C26 Supervisory Control and Data Acquisition (SCADA) Forensics: Network Traffic Analysis for Extracting a Programmable Logic Controller (PLC) System and Programming Logic Files

Irfan Ahmed, PhD, University of New Orleans, 2000 Lakeshore Drive, New Orleans, LA 70122*

After attending this presentation, attendees will understand the message format of the Allen-Bradley Programmable Controller Communication Commands (PCCC) protocol and how the network traffic of the protocol can be analyzed for extracting ladder logic program and system files. Ladder logic is a popular programming language for a PLC that is an essential and critical component for the automation of industrial processes such as gas pipelines, chemical and nuclear plants, and power generation and distribution.

This presentation will impact the forensic science community by providing an overview of a parsing and recovery technique for a ladder logic program and system files from the network traffic of the Allen-Bradley PCCC protocol. The protocol is supported and widely used by the PLCs of the vendor, Allen-Bradley, for transferring configurations and programming logic and control data (such as sensor readings, current state of actuators, counters, and timers). When the programming software, such as Studio 5000® and RSLogix 500™, transfers a ladder logic program from an engineering workstation to a PLC, it transfers system files along with the program.

In order to extract these files, the technique takes into account the PCCC message format allowing the identification and filtering of packets based on the protocol header fields. The fields include byte-count, file-number, file-type, element-number, and sub element number. In particular, the file-type field is used to identify the type of data in a packet. For instance, "O" represents output file data. Each packet contains headers of three industrial protocols in the following sequence: Ethernet/IP, Common Industrial Protocol (CIP), and PCCC. The technique for recovering the files involves parsing the PCCC header, then further filtering out the packets containing the chunks of system and program logic files, which are then combined in a logical sequence to reproduce the files being transferred through the network.

A prototype implementation (tool) of the technique will also be provided in the presentation. The tool can play an important role in the forensic investigation of a SCADA system. For instance, a forensic investigator can determine the presence of any ladder logic code and system files in a network packet capture and further obtain the whole code from the capture in a file for further analysis. The investigator can compare the hash values of the code extracted from the network trace to the original code of the PLC created and downloaded from PLC programming software.

Ladder Logic, SCADA Forensics, Network File Carving