Knowledge Graph Construction for Detecting Cybersecurity Attacks

Shraddha Mukesh Makwana
University of Alberta
smakwana@ualberta.ca

Pranjal Dilip Naringrekar
University of Alberta
naringre@ualberta.ca

1 Overview of Idea

The main focus of our project is to develop Cybersecurity Knowledge Graph (KG) to assist the Security Analyst to make informed decisions about an attack by querying the system. Our project is divided into three sub-categories. First, we would gather data and perform filtering based on the required cybersecurity text. Second, we will identify entities using Named Entity Recognition (NER) and extract the relationship amongst these entities using Transformer Based Model to create semantic triplet. Lastly, we would construct a KG that can be queried. Our aim is to build a relation extraction model which will be a classifier that predicts a relation 'r' for a given pair of entities e1, e2.

For instance, 'cache' and 'Out-of-order execution' are related to one another resulting in attacks like Spectre and Meltdown. If these entities are searched on google it would not be able to relate it to an attack, however, our relation extractor will make sure to find the relation 'combined with' between these two entities.

2 Overview of Timeline

Table 1 specifies a broad overview of a sequence of tasks in given time along with its status.

3 Achieved Tasks

We began by iterating over the problem statement in order to grasp all of the possible solutions. To understand the existing solutions and their limitations, we did a detailed literature review.

Then we were able to extract cybersecurity text from publicly available information sources, including Microsoft and Adobe Security Bulletins, the CVE Corpus, Cybersecurity blogs, and technical publications. We had to use an open source library (nltk) to extract text from HTML, PDF, JSON, and XML sources as we required it in raw text. "Linux is affected by CVExx" is an example of cybersecurity text after pre-processing.

Finally, we concentrated on extracting cybersecurity entities from raw text. NER, which was designed and used in the CyberTwitter system (Mittal et al., 2016), was employed for this purpose. It generates a key-value pair with an entity as the key and a class as defined in the Unified Cybersecurity Ontology 2.0 (Syed et al., 2016).

4 Subsequent Tasks

Currently, we are focused on using a transformer-based model called BERT to extract relations for extracted entities. Model will be fed with a pair of named entities vector embeddings built using the Word2Vec model (Mikolov et al., 2013), which was trained on a cybersecurity corpus and converts it to a vector of fixed dimensions.

Afterwards, we'll construct KG using the produced triples and save it in Neo4j (López and Cruz, 2015). The evaluation will be based on relationships that have been manually annotated by cybersecurity specialists and also relations derived from corpus. Precision (Correct Relation Triples to All Extractions), Recall (Correct Relation Triples to Ground Truth), and F1-Score would be calculated.

Task	End Date	Status
Literature Review	15th Feb	Done
Preprocessing	20th Feb	Done
Extract Entities	28th Feb	Done
Extracting Relationship	5th Mar	In-Progress
Generate Relation Triples	10th Mar	To-Do
Constructing KG	17th Mar	To-Do
Evaluation	24th Mar	To-Do
Buffer For Blockers	1st Apr	To-Do
Report and PPT	5th Apr	To-Do

Table 1: Plan for Completion of the Project.

References

Félix López and Eulogio Cruz. 2015. Literature review about neo4j graph database as a feasible alternative for replacing rdbms. *Industrial Data*, 18:135.

Tomas Mikolov, Kai Chen, Greg Corrado, and Jeffrey Dean. 2013. Efficient estimation of word representations in vector space.

Sudip Mittal, Prajit Das, Varish Mulwad, Anupam Joshi, and Tim Finin. 2016. Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities.

Zareen Syed, Ankur Padia, Tim Finin, Lisa Mathews, and Anupam Joshi. 2016. Uco: A unified cybersecurity ontology.