Knowledge Graph to Detect Trustworthiness of Hardware in Supply Chain

Rakesh Kandula, Dr. Cogan Shimizu
kandula.15@wright.edu, cogan.shimizu@wright.edu
Computer Science & Engineering
KASTLE Lab, Joshi 390

Introduction

- Knowledge Graphs (KG) are used in many fields to get the inferences/insights.
- The application of any technology to safeguard the security and maintain trust is always an interesting aspect. That is what excited us to explore this field.
- The main aim of research is to know whether the hardware/components trusted or not.
- Schema Diagram is used to get an understanding of the Knowledge Graph.

Product Knowledge Graph

- Product Knowledge Graph contains all the details about the product, and it's associated parts along with the manufactured location, organization that is acquired.

Vulnerability Knowledge Graph

- Hardware Vulnerability Knowledge Graph that consists all the details and information about the vulnerability and the product it effects.
- Potential database to get the vulnerabilities are CPE, CVE and NVD database.
- There are different vulnerability types i.e., Software, OS, Application, Vulnerability. To group the hardware type vulnerabilities, NLP and NER techniques are used.

KG Schema Design

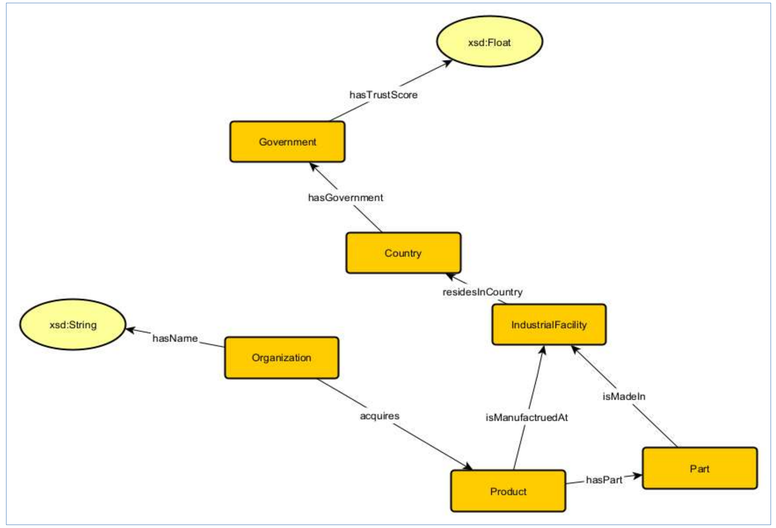

Image 1: Product KG Schema

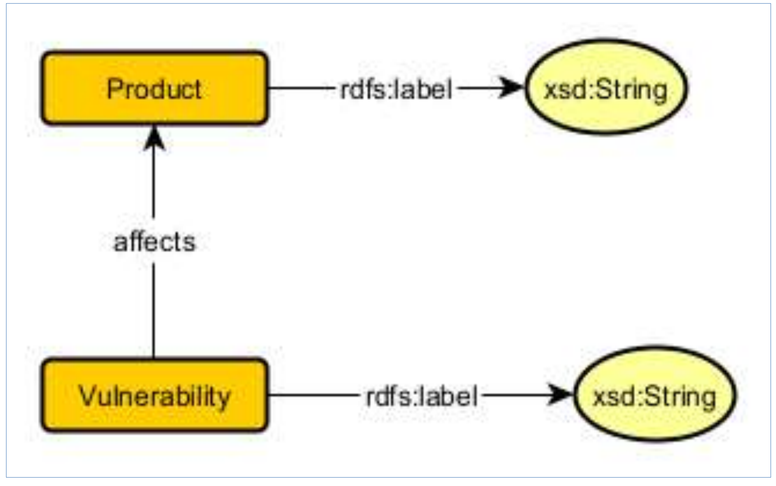

Image 2: Hardware Vulnerability KG Schema

Knowledge Graph Merging and Embedding

- Post creation of the knowledge graphs, both KGs are merged and embedded using KG Embedding techniques.
- TransE, TransR, TransH, ComplEX, RotatE are different types of embedding models.

Knowledge Graph Output

```
@prefix kastle: <https://kastle-lab.org/ontology/> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix schema1: <http://schema.org/> .

kastle:CPU a schema1:Product ;
    rdfs:label "CPU" .

kastle:Intel_i5 a schema1:Product ;
    rdfs:label "Intel_i5" .

kastle:M1_chip a schema1:Product ;
    rdfs:label "M1_chip" .

kastle:Meltdown a schema1:Vulnerability ;
    rdfs:label "Meltdown" ;
    kastle:affects kastle:CPU,
        kastle:Intel_i5,
        kastle:M1_chip .
```

Future Directions

- The work done in this field can be extended to several other fields where security and trust plays crucial role.
- The research conducted now helps future researchers exploring the field of Hardware Trustworthiness in different life spans of Hardware including supply chain.

Acknowledgement: This research work was funded by the Assured Digital Microelectronics Education & Training Ecosystem (ADMETE)