Contribution ID: **243** Type: **Paper**

Visualization and Machine Learning for Interactive Cyber Threats Analysis in Critical Infrastructures

Critical infrastructure is now under constant threat from cyber adversaries searching to exploit vulnerable systems and networks in order to achieve their targets (denial of service, sabotage, financial loss ...). As illustrated in the IAEA Nuclear Security Series No. 17 (Computer Security at Nuclear Facilities, fig. 7), the sophistication of attacks against computer networks is continuously growing disproportionately compared to the growth of defence technologies. Implementing computer security partly relies on strict levels of logging and monitoring of each entity of the system. As recalled in the IAEA reference manual, human errors and previously unknown threats have to be accounted for, to help investigators and operators take appropriate actions to mitigate risks. Therefore the supervision of nuclear industrial processes and related information systems is a mandatory component for security of nuclear facilities. The resulting logs and activity monitoring signals are gathered in a Security Operations Center (SOC). The role of SOCs is to supplement security tools (IDS, Antivirus, $\cdots$) by using machine learning, rule-based or manual investigation approaches to detect suspicious behaviours that deviate from usual and specified activities (anomalies). These additional detections usually generate a large number of alerts, which must be processed automatically or by an operator who is in charge of investigating the severity of these alerts.

This work proposes a software tool, combining machine learning approaches and visualization, designed to provide alerts with adequate supplementary information. The rationale is that a majority of alerts are generated because of a lack of synthetic and comparative knowledge of the involved entities or the generated events. A prominent example is the detection of some SSH-based communication protocols generated between a computer from the monitored network and an external computer. While this activity can appear as suspicious for non-specialized users, the history of the user enables a disambiguation of this kind of alert. Therefore, machine-learning approaches have been developed to model and summarize behaviours and to detect similar behaviours (computer, group of computers, external requests$\cdots$). A key point of the tool is to offer investigators interactive 3D-based visualization, enabling simple and efficient data exploration with multi-level filtering and identification operations.

The visualization methodology relies on:

- Visualizing machine learning raw-data results: visualization helps security analysts to better understand what they are looking at and data-scientists what their machine learning algorithms do.
- Intuitive design for large-scale and heterogeneous data visualization.
- Efficient data exploration and multi-scaling alerts analysis.
- Adding interactive filtering and enabling graphical data selection.
- Interactive annotation and on-demand machine learning algorithms customization.
- Multi-view environment (from user-based activities to Domain-Name requests history summarization).

Various machine-learning algorithms are available in this tool, to enable efficient interactive exploration. Functionally, the goals of these algorithms are of three kinds:

1. **Behaviour modelling and summarization**: the aggregate history of a unique computer is usually difficult to interpret. Approaches have been developed to perform disaggregation of activities into various classes, depending on the necessary level of implication by a human (e.g. periodic log activities have to be separated from other ones). Using pre-processed activities resulting from the disaggregation, events are then modelled through graph-based approaches. Such graphs are designed to naturally represent successive events linked together. The tool then offers graph-based algorithms developed in this context to summarize and characterize behaviours, which are occurrences of random walks on events graphs.
2. **Dimensionality reduction**: the analysis of various activities generate high dimensional spaces. A prominent example is the analysis of domain name requests by computers of the internal network. On an open network, the number of unique requests (number of requests for a unique domain name) can be of the order of a few millions, when observed over a few weeks. It is thus often desirable to perform dimensionality reduction on such spaces, to allow for subsequent manipulations within relatively small durations.

3. **Similarity search, top-k requests and clustering**: once users and events have been correctly described and summarized, it is crucial to allow the operator to perform various comparison actions. It can be of interest to perform a similarity search, which consists in finding entities, successive events, or a group of computers similar to an object already identified. This can be of upmost importance when specific behaviour resulting from a targeted attack has been identified and the investigator wants to ensure that no computer has been also attacked or infected. Variants of such a scenario include situations when the investigator wants to identify the k-most similar users to an identified one, or when he requests users or events to be clustered in a given number of groups.

The methodology and the tools are currently in test in operational configurations. Preliminary results show that it enables an efficient decrease in false positive alerts and helps investigators to better explore complex data and better understand relationships between multi-scale events using a 3D-based interactive visualization.

State

France

Gender

Male

Primary authors: AZZABI, Radhouene; Mr GOUY-PAILLER, Cedric

Co-authors: Mr VALLEY, François; Mr DUBOIS, Hubert

Presenter: AZZABI, Radhouene

Track Classification: CC: Information and computer security considerations for nuclear security