INL/EXP-24-79580-Revision-0

Intern Poster: AIBOMs in Automated Defense: Capabilities & Challenges

August 2024

Faith Kimberley Coslett

Changing the World's Energy Future

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

INL/EXP-24-79580-Revision-0

Intern Poster: AIBOMs in Automated Defense: Capabilities & Challenges

Faith Kimberley Coslett

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

AIBOMs in Automated Defense: Capabilities & Challenges

Intern: Faith Coslett (D520) | University of Wyoming | Mentors: Rita Foster, Zachary Priest, Manuel Vazquez

Problem

- AI is widespread in critical infrastructure and supply chains
- AI is often a black box—can't see "inside" of it, don't understand how it arrived at output
- **Software bill of materials (SBOM)** is like an ingredients list for software
- **AIBOM**, an SBOM for an AI model, might detail its weights, training data, components, hardware, licenses, etc. [1]
- AIBOM is a new concept, so there's a current lack of supporting infrastructure and standardization
- Competing emerging standards (**CycloneDX**, **SPDX**) differ, and none include all desired components [3] [4]

Opportunity

- AIBOMs increase transparency and accountability of AI
- Easy identification of AI's components means more informed evaluation of its risk before use and of vulnerability applicability in the future
- AIBOMs are machine-readable (e.g., **JSON**, **HTML**)
- Can leverage this for automation:
  - Enrich AIBOMs with details from a dataset
  - Incorporate AIBOMs into automated incident response
  - Use AIBOMs in INL tools (e.g. **STIG**, **@DisCo**)

Challenges

- SBOMs often contain inaccurate/incomplete/outdated info
- Can happen whether SBOM was made manually or automatically generated
- SBOM must be updated with each change to a product

- Automatic generation and enrichment of AIBOMs brings possibility of false positives and false negatives being added
- Exacerbated by lack of standardization and available tools

- Dealing with proprietary information and internal data
- Developers may be discouraged from using AIBOMs or including everything they should due to worries of exposing information or losing intellectual property

Solutions

- Use integrity checker methods on SBOMs
- Machine learning and binary analysis can help validate it and compare it to other versions
- Automate update and validation steps within workflow

- Include as much context as possible in AIBOMs
- Use multiple information sources when generating/enriching to make more educated decisions on what to include or not
  - For example, ranking candidate vulnerabilities to add by using multiple vulnerability databases

- AIBOMs do not need to be public
- Can be internal and shared to verified users as needed
- Patents, algorithms, and intellectual property are not necessary properties of an AIBOM

Importance

- AI is only getting more popular and is already used in critical infrastructure and supply chains
- Knowing what's in our tools and responding quickly to risks is crucial to national security
- SBOMs are beginning to be included in legislation
  - **EO 14028** mandates that all software vendors to the US government provide SBOMs for their products [2]

Conclusion

- AIBOMs have a large opportunity to be leveraged in automated defense capabilities, incident response, and trustworthy AI
- Standardization and integration of AIBOMs into workflows will require time and resources, but would alleviate many of the challenges
- Given AIBOMs' potential for security, the investment is worth it

[1] https://c2a-sec.com/its-time-to-talk-about-ai-ml-bom-artificial-intelligence-bill-of-materials-and-vulnerability-management/
[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[3] https://cyclonedx.org/capabilities/mlbom/
[4] https://spdx.dev/learn/areas-of-interest/ai/

www.inl.gov
INL/EXP-24-79580

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy