SECURITY MATTERS

Research Topic: Protecting ICS Networks from Attacks

Problem definition

Industrial Control Systems (ICS) lie at the bottom of every industrial process – from power generation to water treatment and manufacturing. The term ICS refers to the set of devices that govern the process to guarantee its safe and successful execution, and include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control systems such as Remote Terminal Units (RTU) and Programmable Logic Controllers (PLC). A malfunction in any of these systems might cause the entire industrial process to fail, with serious consequences in terms of economic loss and public safety. For instance, think of the disruption of an electricity transmission network; an incorrect distribution of electricity might affect the availability of electric power to households, offices, hospitals, etc.

ICS components (SCADA servers, RTU, PLC, workstation, etc.) are connected to form a network and communicate via specific industrial protocols (e.g. Modbus, DNP3, IEC-104). ICS components, as well as industrial protocols, might suffer from vulnerabilities that an attacker can exploit to damage the ICS environment and cause disruptions. Typically, vendors and security organization (e.g. CERTs) publish bulletins when a new vulnerability (of protocols or products) is discovered. It is important that security monitor and intrusion detection systems (IDS) embed this information in their knowledge base as soon as it is available.

Project description

The main goal of this project is the analysis, design and prototype development of a software that:

(a) Extracts information from security bulletins (e.g. CVE published by CERT) and represents them in a format that can be ingested by SecurityMatters' network monitoring system in an as-automated-as-possible way; and

(b) Research and define a list of possible indicators of compromise, and specify ways to detect them automatically.

In particular, the student is expected to execute the following steps and to address the following challenges:

1. Acquire the necessary knowledge about existing ICS protocols and components, together with their well-known vulnerabilities;
2. Analyse the way security bulletins are typically published, and define a way to interpret them and to represent them in a standard format, for easy ingestion into SilentDefense, our flagship product.
3. Define indicators of compromise (IOCs), namely specific conditions that indicate that a network is vulnerable to certain attacks, and write scripts that detect the presence of such IOCs within a network;
4. Test, document and deliver the software produced.

The project will take place in Eindhoven under the supervision of Dr. Elisa Costante (elisa.costante@secmatters.com). The student will make use of appropriate office spaces allocated for the execution of the project activities. The official language is English.

Student profile

It is preferable if the intern has familiarity with network protocols and scripting languages.

SECURITY MATTERS

About SecurityMatters

SecurityMatters is a Dutch-based company with a young and international environment. SecurityMatters develops cutting-edge network monitoring, intelligence and protection technology for ICS networks where it is sector leader. SecurityMatters has developed a completely new approach to secure ICS networks, called self-configuring deep protocol network whitelisting, which is the result of more than 20 years of research and experience in the field of network intrusion detection. SecurityMatters has business in a number of control industries (oil & gas, power generation, energy distribution, etc.) and financial institutions. Its flagship product - SilentDefense - has been used in production since 2011. 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).