Digital Forensic Tools and Techniques for Investigating Control Logic Attacks in Industrial Control Systems

Summary
While digital forensic capabilities continue to advance, industrial control systems (ICS) environments are notoriously heterogenous and proprietary and techniques for investigating them remain underdeveloped. Tool and knowledge gaps exist regarding how anti-forensic attacks can be realized on ICS devices, which limits forensic analysis. Analysts require tools and techniques to investigate cyber-attacks on industrial control systems in their mission to protect critical infrastructure. This project will enhance the capabilities of ICS owners and operators by providing better understanding of anti-forensic aided control logic modification attacks and equipping them to investigate control logic attacks.

Problem addressed

Control logic attacks on programmable logic controllers (PLCs) are common in industrial control systems (ICS) environments. Acquiring and analyzing control logic from a PLC are necessary steps to investigate an ICS security incident effectively. Developing capabilities to execute these steps will help understand attackers' objectives and how the attack targets the physical processes in critical infrastructure.

Approach

This project has two research thrusts: 1) investigate anti-forensic aided control logic modification attacks, and 2) develop control-logic forensic capabilities. The first thrust explores code-reuse and return-oriented programming attacks on PLCs, and also studies the anti-forensic attacks that incapacitate engineering software's ability to acquire and analyze control logic programs from PLCs. The second thrust develops a novel PLC memory acquisition technique over the network that works by injecting non-malicious memory-extractor code into a target PLC.

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 control logic system attacks.

Research Products:

Publications:

Control Logic Obfuscation Attack in Industrial Control Systems

Gadgets of Gadgets in Industrial Control Systems: Return Oriented Programming Attacks on PLCs