RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: MBS-R12

TRANSPARENCY OF SW COMPONENTS: AN OPEN APPROACH TO BILL OF MATERIALS

Allan Friedman

Director of Cybersecurity
National Telecommunications & Information Administration
US Department of Commerce
@allanfriedman

Should I pay attention or look at my phone?

Tracking and communicating third party components in software and IoT with a "**software bill of materials**" can

- Improve and communicate secure development practices
- Help enterprise customers protect themselves
- Foster better markets for secure products

The US Department of Commerce is convening an open and consensus-driven **multistakeholder process** to develop a shared vision around SBOM and software transparency

We need your help!

SO… WHAT IS AN SBOM, ANYWAY?

Bill of Materials

In the manufacturing world, we track parts and components used in assembly to understand the manufacturing and maintenance process.

So why not software?

Third party components **and dependencies**

Need to capture not just the top-line packages, but each component that will ship with the product.

An example

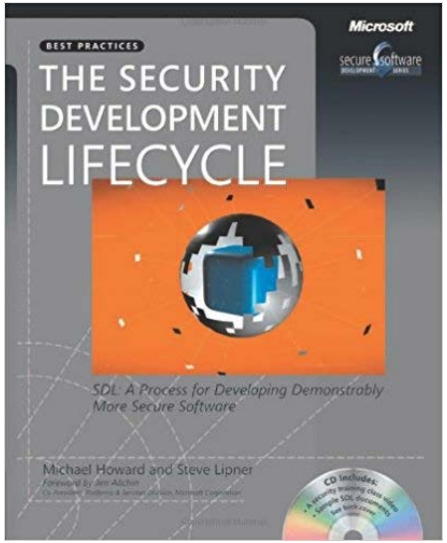
Mercedes published a list of the open source licenses that shipped with the 2013 S-Class. It included libtiff, netcat, and libpcap.

WHY SBOM?

Vendor perspective: Know what you ship

Software vendors should have a clear understanding of what is heading to customers

Vendors Perspective: SDL

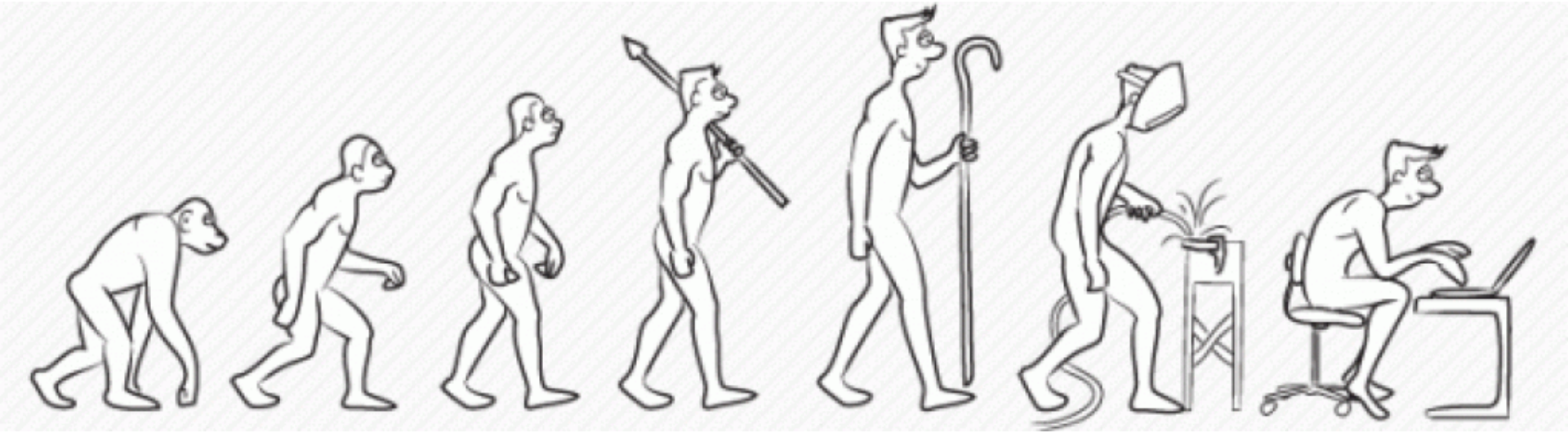


Understanding third party components is integral to a security development lifecycle. It's hard to claim that you have one without tracking third party components.

Vendor perspective: SMEs

An SBOM can signal quality and process, fostering confidence.

Vendor perspective: Mature Companies



A clear SBOM strategy can enable bottom-up tracking of inputs and top-down audit for quality, risk management, and compliance.

Enterprise Perspective

Can't Defend What You Don't Know About

An SBOM isn't a panacea, but knowledge of risks is key

Enterprise Perspective: Acquisition

When comparing two solutions,
an this information can inform the decision from a security perspective.

Enterprise Perspective: Emerging Risks

An enterprise with SBOM-supported products can prioritize a response to newly discovered (or exploited) vulnerabilities.

Enterprise perspective: Isolate potential risks

Not everything can be easily patched, even if a patch is available.
Organizations can take other mitigation steps when they identify potential risks.

Enterprise perspective: Full lifecycle management

When a product is no longer supported, or the vendor goes out of business, owners can make better decisions about how to protect themselves.

IT CAN'T BE THIS EASY, CAN IT?

This isn't a new idea, and there are real challenges that we, as a community, need to understand and tackle together.

Challenge: Namespace

Different vendors may refer to software components differently. Solving a global namespace problem is very hard. We should resist attempts for a single authoritative source. Fortunately, some solutions exist.

Challenge: How can this data be useful?

Integrating this data into vulnerability management processes and tooling.

Challenge: Design considerations & Data

- A standardized solution across sectors can make this much easier
- To avoid going stale, data needs to be versioned, and included in updates.
- Machine readability is necessary to reap gains from automation from vulnerability management tools.

Challenge: Design considerations & Data

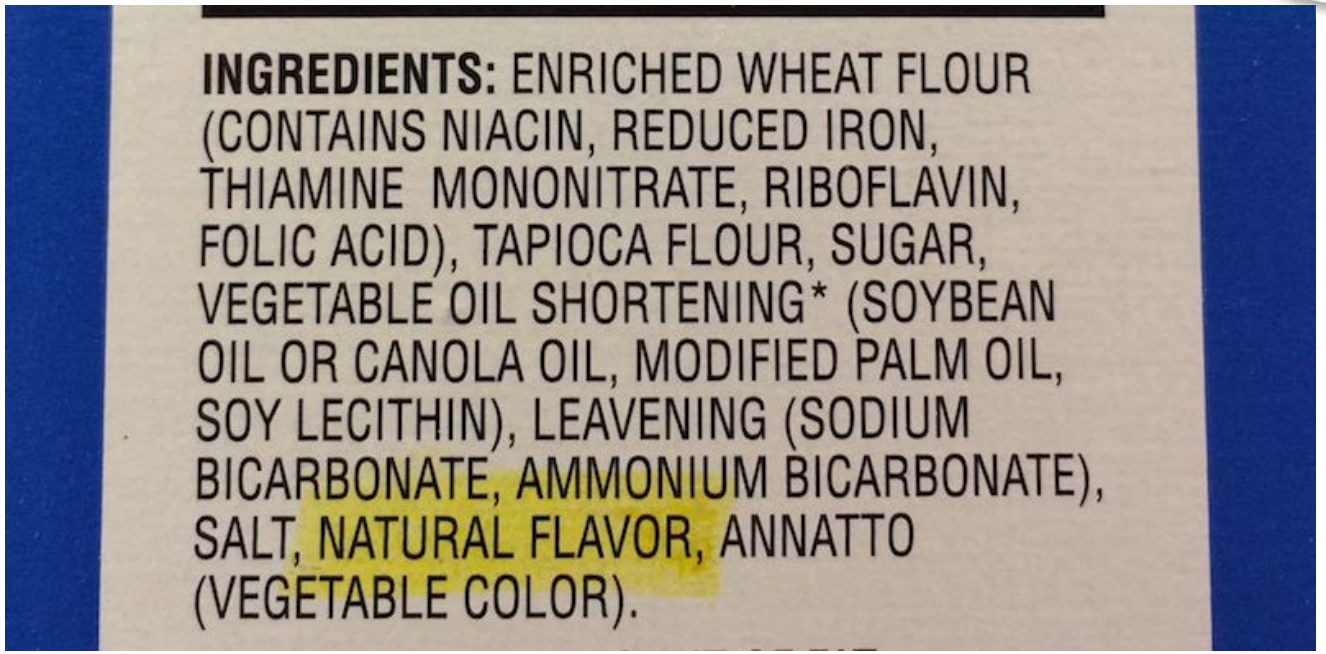
- A standardized solution across sectors can make this much easier
- To avoid going stale, data needs to be versioned, and included in updates.
- Machine readability is necessary to reap gains from automation from vulnerability management tools.

DATA ABOUT DATA ABOUT DATA

Challenge: IP concerns

Vendors may well be concerned about exposing trade secrets if they disclose every single component in their software.

Challenge: IP concerns (cont'd)



A 95% complete SBOM can still be very valuable to the customer.
We need to explore how to communicate the "and natural flavorings" aspect.

Challenge: **Vulnerability** vs **Exploitability**

Vendors can communicate risk (or the lack thereof) with their customers.
We need to enable this process.

What current SBOM solutions don't address

- Configuration risks
- Compiler details
- Hardware manifests

There may be value in using what we have, and addressing these concerns in the future.

HOW WE CAN MOVE FORWARD

Collaboration at the Commerce Department

Standards

The National Institute of Standards and Technology is going to continue its work on SWID tags.
See NISTIR 8060!

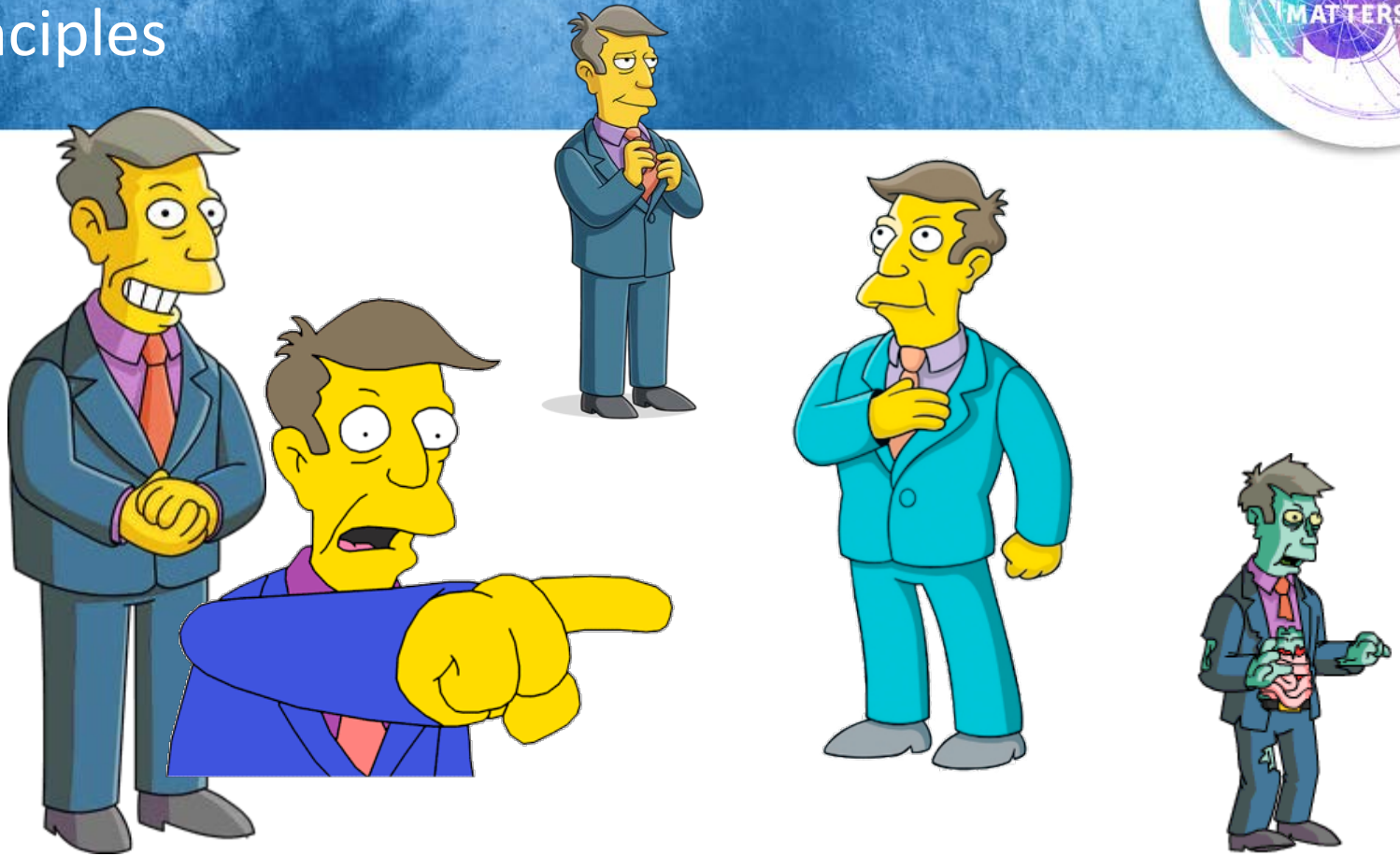
The policy side

Beyond the technical aspects, we need to focus on awareness, adoption, incentives, and understanding further barriers and concerns.

The “multistakeholder process”

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

Principles



Recognition of the dangers of one-size-fits-all

Avoid reinventing the wheel

Stakeholder driven

To recap…

- Tracking third party components is an important part of a secure development process.
- Awareness of reused software makes all of us more secure.
- Transparency about software components can align incentives and foster more efficient, security aware markets.

Applications: What you can do

Short term

- Vendors: Ask real questions about whether your org could do this today. Why not?
  - How can you start building this in your org?
- Enterprises: Would this be useful today? How?
  - What would it take to ask for these from your vendors?
- Policy: What are the concerns? The risks? The barriers?

Medium Term

- Standards: https://csrc.nist.gov/Projects/Software-Identification-SWID
- Stay tuned for the NTIA announcement!
  - Contact afriedman@ntia.doc.gov