A Threat Operating Model (TOM) for Early Warning of Cybersecurity Threats

Motivation

Cyberspace and Cybersecurity

Increasing complexity of Cyberspace
- Increasing number of parties involved
- Loosely regulated infrastructure
- Non-IT human users deeply engaged

User/Event behavior driven approach
- A new dimension over system/data security
- Big data approach to Cybersecurity
- Holistic view on lifecycle of cyber attacks
- Patterns as well as correlations
- Prediction and early alerts/intervention of "Cyber Kill Chain"

Project Description

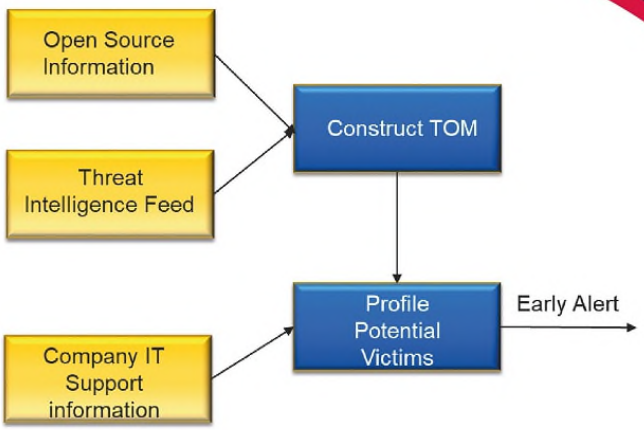
Automatic TOM Generation From Multiple Open Source Threat Intelligence Vendors

In this study, two types of cyber threat intelligence sources are used for illustrating the feasibility of automatically generating TOM:

(i) Type 1 source: automatic multi-scanning service providers e.g. **Threat Expert.**

(ii) Type 2 source: threat intelligence research sources, e.g. **Symantec.**

- Cluster threat intelligence reports according to the threat type.
- For each threat cluster, extract information from the Type 1 threat intelligence reports to identify the attributes and their values for the TOM model.
- Given each attribute, perform information extraction from Type 2 reports in the same cluster in order to enhance the TOM model details.
- The output TOM model may be used for interfacing with other SOC tools and risk analysis tools.



Key steps:

① Construct TOM based on open source information

② Establish the connection between behavior in the log file and potential threat via TOM

③ Similarity analysis between the user/system behavior profile and TOM constructed

Future Work

Structured Threat Information eXpression (STIX)
- a standardized XML programming language
- can convey data about cybersecurity threats in a common language
- can be easily understood by humans and security technologies.

In future work, we will enrich STIX representation by integrating TOM with it to enhance its expressive power.

Yang Wenzhuo, Srinivasu Bodapati and Lam Kwok Yan
School of Computer Science and Engineering, NTU
srini@ntu.edu.sg