Why Cyber Labeling Research?

• “U.S. Cyber Trust Mark” program initiated in 2023 to be led by FCC to “help Americans more easily choose smart devices that are safer and less vulnerable to cyberattacks.”¹

• DOE initiated research to develop a proof-of-concept for cybersecurity labeling for energy products to explore the best methods to present information about security features in energy products to inform consumer decisions.

• Focused on market-facing products: solar inverters and smart meters.

• Output: final research report detailing the results of the pilot and making recommendations to an expanded OT labeling program.
Overlap with SBOM

- Emphasis on information disclosure and transparency
- Goal of promoting energy sector security
- Where else is there overlap?
Who is involved?

• Funded by President Biden’s Bipartisan Infrastructure Law, via DOE CESER²
• Led by a collaborative team of researchers from six National Laboratories (NREL, ORNL, SNL, INL, PNNL, LLNL)²
• Informed by feedback from five volunteer vendor partners with inverter and smart meter products
• In its proof-of-concept phase, the project will seek feedback from broader audiences (auditors, other vendors, the “general public”, you)
• Final implementation decisions will be made by the FCC. If implemented, participation would be voluntary and available to energy sector vendors.
Process so far

• Assessed 19+ standards/recognized research/legislation pertaining to labeling, privacy, and security for IoT and IIoT
  • Key takeaway: no existing standard or labeling regime adequately addresses privacy and security concerns applicable to energy sector ICS technologies such as smart meters and inverters.

• Consulted with policy and technology experts from 5 volunteer vendors, both in 1-1 interviews and group workshops
  • Key takeaway: any label for energy IIoT should be informational (displaying disclosures about security and privacy measures) rather than assessment or certification-based (displaying a rating or seal of approval), due to the context-dependent and highly variable nature of security in these environments.

• Produced an initial mockup of a label and associated data-request form, which will be used to run a pilot/proof of concept with vendor partners.
Building the Label Requirements

• For each proposed data field, lab researchers answered the following questions:
  • How do we describe this element?
  • What types of data could fill this field?
  • What function does inclusion of this element fill?
  • Is it verifiable and/or immutable?
    • How could it be verified? By whom?
    • How do we address elements that are subject to change over time?
  • Is it applicable to smart meters and inverters?
  • Does it map to commonly used standards and best practices?
  • Who does the information provide value to?
Challenges with SBOM inclusion

• Concerns about public SBOM disclosure
• Concerns about public interpretation of SBOMs
  • How to interpret relevance of vulnerability announcements, etc.
• Concerns about maintaining up-to-date, accurate information
21. Hardware Bill of Materials (HBOM)

*Hardware Bill of Materials (HBOM)* refers to a listing of the components (circuit boards, chips, etc.) within a hardware system.

Do you maintain an HBOM for this system?  

- [ ] Yes  
- [ ] No

Is it available upon request?  

- [ ] Yes  
- [ ] No

**Add'l text box will populate if “Yes” is selected:**  To whom and under what conditions may an HBOM be made available?

22. Software Bill of Materials (SBOM)

*Software Bill of Materials (SBOM)* refers to a listing of components (e.g. applications, libraries, files and folders) within a software package.

Do you maintain an SBOM for this system?  

- [ ] Yes  
- [ ] No

Is it available upon request?  

- [ ] Yes  
- [ ] No
Questions

• Can including SBOM in a cybersecurity label help promote acceptance of SBOM?
• How can we best include it?
• What challenges have you faced?
• Are there goals of SBOM that can be achieved through a cyber label or vice versa?
Thank You

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER
Bills of Materials (BOMs)

• What is in system?
  ▪ All the objects for a piece of hardware or software
  ▪ Includes how the objects are related
  ▪ Metadata
    ✓ Part Number
    ✓ Vendor
    ✓ Country of Origin
    ✓ Version

• Required for all software sold to US Government

• No standard format
Comparing Bill of Materials

Questions to Answer

- How do different versions of a BOM compare?
- How do BOMs change over time?
- When there are multiple BOMs for a system, are they the same?
- How similar are the underlying systems of the same model and versions?
- How are classes of systems similar?
- How can we easily identify the differences between two BOMs?

Current Methods

- Set comparisons
- Spreadsheets
- Tabular comparisons
- Side by side version comparisons

The methods don’t account for relationships and can be difficult with large BOMs.
BOMs as Graphs

- Objects become nodes
- Relationships become edges
  - Physical connections
  - DLL calls
  - File structure
  - Package imports
- Metadata becomes attributes in graph

```
---

acme-application  ms-2.example.com

API Gateway

ms-1.example.com  ms-3.example.com

ms-1-pgsql.example.com  s3-example.amazon.com
---
```

CycloneDX SaaS\text{BOM} example*

*https://github.com/CycloneDX/bom-examples
Comparing Graphs
How similar are two graphs? Where are the differences?

Methods
• Distance Methods
• Spectral analysis
• Clustering Techniques
• Deep Learning
• Node Correspondence

Gaps in Current Methods
• Work on specific family of graphs
• Focus on graph structure
• Attributes
• Global solutions
• Do not predict individual possible mappings
• End-to-end solution
Overall Approach
Method

- Based on Depth First Search
  - Linear time graph traversal
  - Parallelized
- Considers neighbors of a node as well as multiple attributes
- Incorporates record linkage
- Can predict non-exact matches
Supernodes

- In large graphs, can be difficult to see differences, especially with overplotting
- Collapse leaf nodes of same neighbor into supernode
- Can spot differences more easily

Images of large SBOM compared with manually modified copy
SBOM Graph Comparison

CycloneDX open source SBOMs

Proton-bridge v.1.6.3

Proton-bridge v.1.8.0

Proton-bridge Combined
HBOM Graph Comparison

Version 1 of hardware

Version 2 of hardware

Merged Graph – Blue indicates nodes in both
Predicting Possible Node to Node Correspondence

- Reran algorithm on nodes that are not in both graphs using fuzzy matching (Jaro-Winkler)
- Overlay predicted edges (in green)
- Found differences that could be user error S/5
Conclusion

• Created new end-to-end system to compare Bill of Materials
• Graph representation improved analysis compared to sets and lines of code
• Quick algorithm and collapsing supernodes accommodate large BOMs
• Interactive visualization allows for differences in BOMs to be quickly identified
• Were able to find locations of discrepancies in BOMs in hardware
Future Work

• Compare multiple Bills of Materials at a time
• Consider directed graphs
• Account for types of edges/edge attributes
• Identify subgraphs of interest
Acknowledgements

• The Department of Energy (DOE)
• The Cybersecurity Energy Security, and Emergency Response (CESER)
• The Cyber Testing and Resilience of Industrial Control Systems (CyTRICS) Program
  • Idaho National Laboratory (INL)
  • Lawrence Livermore National Laboratory (LLNL)
  • National Renewable Energy Laboratory (NREL)
  • Oakridge National Laboratory (ORNL)
  • Sandia National Laboratory (SNL)
Thank you