Chapter 6

LIGHTWEIGHT JOURNALING FOR SCADA SYSTEMS VIA EVENT CORRELATION

Antoine Lemay, Alireza Sadighian and Jose Fernandez

Abstract Industrial control systems are not immune to cyber incidents. However, the support for incident responders and forensic investigators is low. In particular, there are limited journaling capabilities for operator actions. Barring the preservation of full packet captures and operator workstation security logs, which can generate unmanageable amounts of data on production networks, it is generally not possible to attribute control events (e.g., opening a valve or operating a breaker) to individual operators. This information can be necessary to perform security investigations, especially in cases involving malicious insider activities. This chapter presents a lightweight journaling system for SCADA networks based on event correlation. By correlating network events and operating system logs, a journal is generated of all Modbus protocol write events along with the usernames of the operators who performed the actions. The journal is much more compact than a full packet capture, achieving compression ratios of around 570 to 1 in conservative conditions and more than 2,000 to 1 in typical operating conditions, allowing for the preservation of valuable information for security investigations.

Keywords: SCADA networks, network forensics, journaling, event correlation

1. Introduction

The number of cyber incidents has been rising in recent years. Industrial control networks (also referred to as supervisory control and data acquisition (SCADA) networks) are not immune to cyber threats; examples are the Havex malware [10] and a serious incident at a German steel mill [1]. This trend underscores the need for better incident response capabilities in industrial control or SCADA networks.
One of the first instincts of an incident responder is to review logs to find clues about the incident. However, this is usually not possible in SCADA networks. In the vast majority of these networks, the control systems do not support the journaling of relevant security information. This lack of journaling is critical from a security perspective. In a SCADA system, the controllers perform all the interactions with the physical network. An attacker who wishes to create a physical impact must interact with the controllers. Yet, there is no convenient way to track these attacker interactions.

Full packet captures can be used to track most interactions with controllers. Typical controllers do not possess any keyboards or user displays and, unless an individual is performing maintenance using physical access, the controllers are usually only accessed remotely via the control network. In this sense, full packet captures record the interactions with the controllers. However, they also contain large volumes of irrelevant network activity, preventing their storage for extended periods of time.

As an example, the limited test network used in this research generates traffic in the order of gigabytes per month. In a production network, with many more controllers and field devices, the network traffic would be orders of magnitude higher. As such, there is a need to preserve summary information that would enable incident responders to gather key information about the interactions with controllers. This chapter describes an event correlation approach that creates a log of interactions between operators and controllers by combining data from network sensors and data from security logs in operator workstations.

2. Background

This section presents background information about SCADA systems. In particular, it describes the architecture and operation of SCADA networks that use the popular Modbus protocol.

Many SCADA networks are organized around the Purdue Enterprise Reference Architecture [15]. In this architecture, Level 0 is the physical process. Intelligent field devices, namely, sensors, actuators and their controllers, are located in Level 1. Higher level controls, such as SCADA systems, are in Level 2. All Level 1 equipment is grouped together on the same local-area network (plant local-area network). Similarly, all Level 2 equipment is grouped in the control center local-area network.

Figure 1 presents the architecture of a Modbus system. In the architecture, each operator workstation hosts a SCADA program. The SCADA program comprises two main components. The first component is the master terminal unit (MTU), which is responsible for maintaining information about the state of the physical process in the operator workstation. In Modbus, this is accomplished by continually polling each controller to request updates on the states of all the field devices attached to the controller. Every few seconds, the exact time being defined by the polling interval configuration option, the master terminal unit sends a Modbus read packet to each controller. The controller