draft-ietf-sbom-access-02

Eliot Lear

Scott Rose

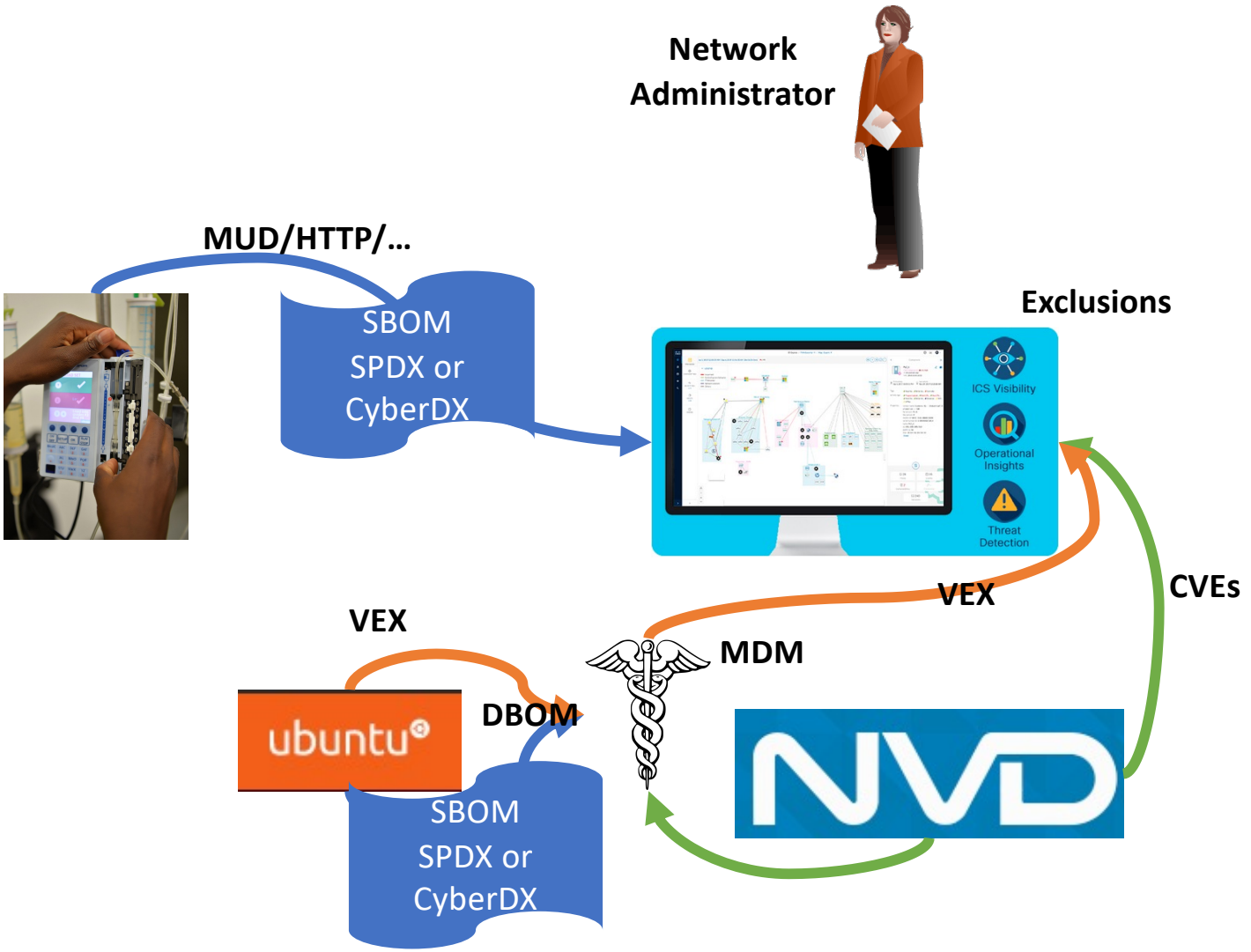
What is all this about?

- What software is on a system?
- What vulnerabilities does that software have?

Changes since -01

- Added support for vulnerability information (see next slide)
- Reworded introduction to make clear the motivation
- Redid the /.well-known prefix to handled both vuln and sbom
- Added support for openc2
- Fixed versioning so that only cloud-based access has versioning
- mudmaker.org/test has the capability

System view


Network Administrator
MUD/HTTP/…
SBOM SPDX or CyberDX
Exclusions
ICS Visibility
Operational Insights
Threat Detection
VEX
CVEs
VEX
MDM
DBOM
ubuntu
NVD
SBOM SPDX or CyberDX

Different methods

- On the box
  - For fast changing devices that have lots of capability
- Off the box
  - For limited capability devices that have no retrieval interfaces
- OpenC2 On the box
  - For those who implement the OpenC2 framework

Format Neutral

The model

```
module: ietf-mud-transparency
  augment /mud:mud:
    +--rw transparency
       +--rw (sbom-retrieval-method)?
       |  +--:(cloud)
       |  |  +--rw sboms* [version-info]
       |  |     +--rw version-info    string
       |  |     +--rw sbom-url?       inet:uri
       |  +--:(local-well-known)
       |  |  +--rw sbom-local-well-known?   enumeration
       |  +--:(sbom-contact-info)
       |     +--rw sbom-contact-uri         inet:uri
       +--rw (vuln-retrieval-method)?
          +--:(cloud)
          |  +--rw vuln-url?                inet:uri
          +--:(vuln-local-well-known)
          |  +--rw vuln-local-well-known?   enumeration
          +--:(vuln-contact-info)
             +--rw contact-uri              inet:uri
```

Open Questions

- Does it make sense for vulnerability information to be available “on the box”?
- Do we have the correct security model (leave it to HTTP/CoAP/OpenC2)?
- Do we want to support CoRIM/CoSWID?
  - Yes, we’re format-neutral, but these two are sort of SBOMs sort of not.
  - Henk can say more

Proposed next steps

- Request early reviews?
  - /.well-known URI review
  - Security review
- Aim for WGLC before next IETF
  - Depending on what you have to say and what the reviews say

draft-lear-opsawg-ol-01

- Problem
  - Carsten felt he couldn’t copy MUD files because there was no permission to do so
- Solution
  - Include a list of owners and an SPDX licensing tag field or a URL in a MUD file
  - Allow the grouping to be used by others as well.

The model

module: ietf-ol

```
augment /mud:mud:
  +--rw ol
     +--rw owners*              string
     +--rw (license-type)?
        +--:(spdx-lt)
        |  +--rw spdx-tag?      string
        +--:(url)
           +--rw license-info?   inet:uri
```

Why adopt this draft?

- Providers of MUD files who want their stuff copied can’t give permission
- We won’t be the only serialized YANG module with this problem

Discuss