What’s in my Software?
Introducing a Software Bill of Materials Specification

Robert Martin
MITRE

Allan Friedman
NTIA
US Dept of Commerce
How many organizations can answer: Am I potentially affected by vulnerability?
Should I pay attention or look at literally anything else on the Internet?

• Transparency helps markets across the supply chain
• Progress towards SBOM and transparency
  • The *what*, the *why*, and the *how*
• Introducing a new SBOM specification
• How you can get involved
  • Join this international, cross-sector community
  • SBOM – ask for it by name!
INGREDIENTS: ENRICHED BLEACHED WHEAT FLOUR [FLOUR, REDUCED IRON, “B” VITAMINS (NIACIN, THIAMINE MONONITRATE (B1), RIBOFLAVIN (B2), FOLIC ACID)], WATER, SUGAR, CORN SYRUP, HIGH FRUCTOSE CORN SYRUP, PARTIALLY HYDROGENATED VEGETABLE AND/OR ANIMAL SHORTENING (SOYBEAN, COTTONSEED AND/OR CANOLA OIL, BEEF FAT), WHOLE EGGS, DEXTROSE. CONTAINS 2% OR LESS OF: SOY LECITHIN, LEAVENINGS (SODIUM ACID PYROPHOSPHATE, BAKING SODA, CORNSTARCH, AND MONOCALCIUM PHOSPHATE) WHEY, MODIFIED CORN STARCH, GLUCOSE, SOY FLOUR, SALT, MONO AND DIGLYCERIDES, CELLULOSE GUM, CORNSTARCH, SODIUM STEAROYL LACTYLATED, NATURAL AND ARTIFICIAL FLAVOR, SORBIC ACID (TO RETAIN FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM CASEINATE, YELLOW 5, RED 40. CONTAINS WHEAT, EGG, MILK AND SOY
Hostess Twinkies

Nutrition Facts

Serving Size: 1 Twinkie (1.3 oz/35 g)
Servings Per Container: 8

Calories: 170
Total Fat: 13g (20% DV)
Saturated Fat: 9g
Trans Fat: 0g
Cholesterol: 70mg (23% DV)
Sodium: 290mg (12% DV)
Total Carbohydrate: 18g (6% DV)
Dietary Fiber: 0g
Sugars: 12g
Protein: 1g

Ingredients:
Enriched Wheat Flour (Flour, Reduced Iron, "B" 1, Riboflavin (B2), Folic Acid), Hydrogenated Corn Syrup, Partially Hydrogenated Soybean Oil, Natural Flavor, Leavenings (Sodium Acid Pyrophosphate, Sodium Bicarbonate, and Monocalcium Phosphate), Salt, Cornstarch, Soy Protein Isolate, Calcium and Sodium Caseinate, Yellow 5, Red 40.

Contains wheat, egg, milk and soy.
INGREDIENTS: ENRICHED BLEACHED WHEAT FLOUR [FLOUR, REDUCED IRON, "B" VITAMINS (NIACIN, THIAMINE MONONITRATE (B1), RIBOFLAVIN (B2), FOLIC ACID)], WATER, SUGAR, CORN SYRUP, HIGH FRUCTOSE CORN SYRUP, PARTIALLY HYDROGENATED VEGETABLE AND/OR ANIMAL SHORTENING (SOYBEAN, COTTONSEED AND/OR CANOLA OIL, BEEF FAT), WHOLE EGGS, DEXTROSE. CONTAINS 2% OR LESS OF: SOY LEICHTIN, LEAVENINGS (SODIUM ACID PYROPHOSPHATE, BAKING SODA, CORNSTARCH, AND MONOCALCIUM PHOSPHATE) WHEY, MODIFIED CORN STARCH, GLUCOSE, SOY FLOUR, SALT, MONO AND DIGLYCERIDES, CELLULOSE GUM, CORNSTARCH, SODIUM STEARYL LACTYLATE, NATURAL AND ARTIFICIAL FLAVOR, SORBIC ACID (TO RETAIN FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM CASEINATE, YELLOW 5, RED 40.

CONTAINS WHEAT, EGG, MILK AND SOY
What is the software equivalent?
A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software.

An SBOM is effectively a nested inventory: a list of ingredients that make up software components.

An SBOM identifies and lists software components, information about those components, and the relationships between them.
Secure Development Process

Supply Chain

Risk Management

Vulnerability Management

Produce Software

Choose Software

Operate Software

SBOM
How are we going to do this?
NTIA’s Process on Software Component Transparency

Cross sector

Multistakeholder Characteristics
Open to all Stakeholders
Accountable
Transparent
Consensus Driven
Bottom up process

Open source
Middleware
Commercial SW
Embedded
Customers

Healthcare  Energy  Auto  ICT  Finance  Government

Entire Supply chain

NTIA’s open, transparent, consensus-based processes bring together diverse stakeholders can catalyze real progress across the ecosystem.
What the NTIA process is **not** doing

- Regulation
- Source code disclosure
- Standards Development
- Solving all supply chain issues
Making progress

- Clear appreciation across sectors on the potential value of transparency
- Consensus on
  - The broad scope of the problem
  - Focus on a baseline SBOM
  - Machine-readability of the solution
  - Modularity and Scalability
- Resources: ntia.gov/SBOM

✓ What is an SBOM
✓ Why should we SBOM
✓ How do we SBOM
✓ Can we SBOM today?

Current work: focus on deployment and SBOMs in the real world
What is an SBoM?
A toy example
A toy example

Carol’s Compression Engine v3.1

Bob’s Browser v2.2

Bingo Buffer v2.1

Acme Appliance v1.1

Known

Unknowns

Included in

unknown

Included in

known

Included in

partial

root
Software Components

Supplier

Component

Version

Hash
How many levels deep?

Must include all top-level includes.
Should ask for includes’ SBOMs.
Ideally makes a best-effort for all known components.
Why should we SBoM?
SBOM Roles and Benefits

**Produce Software**
- Understand component and code dependencies
- Monitoring/reviewing for vulnerabilities
- Awareness of component EOL, orphan, etc.
- Enable allow- and deny-lists
- Less unplanned maintenance work
- Transparency for customers

**Choose Software**
- Identify vulnerable components
- Compliance with policies
- Awareness of component EOL, orphan, etc.
- Show best practices by supplier
- Know and comply with licensing

**Operate Software**
- Easily ID vulnerabilities
- Better risk analysis - “Roadmap for the defender”
- Streamline administration
- Drive independent mitigations
How should we SBoM?
Translation between formats

• We have identified the common elements.
• A ‘multilingual’ ecosystem does not offer too many challenges
• Rather than pick a winner, focus on guidance to support all relevant, active, and approved formats with effective interoperability.
## Implementing core SBOM fields

<table>
<thead>
<tr>
<th>Field</th>
<th>SPDX</th>
<th>SWID</th>
<th>CycloneDX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplier</td>
<td>(3.5) PackageSupplier: &lt;Entity&gt; @role (softwareCreator/publisher), @name</td>
<td>publisher</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>(3.1) PackageName: &lt;softwareIdentity&gt; @name</td>
<td>name</td>
<td></td>
</tr>
<tr>
<td>Unique Identifier</td>
<td>(3.2) SPDXID: &lt;softwareIdentity&gt; @tagID</td>
<td>bom/serialNumber and component/bom-ref</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>(3.3) PackageVersion: &lt;softwareIdentity&gt; @version</td>
<td>version</td>
<td></td>
</tr>
<tr>
<td>Component Hash</td>
<td>(3.10) PackageChecksum: &lt;Payload&gt;/../&lt;File&gt; @[hash-algorithm]:hash</td>
<td>hash</td>
<td></td>
</tr>
<tr>
<td>Relationship</td>
<td>(7.1) Relationship: CONTAINS &lt;Link&gt;@rel, @href</td>
<td>(Nested assembly/subassembly and/or dependency graphs)</td>
<td></td>
</tr>
<tr>
<td>SBOM Author</td>
<td>(2.8) Creator: &lt;Entity&gt; @role (tagCreator), @name</td>
<td>bom-descriptor: metadata/manufacture/contact</td>
<td></td>
</tr>
</tbody>
</table>
Healthcare Proof of Concept
A new SBOM standard!
What’s coming next from the SBOM community

- Refining and extending the SBOM approach
  - Software namespace
  - Mechanisms for sharing SBOM data
  - Vulnerability vs Exploitability
  - High assurance: integrity, pedigree, provenance
  - Cloud & containers
  - Dock with other efforts around supply chain

- Tooling for automation
  - What tools exist today?
  - What tools do we need?

- Awareness and adoption
  - Get the message to the community
  - Draft contract language
  - Further demonstrations in different sectors

- Playbooks and how-to guides
To recap...

• Tracking third party components can help understand and address a wide range of risks across the entire ecosystem
• Cross-sector supply-chain driven approach
  • What a Software Bill of Materials is
  • Why it can help across the supply chain
  • How we can implement it
• Sectors and orgs can shape their own future through Proof-of-Concept exercises
• New standards emerging for even more power and options
• Ongoing work needs your help to build and use SBOM data

Get involved in the NTIA process!
Contact: afriedman@ntia.gov
Read: ntia.gov/SBOM
Join the conversation
@allanfriedman #SBOM