draft-lear-opsawg-mud-sbom

28 Jul 2020

Eliot & Scott

What is an SBOM?

- Software Bill of Materials – a manifest of software contained in a package or on a device.
- On Linux systems, think:
  - “apt” or /var/lib/dpkg/status or…
  - “rpm –qa”
- (At least) three emerging standards to describe a software bill of materials
  - SPDX (spdx.org)
  - SWID (ISO 19770)
  - CycloneDX

IETF

What can SBOMs be used for?

- Upstream license management
- Cybersecurity vulnerability analysis
- Dependency analysis for critical systems

What does this have to do with the IETF?

- Need a discovery mechanism for devices that connect that have SBOMs
  - Is the SBOM on the device itself?
  - Is the SBOM somewhere in the cloud?
  - Does the owner have to call or email to get at it?
- What format is it in?
  - SWID, CycloneDX, SPDX, Microsoft Excel, …

draft-lear-opsawg-mud-sbom

- Extends MUD to indicate that a device has an SBOM associated with it
- Allows for local, cloud, and “call me” use cases
- Specifies mechanism for local access (e.g., coap, http)
- Local access makes use of .well-known registry
- Relies on underlying protocols to specify which format is being served up (we call these … “media types”)
- Relies on underlying protocols to establish whatever necessary security model is required for access

Open Questions

- What if there is more than one (perhaps disjoint) SBOM on a device?
  - Today's assumption is that there would be a link inside the SBOM to this other object
- Should SBOMs be searchable?
- Should particular packages in SBOMs be directly addressable?
- **MOST IMPORTANT**: Just because a package with a particular name (like OpenSSL 1.0.1b) is on a system doesn't mean that it is vulnerable

Next Steps

- Want to pace the work with other efforts
- Need to get an answer on “multiple SBOMs”
- Liaise this work with others for input?
- How to address whether system is patched or actually vulnerable?

- WG Interest?