Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE

GEORGE MASON UNIVERSITY

VCU

PLC Forensic Toolset for Industrial Control Systems

LEAD PI: IRFAN AHMED

Forensics

SUMMARY

In industrial control systems (ICS), programmable logic controllers (PLCs) directly control and monitor physical processes such as power grid stations. When attackers (e.g., Stuxnet) target ICS environments, they typically aim to compromise PLCs to sabotage physical processes. In case of a cyberattack on an ICS facility, memory forensic analysis of suspicious PLCs can answer many questions about the attack, such as what PLCs were affected, how the control logic and firmware were maliciously modified, and whether the attack still is active, and can be repeated. This project will enable memory forensics for PLCs including device memory acquisition and analysis.

PROBLEM STATEMENT

In a recent ransomware attack on the Colonial pipeline, the attackers infiltrated the company's computer servers but did not target the pipeline. Unfortunately, the company could not tell with certainty whether their physical infrastructure (i.e., pipeline) was also under attack, resulting in a shutdown of the entire infrastructure to eliminate the risk of physical process damage. PLCs also pose several challenges to forensic capabilities, including heterogeneous hardware and proprietary protocols. The memory forensic capabilities developed in this project will address these challenges and enable these asset owners/operators to investigate a potential compromise of PLCs at field sites to make an informed decision.

APPROACH

This project has two research thrusts: 1) Develop a reliable PLC memory acquisition framework, including automated ICS protocol reverse engineering and, 2) develop a set of device memory profiles of several PLCs of popular vendors for memory forensic analysis. The research builds upon and goes beyond prior work to systematically improve the state-of-art in ICS forensics.

ANTICIPATED IMPACT FOR DHS

The tools and techniques developed in this project will enable DHS and ICS incident response teams to more effectively, efficiently, and completely investigate field devices in industrial control systems.