MSc Thesis Research Topic: Semantic Alert Correlation 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. Unfortunately, existing intrusion detection systems cannot completely protect ICS networks from semantic attacks since they are unaware of the underlying ICS process' semantics. Addressing the problem of devising innovative solutions to add semantic attack detection capabilities to NIDS is a top-ranked research topic.

Background Information

Operators of critical infrastructure networks use a multitude of security tools such as NIDS, asset management and flow analysis tools to monitor and protect their assets from cyber-attacks. These security tools typically consist of sensors probes that collect an increasing amount of data and produce a high volume of security events (or alerts). It is increasingly challenging, for security analysts, to monitor the ever-growing amount of events generated by such tools[1]. A way to reduce the effort required to analyse a multitude of events is to use techniques for alert correlation. Alert correlation aims at reducing the number of events, at conceptually grouping related events and at assigning a semantics to them[2]. Existing techniques for alert correlation include:

- Rule based systems, which use predefined correlation, rules to identify known threats and attacks.
- Data mining, which leverages machine learning and mining techniques to extract implicit and unknown information from very large volume of data.
- Text mining, which automatically maps security events to Common Attack Pattern Enumeration and Classification (CAPEC)[3]. CAPEC is a publicly available comprehensive dictionary and taxonomy of known attack patterns that can be used by analysts, developers, testers, and educators to increase the knowledge of threats and enhance defences.
- Logic based systems[4], which model the ICS world by using first order logic to enable querying and asserting information about network events.

Research Goals

The goals of this MSc thesis project are:

1. **Knowledge representation**: devise a solution for modelling (and reasoning about) raw data and security events collected by NIDS in ICS environments. The model should represent the basic

[1] Scarabeo et al. (2015), Mining known attack patterns from security-related events. PeerJ Comput. Sci. 1:e25; DOI 10.7717/peerj-cs.25

[2] G. Jakobson and M. D. Weissman. Alarm correlation. IEEE Network Magazine, pages 52–60, 1993.

[3] The MITRE Corporation. 2015. Comment attack pattern enumeration and classification. Available at https://capec.mitre.org/.

[4] Morin, Benjamin, et al. "M2D2: A formal data model for IDS alert correlation."*International Workshop on Recent Advances in Intrusion Detection*. Springer Berlin Heidelberg, 2002.

concepts of the ICS world (e.g. field devices, control server, network components) together with the concepts of ICS security (e.g. vulnerabilities, attacks, generic threats to the process). This model should be used as basis for reasoning and inferring additional information about network activities as explained in the following point.

2. **ICS Attacks and vulnerabilities modelling**: based on the model built in the previous step, device a solution able to model (and reasoning about) attacks and vulnerability specific to ICS systems and to network security events. Despite many attempts, there is currently no agreement between ICS security actors on how to describe the characteristics of attacks. Therefore, we need a way to classify and model attacks in order to reason about them and connect security events to certain attacks. This solution should help to (in)validate (a set of) alerts raised by intrusion detection systems (e.g. to confirm or deny the presence of an attack).

Example

Let assume that, as results of the first research goal, we have derived the following model represented as first logic order:

- *host (x) ← workstation(x)*
- *host (x) ← field_device(x)*
- *workstation(H); -- H is a workstation*
- *isInNetwork(H,enterprise); - H is in an enterprise network;*
- *field_device(F); -- F is a filed device*
- *isInNetwork (F,control); -- F is in a field network*
- *isCommunicating (H,F)*; --H is *communicating with F*

Then, as a result of the second research goal, we could have the following information:

- *undesired_flow(x,y) ← host (x) && host (y) && ((isInNetwork(x,enterprise) && isInNetwork (y,control)) || (isInNetwork(y,enterprise) && isInNetwork (x,control)))*

In the example, we can use our models to infer undesired between control networks while and enterprise networks.

Student profile

The student should have basic understanding of networks and network security together with knowledge in the field of formal methods and knowledge representation.

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 website at: www.secmatters.com.

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