Case Study

C7: The OPC-UA protocol

Description

Organizations can communicate and share digital content in real-time, using machines to machine (M2M) protocols. The unstoppable growth of data produced by all electronic devices (smartphones, personal computers, sensors, industrial machines, etc.) and related activities performed with them (web site navigation, social network interactions, online shopping, or financial activities), drive many researchers and companies to focus on managing and analyzing this data. Recent research on IT security conducted by Verizon [1], shows that also criminal organizations, driven by an economical goal, trying to catch this digital information for illegal purposes. Industrial Internet of Things (Industrial IoT) systems potentially constitute a considerable safety and security risk, especially if they are used in critical infrastructures as e.g. in the power industry [4]. OPC-UA is an open-source standard for machine-to-machine communication in the area of industrial automation that incorporates measurements for authentication and encryption as central countermeasures against cyber-attacks [3]. Today, the importance of being able to detect cyber-attacks and the attempts to tamper critical infrastructures, especially in the field of industrial IoT has become an essential element for our society.

A basic activity in IT cyber-attack detection is the reading of Log files that contains all events to recognize what happened. The sub-discipline in Data Science that encloses the study of the events and the processes derived from them is called Process Mining. Process Mining (PM) techniques can be applied to any context that requires a deep analysis of data and processes. With this internship project, we want to demonstrate that process mining can also contribute to the field of information security. We also notice that actually, there is a lack of research that describes solutions in this direction, and our initial results are promising.

The three types of attacks included in the dataset are Denial of Service (DoS), Impersonation, and Man in the middle (MiTM). After the dataset has been identified, we developed a methodology able to perform one or more experiments and analyze the final results. In the proposed methodology, we start analyzing the original dataset to understand what kind of data we have. In the second step, the metrics for techniques evaluation have been selected. Having performed the two initial steps, we can extend the original dataset (if necessary) and create an event log for our analysis. Typically, event log creation is influenced by which perspective we'd like to obtain and this may be performed several times during the proposed method. When the event log is ready, the process mining technique is executed to discover an attack. Next, the resulting models and metrics are analyzed.

Assignment

Use Process Mining techniques to discover the PP and identify possible improvements.

The following questions can guide the exercise:

- Study the event log and propose multiple approaches to identify the case_id of the exchanges to be analysed.
- Use PM process discovery techniques to create models that represent normal behavior and attack behavior.

- Use Conformance Checking techniques to detect the attacks and compute a set of quality metrics to validate the different tested techniques.

Dataset

The dataset contains network traffic with special attributes called multi_label for normal/attacks behavior identification. Each row in the dataset corresponds to an event that represents a bi-directional packet exchange (request and response). The author of the dataset has obtained the anomalies with special software that was able to simulate three types of attacks: DoS (Denial of Services), Eavesdropping or Man-in-the-middle (MiTM), Impersonation or Spoofing attacks.

The URL of the dataset is: https://ieee-dataport.org/open-access/m2m-using-opc-ua

Bibliography

[1] 2020 Data Breach Investigation Report - Verizon

[2] Process Mining Manifesto (IEEE Task Force on Process Mining)

[3] Charles Varlei Neu, Ina Schiering, and Avelino Zorzo. 2019. Simulating and Detecting Attacks of Untrusted Clients in OPC UA Networks. In Central European Cybersecurity Conference (CECC 2019), November 14–15, 2019, Munich, Germany. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3360664.3360675

[4] Maria B. Line, Ali Zand, Gianluca Stringhini, and Richard Kemmerer. 2014. Targeted Attacks Against Industrial Control Systems: Is the Power Industry Prepared? In Proceedings of the 2Nd Workshop on Smart Energy Grid Security (SEGS'14). ACM, New York, NY, USA, 13–22. https://doi.org/10.1145/2667190.2667192