INL/EXP-24-79647-Revision-0

Visualizing a Vulnerability: Its Connections to Hardware and Software

August 2024

Benjamin Aaron Keller

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/EXP-24-79647-Revision-0

Visualizing a Vulnerability: Its Connections to Hardware and Software

Benjamin Aaron Keller

August 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Final Edge of Poster

Visualizing a Vulnerability:

Its Connections to Hardware and Software

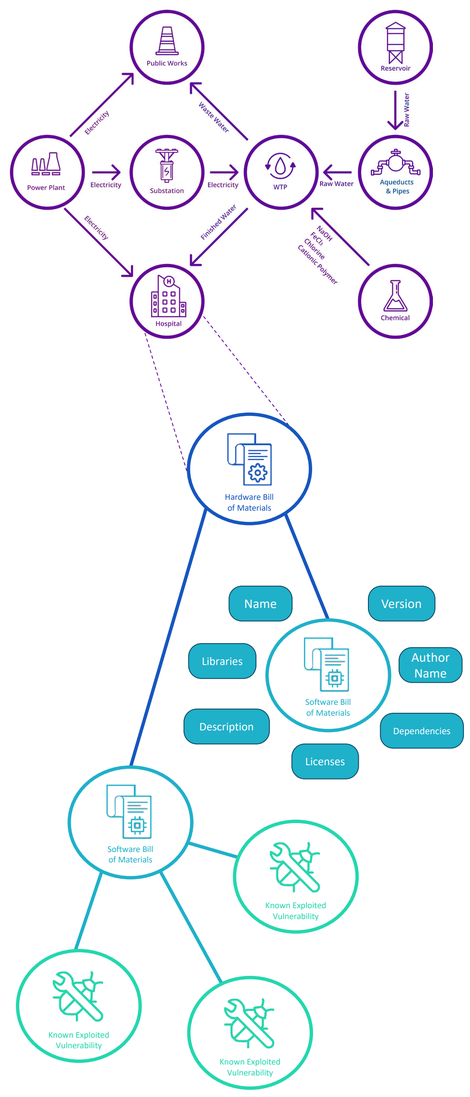
Ben Keller | Kansas State University | D570 | Michael Hoover, Kyle Hanson

Context & Objective

All Hazards Analysis (AHA) is a framework developed by Idaho National Laboratory that provides capabilities to collect, store, analyze, and visualize critical infrastructure information. A core function of AHA is its ability to simulate faults or outages in networks of infrastructure originating from a plethora of causes, ranging from natural disasters to cyberattacks.

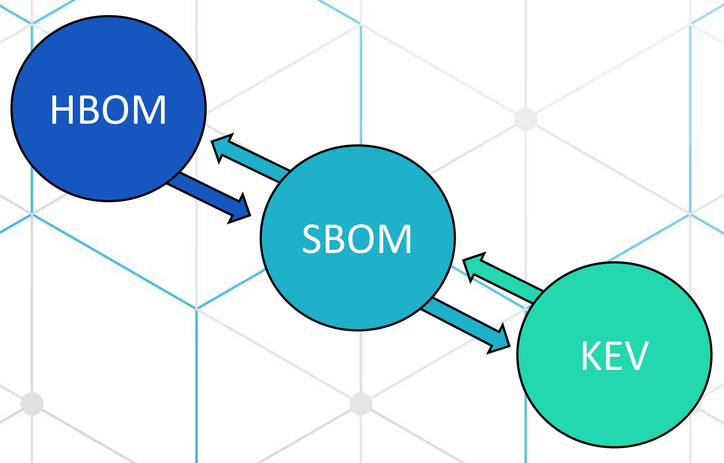
AHA utilizes Hardware and Software Bills of Material (HBOM and SBOM, respectively) along with Known Exploited Vulnerabilities (KEVs) to document the potential attack vectors for each piece of infrastructure.

The objective of this contribution to AHA was to create a visualization tool that could capture the small details held in each individual artifact as well as preserve the large-scale connections that link them together to aid threat modeling.

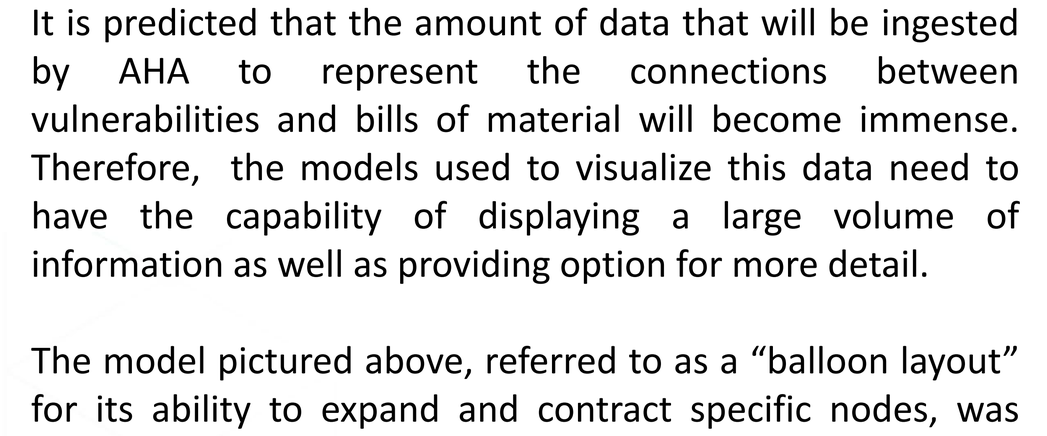


Hierarchy Design

To best suit the dynamic nature of its use, a flexible, two-way hierarchy design was employed (pictured below). This means that either an individual HBOM or KEV could act as the "top" of the hierarchy, and the subsequent elements can be accessed from them.



Large Dataset Visualization



It is predicted that the amount of data that will be ingested by AHA to represent the connections between vulnerabilities and bills of material will become immense. Therefore, the models used to visualize this data need to have the capability of displaying a large volume of information as well as providing option for more detail.

The model pictured above, referred to as a "balloon layout" for its ability to expand and contract specific nodes, was selected for its ability to concisely display individual HBOMs, SBOMs, and KEVs and for its efficiency dealing with large data sets.

The Graph Info panel to the left of the diagram provides additional functionality to complement user experience. Selecting any of the nodes present on the following graph will display additional information about it, which can be found on the bottom half of this panel

Conclusion

The BOM Visualizer is a tool intended to function as an aid to a user of AHA in understanding the dynamic between a particular entity, whether it be an SBOM, HBOM, or KEV, and its connections/dependencies.

Future work on this project will consist of equipping AHA with the capability of handling KEV data through imports and including features that allow analysts to build the dependencies between KEVs and their associated SBOMs. Once this is complete, it will be possible to expand the BOM Visualizer to include KEV data.

Final Edge of Poster

Not available for content • Not available for content • Not available for content • Not available for content