Research Topic: From Alerts to Incidents in ICS/SCADA

Industrial control systems (ICS) monitor and control physical processes, often inside critical infrastructures like power plants and power grids, water, oil and gas distribution systems. In recent times, sophisticated attacks against owners and operators of industrial control systems across multiple critical infrastructure sectors have increased. Examples of such attacks include the so-called targeted-attacks (e.g. Stuxnet or Aurora) which specifically target the ICS with the aim of damaging it e.g. by tampering with a plant's physical process to drive it into an unsafe state. Since these attacks are built with knowledge of the targeted process, they are also referred to as semantic attacks.

Network-based Intrusion Detection System (NIDS) are widely deployed security tools used to detect cyberattacks by monitoring network traffic. Typically, NIDS generate alerts (a.k.a. security events) anytime a suspicious network activity is identified. Alerts can be of different types and they are composed of several details (e.g., the source and destination of the network activities and the reasons why it is considered dangerous). During an attack (a.k.a. incident), it is likely that a multitude of alerts is generated by the NIDS. Such alerts can be of different types and some of them might be false positives (especially in case of anomaly-based NIDS). In case of incidents, any of the existing NIDS limit their scope to generating alerts but leave the task of interpreting them to the end user. Unfortunately, this approach has several drawbacks: i) the task is expensive and error prone (the user might overlook some alerts) and ii) the user often lacks the knowledge necessary for the task.

Research Goals

The main goal of the project is to devise a solution for the aggregation and interpretation of alerts related to the same security incident. The solution might include the following steps:

- Analyse the alerts typically generated by a NIDS and create a taxonomy of events that fall in the same threat category. For instance, events such as *protocol scan* or *port scan* fall under the general category of *Scanning* threat.
- Build a model that can map security events and security categories to certain threat scenario (e.g., via attack trees) that represent the different phased of an attack. For instance, to infect a host an attacker could first execute a **Scan**, and then perform a vulnerability **Exploitation** and finally a malware **Injection**. These three steps can generate a multitude of events that, altogether, belong to the **Host Infection** scenario. The model can be build according to the cyber-kill-chain phases[1].

Student profile

The student should have basic understanding of networks and network security.

About SecurityMatters

SecurityMatters is a Dutch-based company with a young and international team. SecurityMatters develops cutting-edge network monitoring, intelligence and protection technology for ICS networks. The company has business in a number of control industries (oil & gas, power generation, energy distribution, etc.) worldwide. Its flagship product - SilentDefense - has been used in production since 2011. Most of the research activities will be executed in Eindhoven, under the supervision of Dr. Elisa Costante. The official language is English. For more information about SecurityMatters please visit our

[1] Hahn, Adam, et al. "A multi-layered and kill-chain based security analysis framework for cyber-physical systems." International Journal of Critical Infrastructure Protection 11 (2015): 39-50.

website at: www.secmatters.com. For more information about the research topic, please contact Dr. Elisa Costante (elisa.costante@secmatters.com).