Siri Bromander

COINS Winter School Finse 2017: IMT6002

02/05/2017

TOCSA: Threat Ontologies for CyberSecurity Analytics

Project owner: MNEMONIC AS

Project Manager and company supervisor: Dr. Martin Eian, MNEMONIC AS

Ph.D. Candidate: Siri Bromander

Supervisor: Prof. Audun Jøsang, University of Oslo and Dr. Christian Johansen, University of Oslo.

Duration: August 2016 – July 2020

Project Summary

Threat Ontologies for Cyber Security Analytics, TOCSA, is a project funded by mnemonic and the Research Council of Norway (NFR) and serving as a PhD project for PhD Candidate Siri Bromander who is on the NFR Industry PhD program. The University of Oslo supervises the PhD candidate and project in cooperation with mnemonic. The project aims to create ontologies in the domain of cyber security threats.

When security incidents occur there is typically limited understanding of who the threat actor is, why they attack or how they operate, which makes it difficult to make well informed decisions about countermeasures. Threat actors who are not identified and made responsible for their actions, will continue their criminal behavior. When we do not understand the attacker we can only see - if even that- the results of the attacker's actions. Improved cyber security requires digital threat intelligence - structured and partly automated analysis and sharing of information.

Threat intelligence is *evidence-based knowledge*, including context, mechanisms, indicators, implications and actionable advice, about an *existing or emerging menace or hazard* to assets that can be used to *inform decisions* regarding the subject's response to that menace or

hazard[1]. In the domain of cyber security, this task is characterized by large amounts of data from different sources and on different formats, which to a large extent is being used to do manual analysis. The type of data and information gathered is historically technical of nature, but emerging to include more non-technical aspects relevant to do technical operations.

Semantic technologies and ontologies are a relatively new logic-based landscape of technologies and tools aimed at giving better meaning to large and unstructured corpuses of data. Semantic technologies are applied in domains such as medicine, production, energy, oil and gas, and the Semantic Web.

Interesting research challenges are for example to investigate semantic representations of relevant concepts in the domain of cybersecurity big data, in order to facilitate advanced machine learning, search and discovery.

The potential benefit of this project is that the developed ontologies and related technologies will provide a flexible framework for representing and structuring the large variety of data with which security analysts are confronted. The framework can further be used for the implementation of cybersecurity analytics tools.

The objectives of this PhD project, as described in the project proposal, are:

1. Identify state-of-the-art in ontology development in the security area and how they are currently being applied to threat analysis and identification.
2. Extend and develop ontologies appropriate for automated threat analysis.
3. Use (maybe extend if needed) reasoner tools to do automatic and smart analysis of streams of online threat relevant data (e.g., network traffic).
4. Perform case studies to validate and test the developed method and tools on realistic data as provided by the industry part mnemonic AS.

The presentation given at Finse will present the TOCSA background and objectives. It will describe the current status of the TOCSA project, including the first publication made[2]. It will give a short overview of existing ontologies within the security domain and describe the next steps of our own ontology creation.

[1] https://www.gartner.com/doc/2487216/definition-threat-intelligence
[2] Bromander, Siri, Audun Jøsang, and Martin Eian. "Semantic Cyberthreat Modelling."