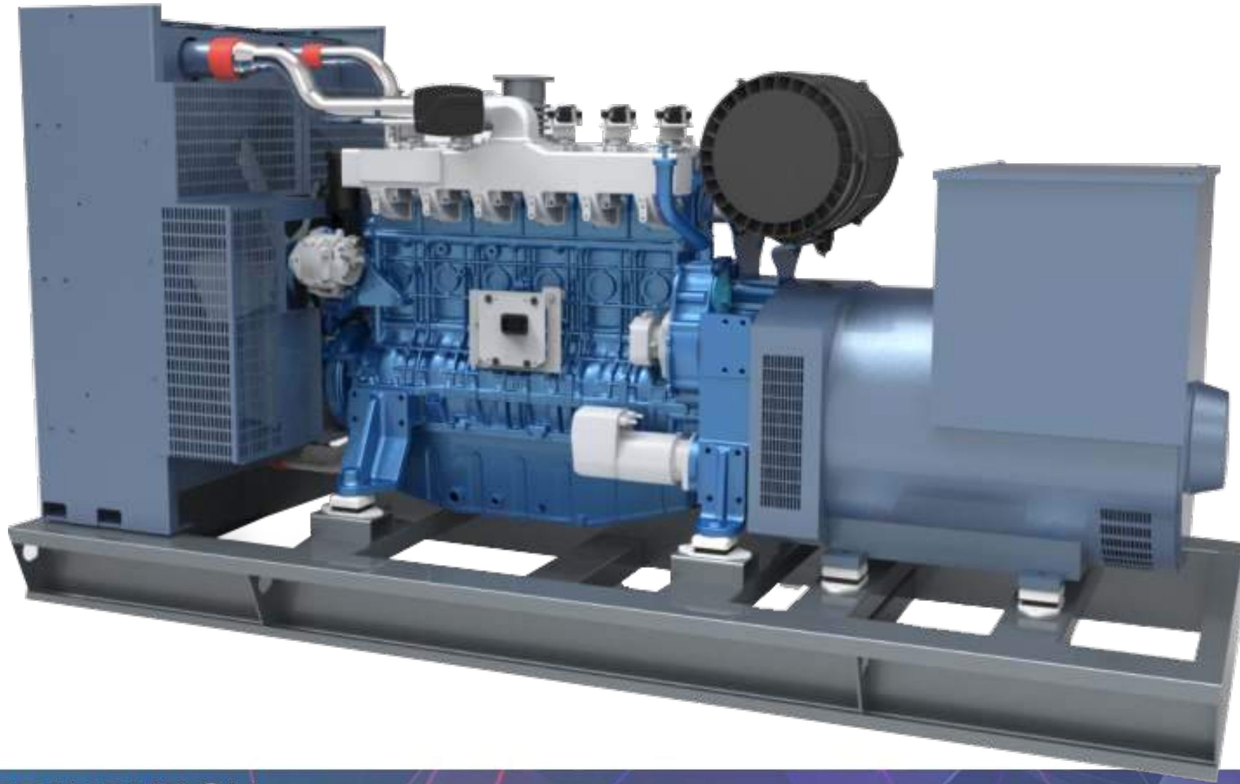
9. Physical and Chemical Properties

Appearance: Liquid of varied colors
Odor: Slightly pungent
Odor Threshold: No data available
pH: Not applicable
Melting Point: No data available
Boiling Point: No data available
Flash Point: > 350°F (>177°C)
Evaporation Rate: No data available
Upper/Lower Flammability Limits: No data available
Vapor Pressure: <0.01 mm Hg @ 25°C
Vapor Density: No data available

Date Prepared/Revised: Dec. 6, 2013; **Supersedes**: April 3, 2013
X:\MSDS PDF\74 PDF\74-B-13-GHS.docx

Updated Polytek® Safety Data Sheet [Page 1 Only]

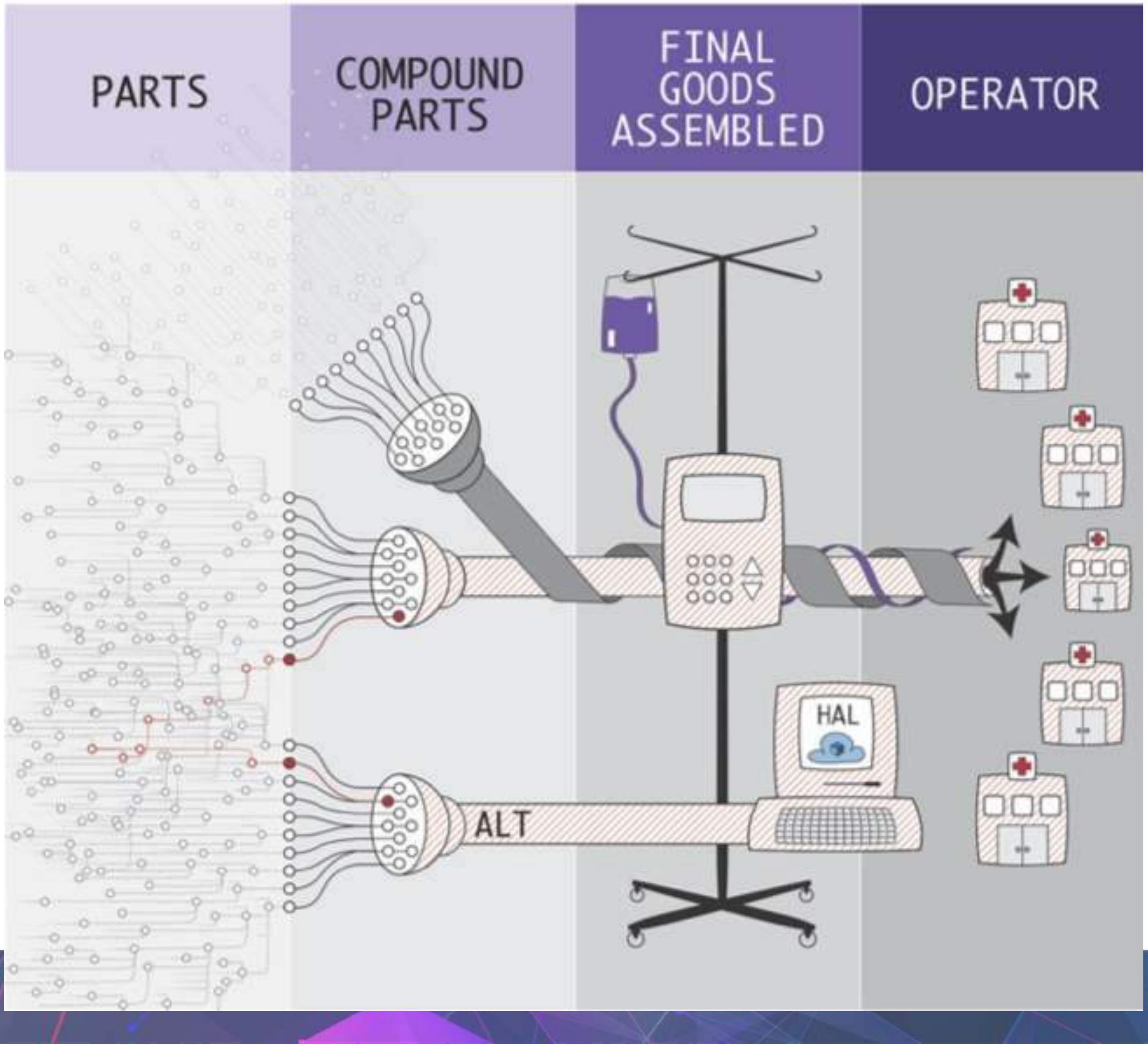
Analogies (cont'd)



A data layer to drive innovation

Supply chain

- Supplier selection
- Supply selection
- Supply vigilance



Three perspectives across the supply chain

- Produce software
- Choose software
- Operate software

Use Cases: Producing software

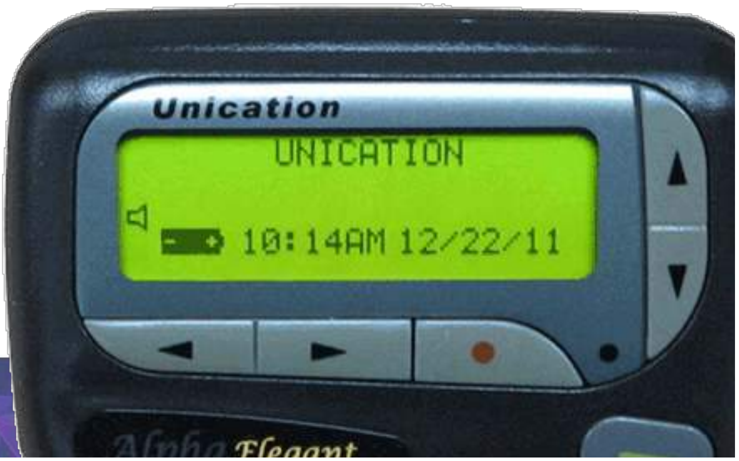
- Monitor for vulnerabilities in components
- Better manage code base
- Execute white-list or black-list practices
- Prepare and respond to end-of-life contingencies
- Minimize code bloat
- Know and comply with license obligations
- Provide an SBoM for customers

Use Cases: Choosing software

- Identify known vulnerabilities
- More targeted security analysis
- Verify sourcing
- Compliance
- EOL awareness
- Verify some supplier claims
- Understand software integration
- Market signal of secure development process

Use Cases: Operating software

- Vulnerability management
- Better understanding of operational risks
- Real time data on components in assets
- Improved understanding of potential exploitability
- Enable potential non-SW mitigations



So why aren't we doing this already?

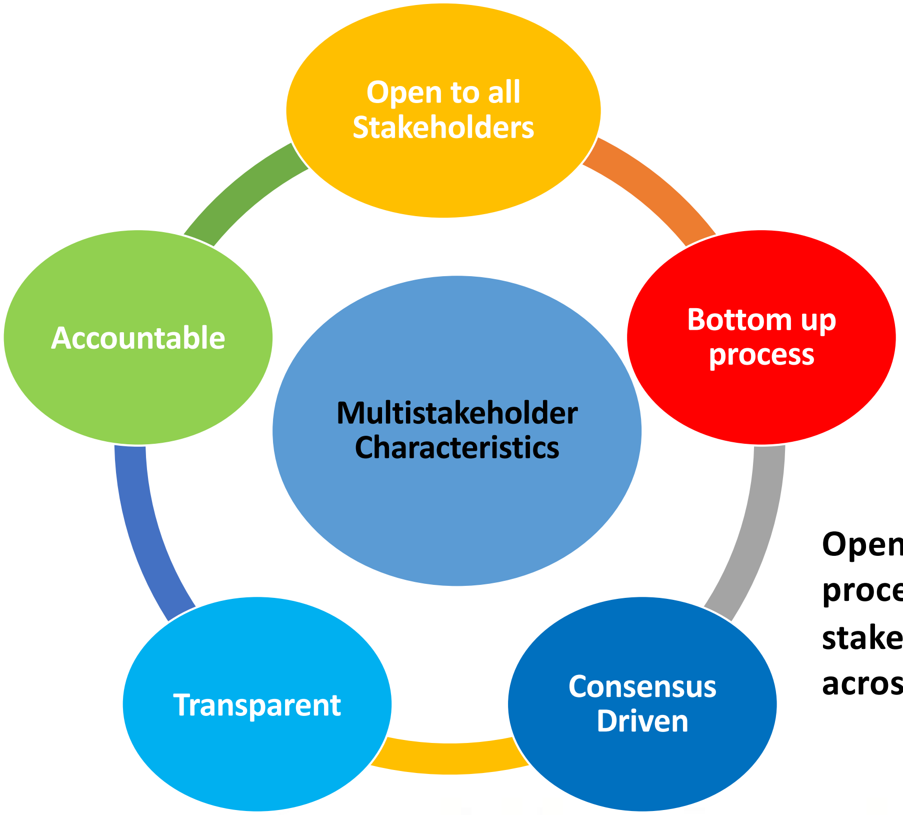
It’s hard.

- Apache2
- Apache Web Server
- Apache
- HTTPd
- HTTPd2

A market failure?

Enter your friends, the Feds

The ‘multistakeholder’ model



Open, transparent, consensus based processes that bring together diverse stakeholders can catalyze real progress across the ecosystem.

The “multistakeholder” model

The “multistakeholder” model

What we're not doing

- Regulation
- Source code disclosure
- Standards development

- **Harmonization**
- **Amplification & routinization**
- **Extensions & innovation**

Making progress

- Clear appreciation across sectors on the potential value of transparency
- Consensus already on
  - The broad scope of the problem
  - Machine-readability of the solution
- **“Minimum Viable Identity” (MVI)**

Framing

- Conceptual design
- Terminology
- Broad requirements
- Cross-cutting issues

Emerging consensus, or at least temporary acceptance

Éamonn Ó Muirí
https://flic.kr/p/46dsiz
https://creativecommons.org/licenses/by/2.0/legalcode

What is an SBoM?

1. Core information elements: Minimum Viable Identity (MVI)
    - Cryptographic hash (or signature)
2. Other very, very important and useful identify information
    - Supplier (aliases), author, component (aliases), version, relationships
3. Other information necessary for most use cases and applications
    - License, entitlement, vulnerability mapping, formulation, provenance

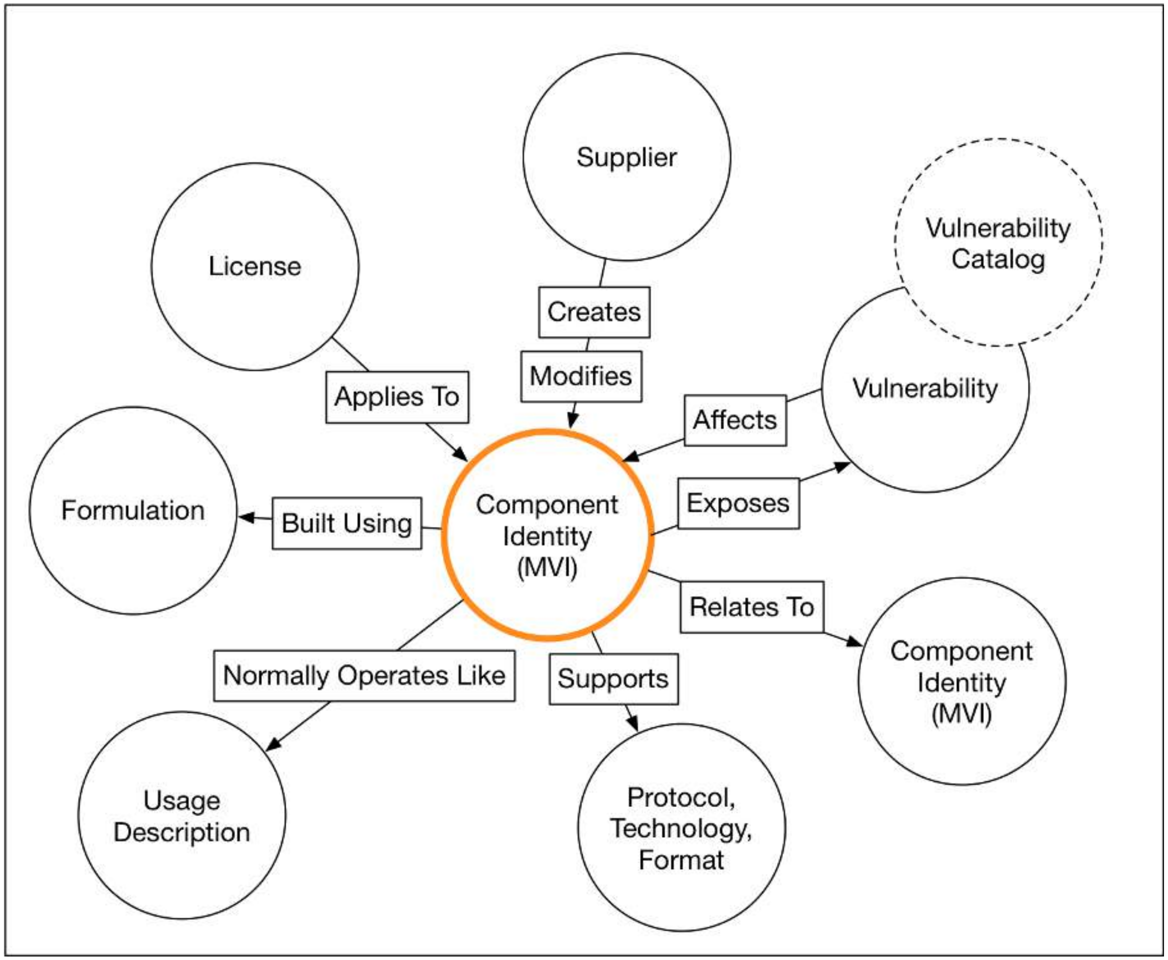
- Software components
    - Defined and named by suppliers, at time of delivery (build, package, install, deploy)
    - Hardware not excluded
    - Source code not excluded

Applications

- Intellectual property management
  - Licensing, entitlement
  - Most mature application
- Vulnerability management
  - What components are affected by vulnerabilities?
  - Transitivity – vulnerability is not necessarily exposure or exploitability
- High assurance
  - Provenance, pedigree, formulation, integrity, chain of custody
- Economic benefits of supply chain hygiene

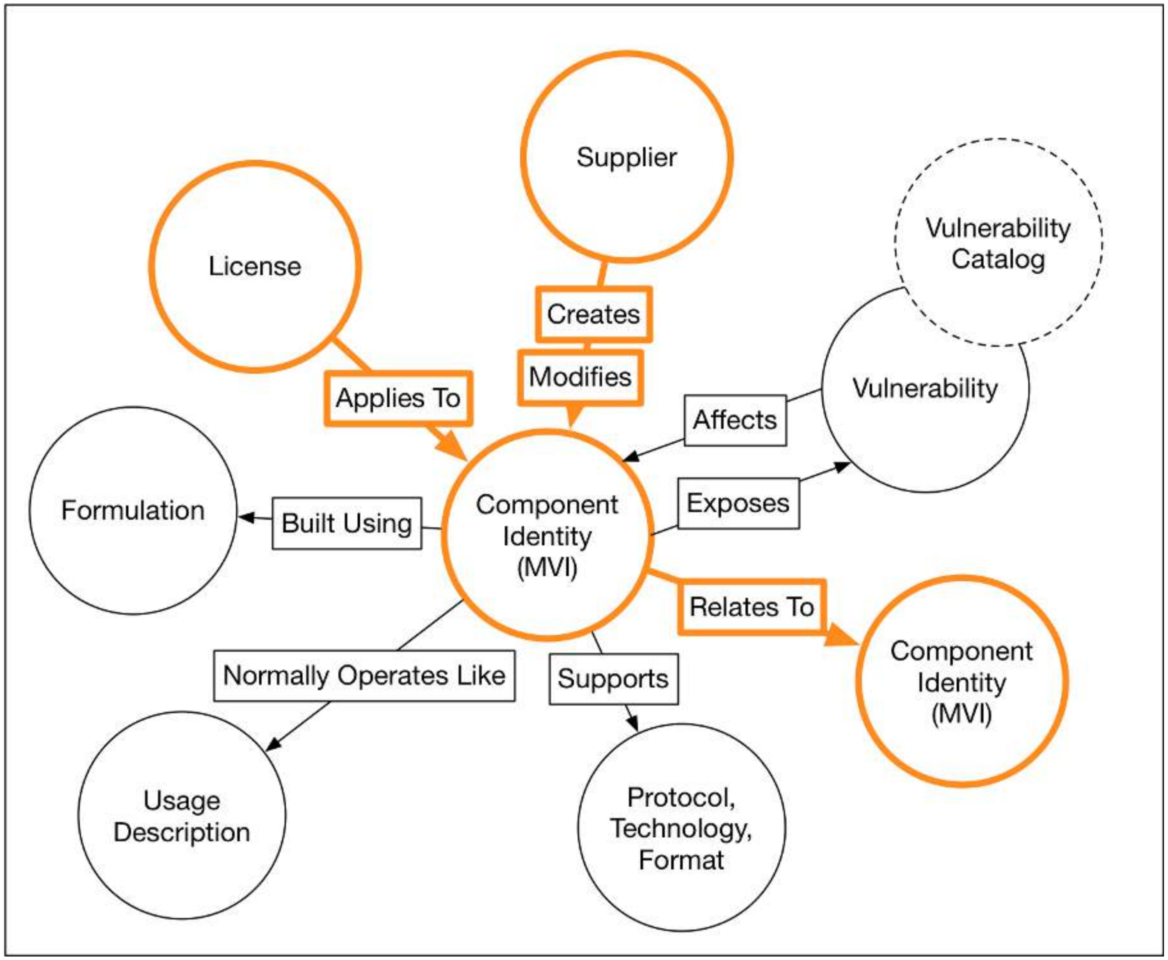
Selected SBoM Elements

- No SBoM without MVI



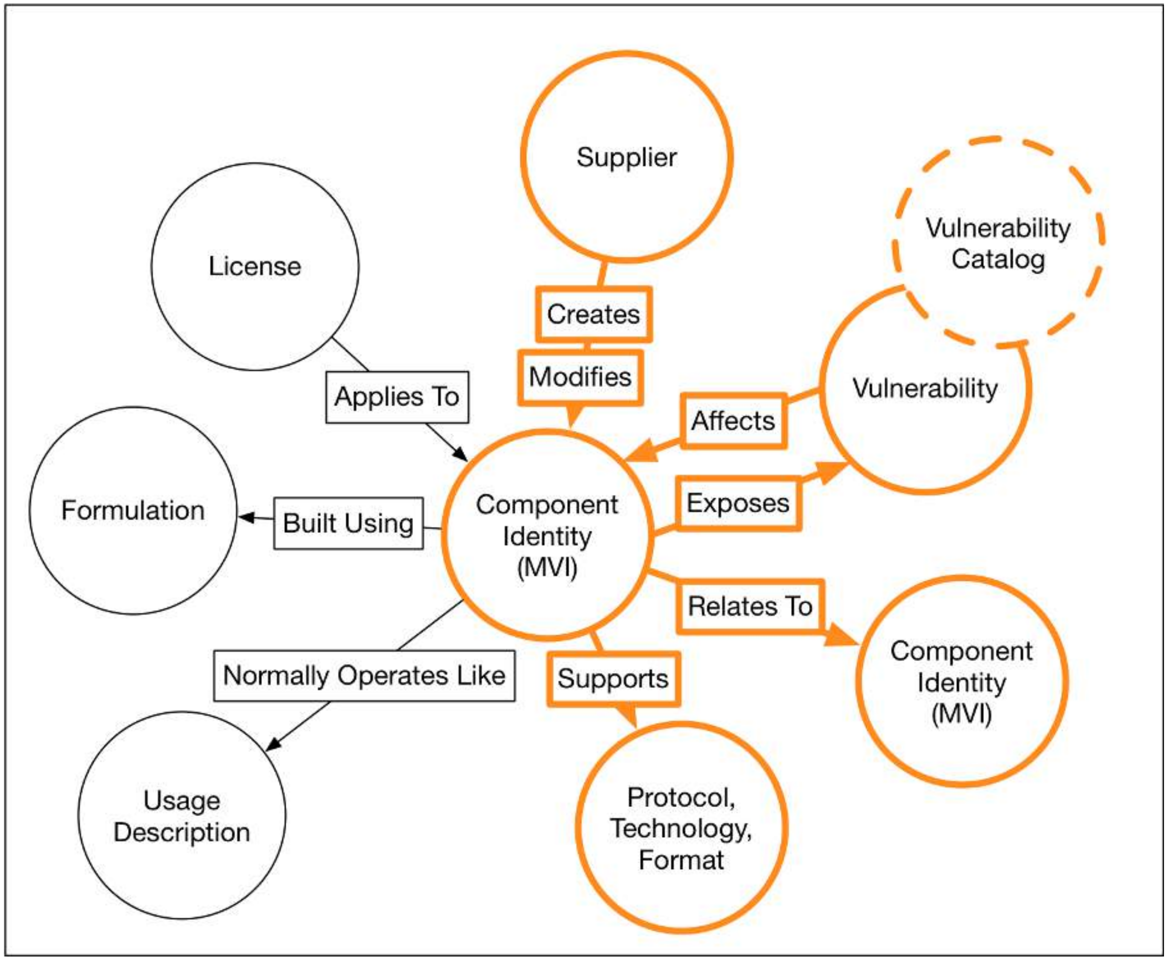
Intellectual Property

- Well-established application
- Licensing, liability, entitlement



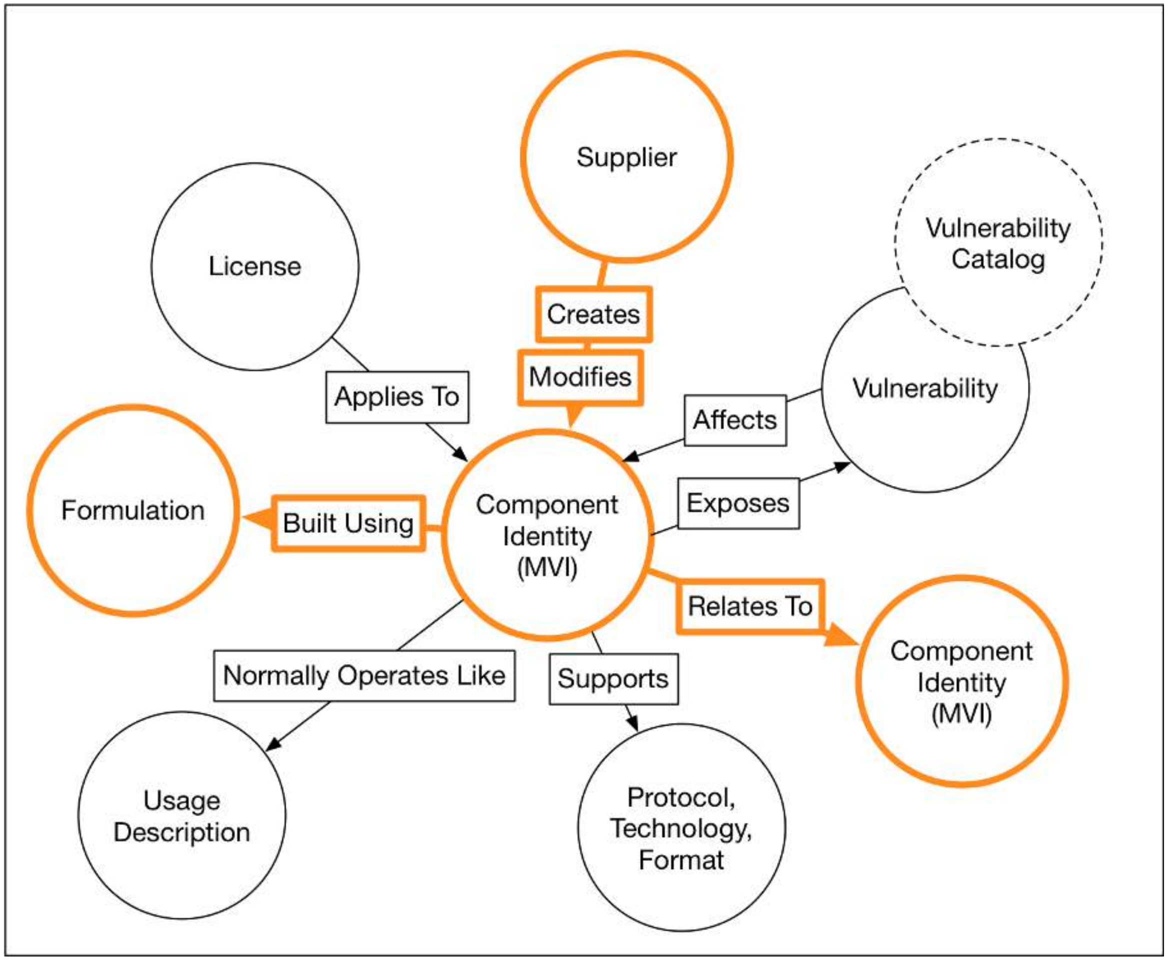
Vulnerability Management

- Requires vulnerability mapping to external catalog
- Related technologies and other components helpful for coordinated disclosure



High Assurance

- Critical systems, national defense
- Formulation: How component was built
- Not shown: Provenance, pedigree, chain of custody



SBoM Processes

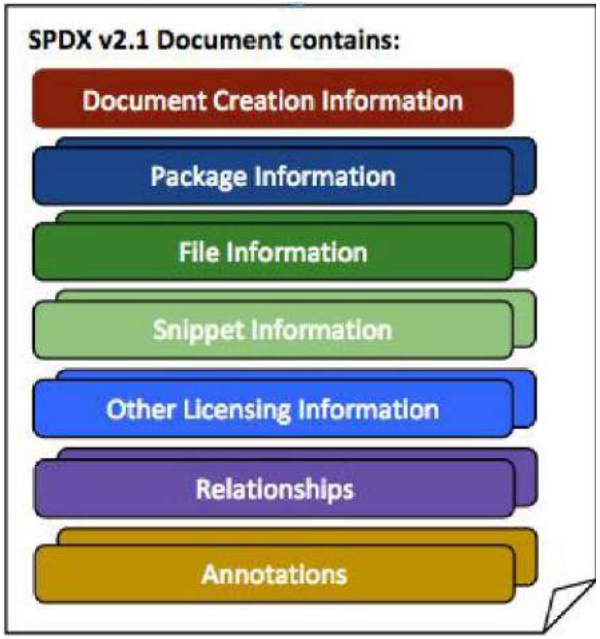
- Supplier responsibilities
  1. Define self-created components and create SBoMs
  2. Obtain SBoMs from direct, immediate suppliers
  3. Provide collected set of SBoMs to consumers
- Change SBoM when software changes
  - Patch, update, new version
- Change SBoM when other information changes
  - License, new upstream information
- Challenge: Claims about other suppliers’ SBoMs
  - Author and Supplier are different

Terminology

- SBoM (Software Bill of Materials): inventory and associated information in a standardized format
- Inventory: list of components using Minimum Viable Identity
- Author: entity that creates SBoMs
- Supplier: entity that defines and identifies components and creates associated SBoMs
- Consumer: entity that obtains SBoMs
- Component: unit of software defined by a supplier at the time the component is built, packaged, or distributed

Existing Work

- Software Identification Tags (SWID)
  - ISO/IEC 19770-2, NIST (US)
- Software Package Data Exchange (SPDX)
  - Linux Foundation
- Software Heritage
  - Focus on source code
  - Identifiers for Digital Objects
- package URL (purl)
- Common Platform Enumeration (CPE)
- Software Asset Management (SAM)
- Software Composition Analysis (SCA)
- Supply Chain Risk Management (SCRM)



SPDX v2.1 Document contains:

Document Creation Information

Package Information

File Information

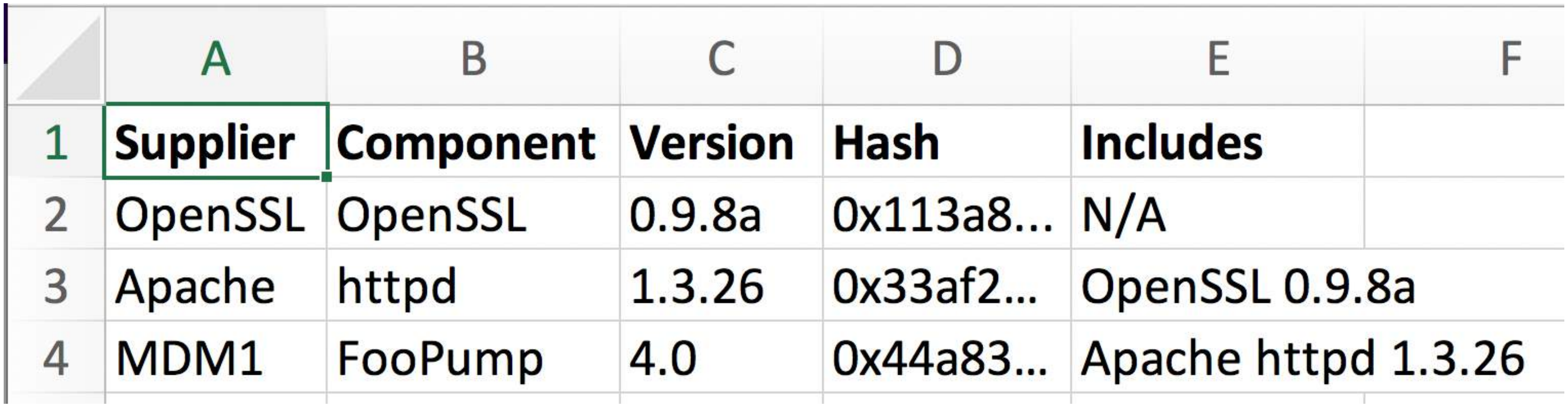
Snippet Information

Other Licensing Information

Relationships

Annotations

Example: Simple Table



	A	B	C	D	E	F
1	**Supplier**	**Component**	**Version**	**Hash**	**Includes**	
2	OpenSSL	OpenSSL	0.9.8a	0x113a8...	N/A	
3	Apache	httpd	1.3.26	0x33af2...	OpenSSL 0.9.8a	
4	MDM1	FooPump	4.0	0x44a83...	Apache httpd 1.3.26	

Example: namespace:name

org.openssl:”OpenSSL 0.9.8a”

org.apache:”httpd 1.3.26”

com.mdm1:”FooPump 4.0 0x44a83…”

Example: purl

pkg:tgz/org.openssl/OpenSSL@0.9.8a

pkg:tgz/org.apache/httpd@1.3.26?requires=pkg:tgz/org.openssl/OpenSSL@0.9.8a

pkg:device/com.mdm1/FooPump@4.0?hash=0x44a83…&requires=pkg:tgz/org.apache/httpd@1.3.26

Example: SWID

```
<SoftwareIdentity name="openssl" tagId="openssl/openssl@0.9.8a"
version="0.9.8a"/>

<SoftwareIdentity name="apache_httpd" tagId="apache/httpd@1.3.26"
version="1.3.26"/>
<Link href="swid:openssl/openssl@0.9.8a" rel="requires"/>

<SoftwareIdentity name="MDM1 FooPump" tagId="MDM1/FooPump@4.0"
version="4.0"/>
<Link href="swid:apache/httpd@1.3.26" rel="requires"/>
```

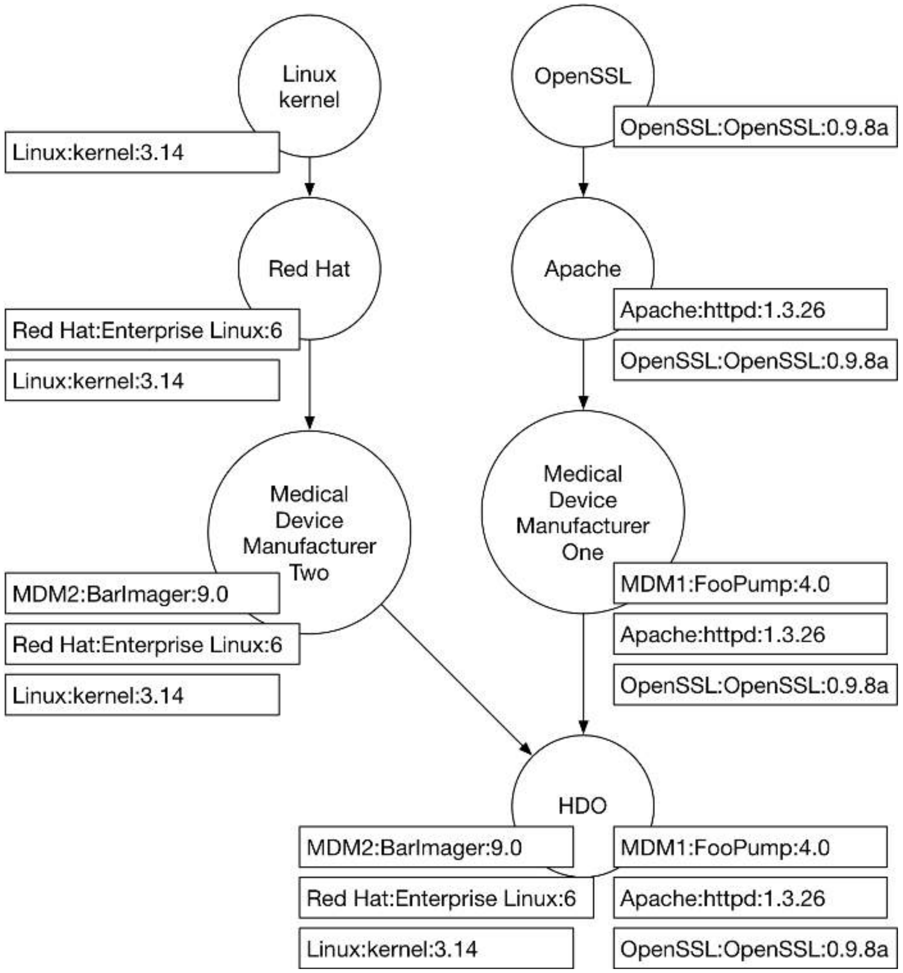
Example: SPDX

```
PackageName: openssl
SPDXID: openssl/openssl@0.9.8a
PackageVersion: 0.9.8a

PackageName: apache_httpd
SPDXID: apache/httpd@1.3.26
PackageVersion: 1.3.26
Relationship: openssl/openssl@0.9.8a PREREQUISITE_OF apache/httpd@1.3.26

PackageName: ”MDM1 FooPump”
SPDXID: mdm1/foopump@4.0
PackageVersion: 4.0
Relationship: apache/httpd@1.3.26 PREREQUISITE_OF mdm1/foopump@4.0
```

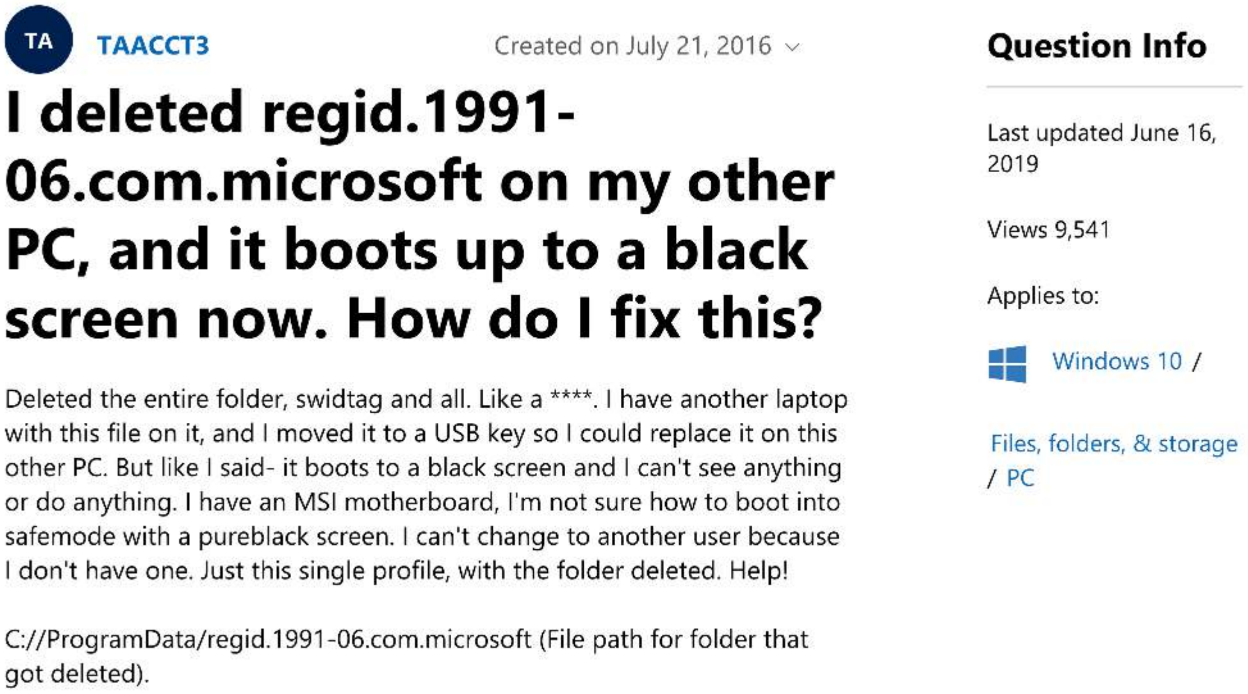
Example: Graph



Example: Additional SBoM Data

	SWID	SPDX
Hash	hash-entry hash-alg-id hash-value	PackageVerificationCode PackageChecksum FileChecksum
License		LicenseConcluded PackageLicenseDeclared LicenseName
Entitlement	@entitlementKey	

SWID IRL



TA TAACCT3 Created on July 21, 2016

I deleted regid.1991-06.com.microsoft on my other PC, and it boots up to a black screen now. How do I fix this?

Deleted the entire folder, swidtag and all. Like a ****. I have another laptop with this file on it, and I moved it to a USB key so I could replace it on this other PC. But like I said- it boots to a black screen and I can't see anything or do anything. I have an MSI motherboard, I'm not sure how to boot into safemode with a pureblack screen. I can't change to another user because I don't have one. Just this single profile, with the folder deleted. Help!

C://ProgramData/regid.1991-06.com.microsoft (File path for folder that got deleted).

Question Info

Last updated June 16, 2019

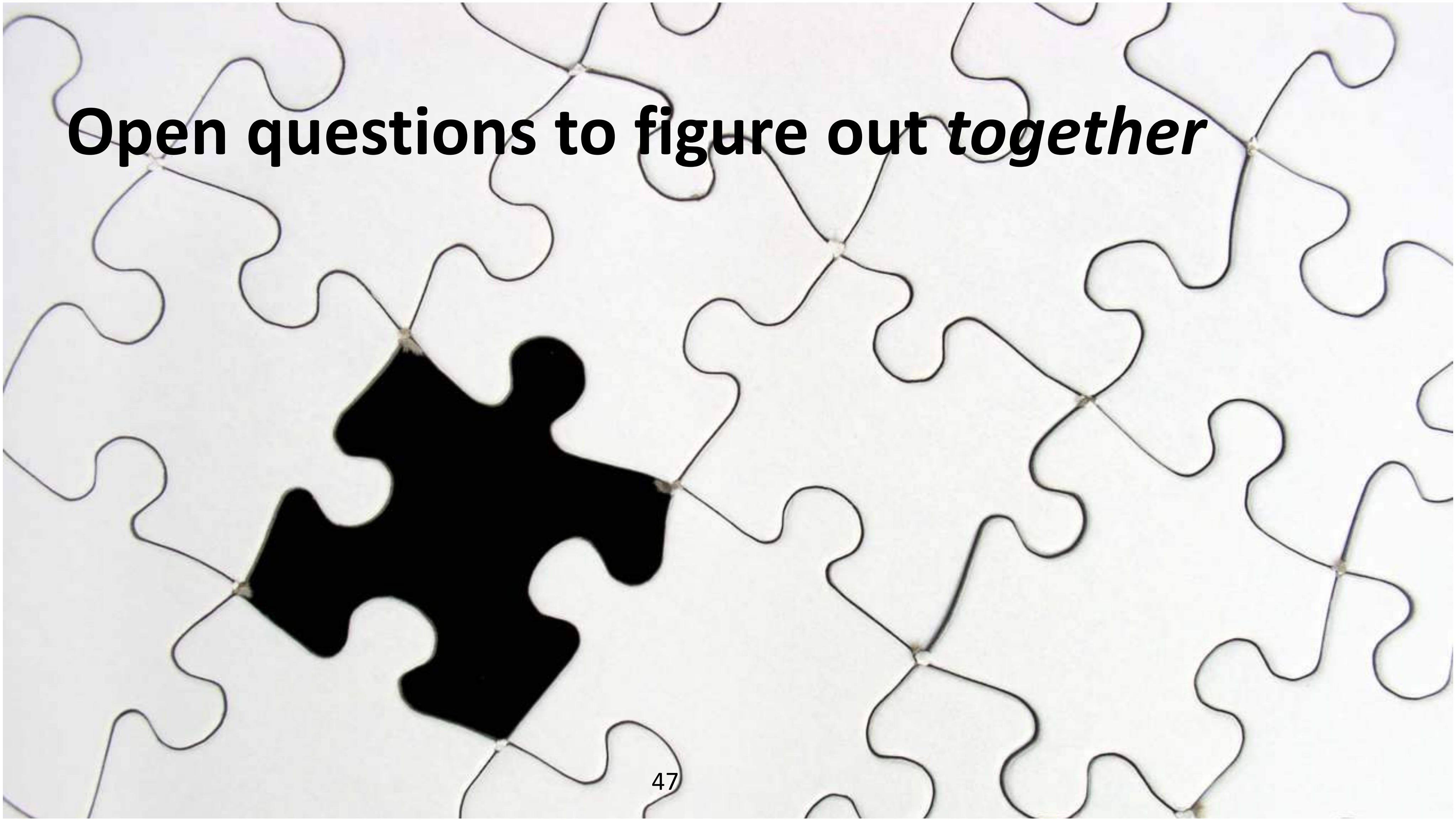
Views 9,541

Applies to:

Windows 10 /

Files, folders, & storage / PC

Open questions to figure out *together*



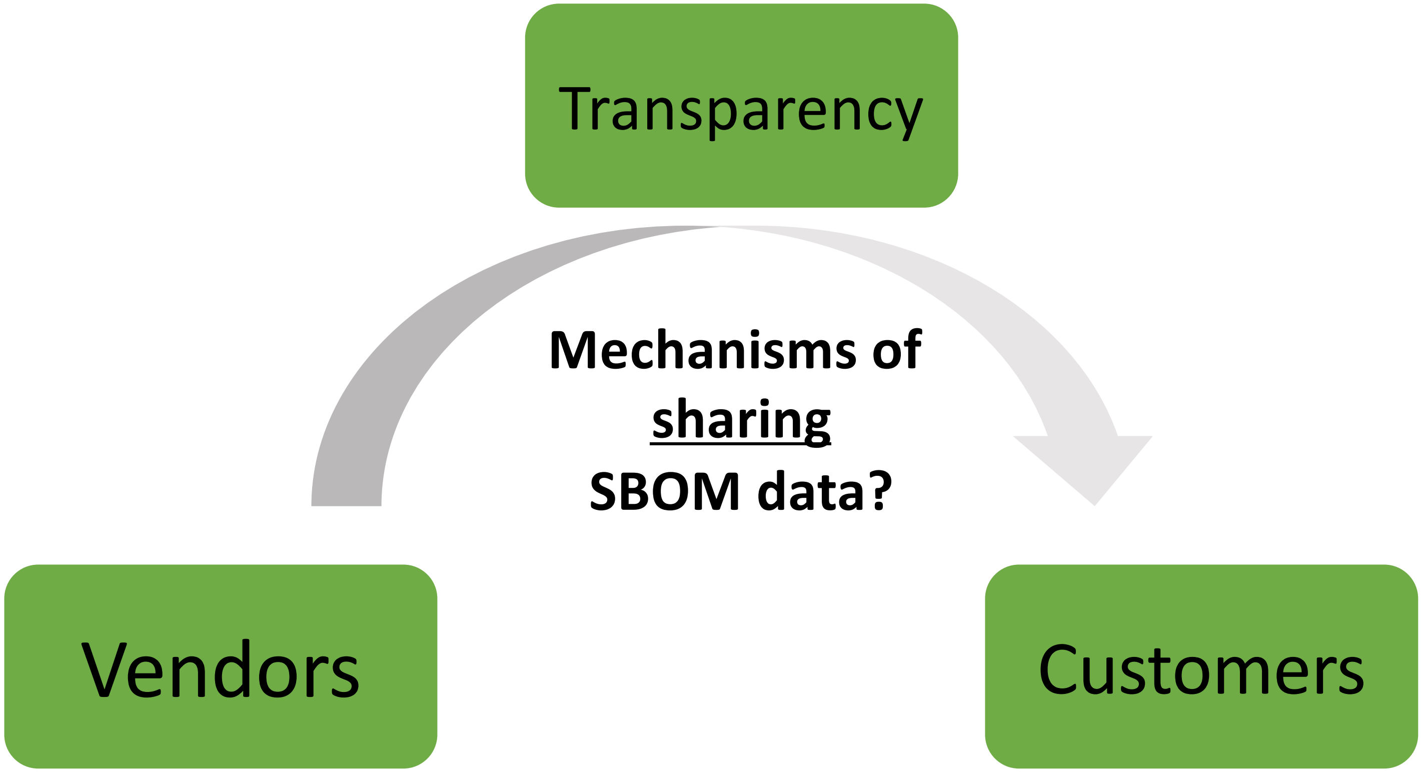
Obstacles to obtaining SBOM data?

Federation

- Vertical slices of solution
  - Automatic updates, package managers
- Centralized authority and collection does not scale
  - NIST (US) Common Platform Enumeration (CPE)
  - NIST (US) National Software Reference Library (NSRL)
  - TagVault (for SWID)
- Distribute effort to suppliers (vendors)
  - Least Cost Avoider
  - Most suppliers are also consumers

Opacity and Translucency

- Suppliers have first-hand knowledge about components they originate and those they directly obtain from an upstream supplier
- What happens when SBoM is not available?
  - Knowledge that there are no further upstream dependencies
  - Lack of such knowledge
  - Third-party claims is fragile design



Transparency

Mechanisms of sharing SBOM data?

Vendors

Customers

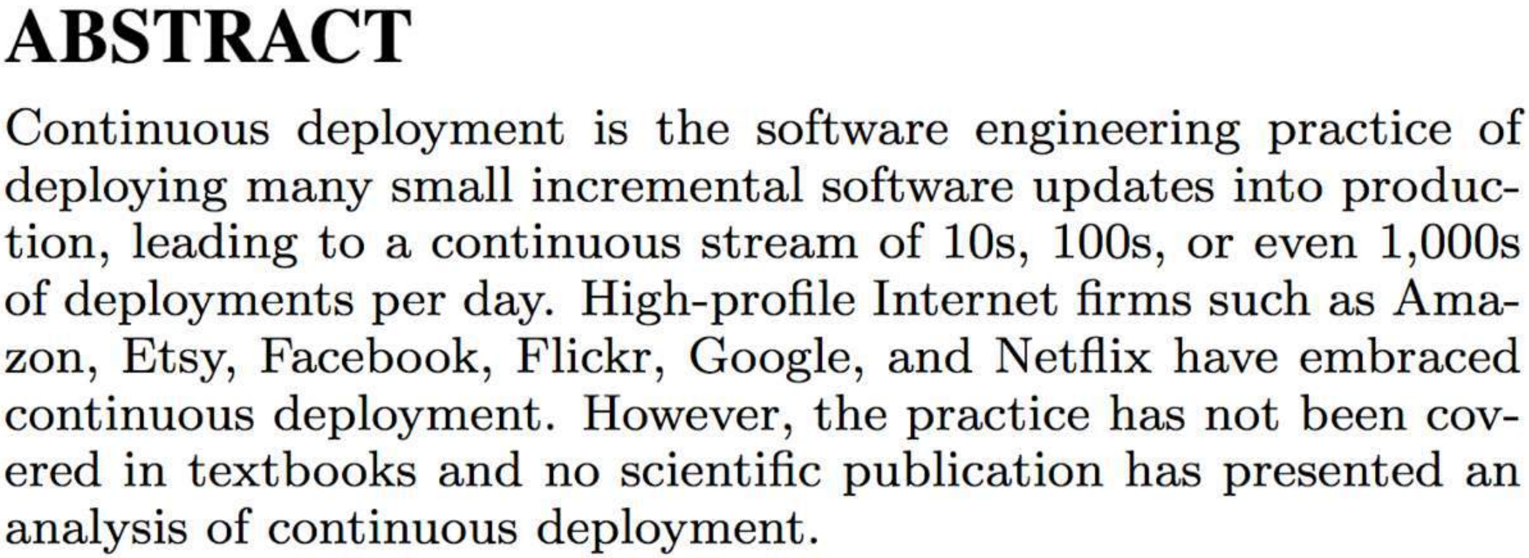
Transparency Options

- Include SBoM files with install: SWID, SPDX
  - Constrained storage? CoSWID
- Even more constrained storage? Lookup
- Publication
  - ROLIE Software Descriptor Extension
- Cataloging

Vulnerability vs. Exploitability

High Assurance SBoMs

SBoM for Services



ABSTRACT

Continuous deployment is the software engineering practice of deploying many small incremental software updates into production, leading to a continuous stream of 10s, 100s, or even 1,000s of deployments per day. High-profile Internet firms such as Amazon, Etsy, Facebook, Flickr, Google, and Netflix have embraced continuous deployment. However, the practice has not been covered in textbooks and no scientific publication has presented an analysis of continuous deployment.

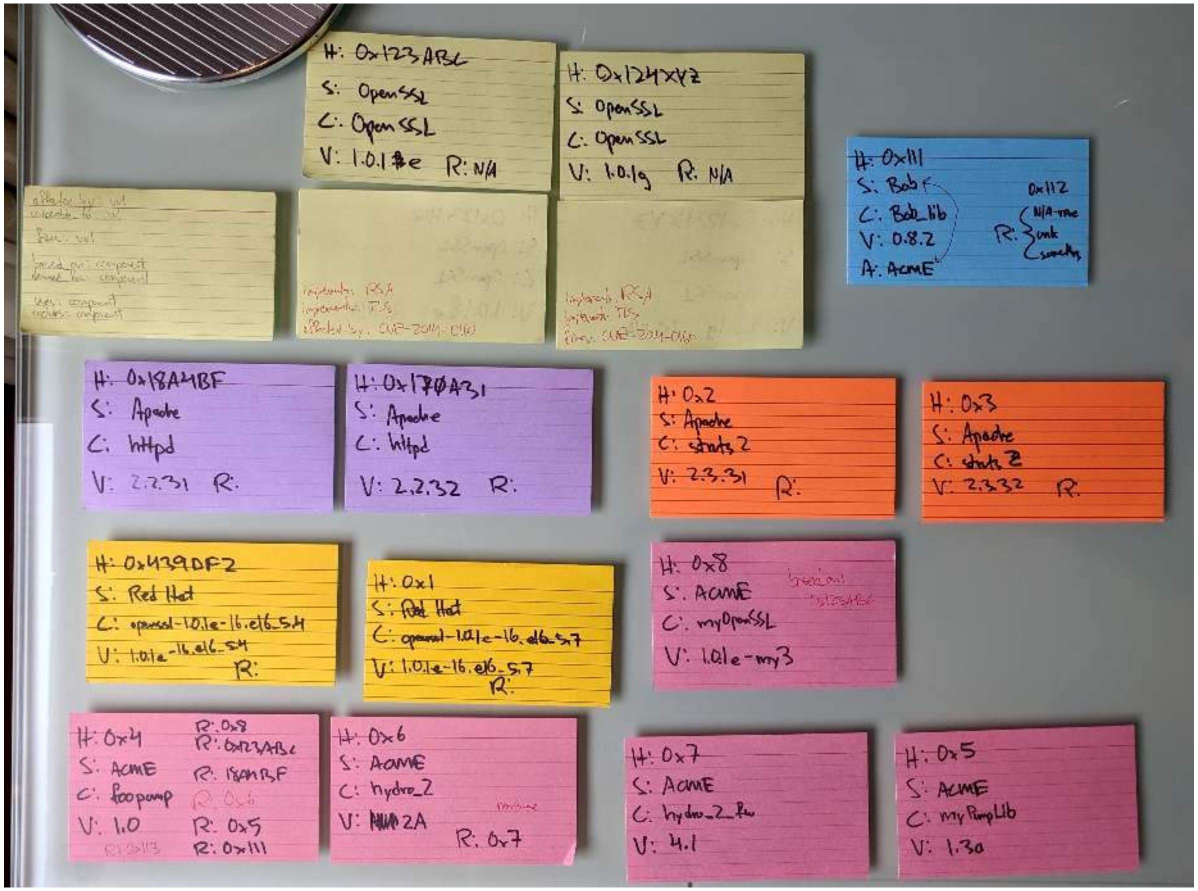
https://research.fb.om/wp-content/uploads/2017/01/paper_icse-savor-2016.pdf

Next steps

- Drafts of "minimum viable" by late June for feedback
- After minimum viable:
  - Extending the model
  - Developing and collecting tooling
  - Awareness and adoption
  - Testing ⟷ revision

Testing

- Previous attempt at CERT/CC: Component Relationship Database (CRDb)
    - Neo4j, Sesame, RDF
- Next experiment: Index cards and Sharpie



H: 0x123ABC
S: OpenSSL
C: OpenSSL
V: 1.0.1~~f~~e R: N/A

H: 0x124XYZ
S: OpenSSL
C: OpenSSL
V: 1.0.1g R: N/A

H: 0x111
S: Bob
C: Bob_lib
V: 0.8.2
A: ACME
R: 0x112 N/A-rme unk security

affected by: vul
vulnerable to: vul
fixes: vul
based on: component
derived from: component
uses: component
includes: component

implements: RSA
implements: TLS
affected by: CVE-2014-0160

implements: RSA
implements: TLS
fixes: CVE-2014-0160

H: 0x18A4BF
S: Apache
C: httpd
V: 2.2.31 R:

H: 0x17ØA31
S: Apache
C: httpd
V: 2.2.32 R:

H: 0x2
S: Apache
C: struts 2
V: 2.3.31 R:

H: 0x3
S: Apache
C: struts 2
V: 2.3.32 R:

H: 0x439DF2
S: Red Hat
C: openssl-1.0.1e-16.el6_5.4
V: 1.0.1e-16.el6_5.4
R:

H: 0x1
S: Red Hat
C: openssl-1.0.1e-16.el6_5.7
V: 1.0.1e-16.el6_5.7
R:

H: 0x8
S: ACME
C: myOpenSSL
V: 1.0.1e-my3
based on 0x123ABC

H: 0x4
S: ACME
C: foopump
V: 1.0
R: 0x8
R: 0x123ABC
R: 18A4BF
R: 0x6
R: 0x5
R: 0x113
R: 0x111

H: 0x6
S: ACME
C: hydro_2
V: 2A
R: 0x7

H: 0x7
S: ACME
C: hydro_2_fw
V: 4.1

H: 0x5
S: ACME
C: myPumpLib
V: 1.3a

To recap…

- Tracking third party components can help understand and address a wide range of risks across the entire ecosystem
- An ongoing, open process convened by NTIA is bringing together experts to address:
    - What a Software Bill of Materials is
    - Why it can help across the supply chain
    - How we can implement it
- Get involved in the NTIA process!
    - afriedman@ntia.gov @allanfriedman
    - amanion@cert.org @zmanion

phillipmartin.info