Cyber Forensic Tool Kit for Machinery Control

Project Summary

OBJECTIVE: Develop live digital forensics that, at run time, provide a cyber-protection strategy and aid in identification of malfunctions due to malicious and non-malicious events, while ensuring minimal impact on overall system performance.

DESCRIPTION: Shipboard machinery control systems utilize SCADA to monitor and control these systems. Common components of the SCADA systems include human-machine interfaces (HMI), remote terminal units (RTU), input/output devices (I/O), programmable logic controllers (PLC), and communication networks. Digital forensics, consisting of activities associated with the collection and analysis of digital data from various sources, is an essential part of an overall cyber defense strategy both prior to and after a breach of security. For SCADA systems, forensics is not only a vital part of the protection strategy but also can aid in the troubleshooting and identification of non-malicious events that cause the system to malfunction.

A number of unique challenges exist for the forensic analysis of SCADA based systems. Components of a SCADA system are often resource constrained. The opportunity to run forensic resources on devices in the SCADA system depends on the availability of processor, memory, I/O, and other system resources. Many systems running in the field have legacy hardware and lack the computing capabilities of modern hardware systems. The collection of log data in SCADA systems is often inadequate. In particular, immediately following an incident, the collection of log data is critical to being able to re-create the sequence of events leading up to the incident. There are currently no effective methods for capturing the volatile data that exists in the control system registers, cache, memory, routing tables, and temporary file systems. Much of the data that exists in SCADA systems is at the lower layers of the architecture making it more difficult to access. At those layers, sometimes there is such a large amount of data that analysis becomes challenging due to scale and dimensionality.

The solution sought should incorporate data acquisition tools used to support forensics analysis that has minimal impact on the overall operation of the control system. The application must be able to operate as a plug in to an open source forensic tool kit such as Autopsy and have an open system architecture. The application should enable reconstruction and replay of the state of the SCADA system to support incident response. The government will be responsible for scheduling testing and certification of the application in a land based SCADA test facility prior to transition. It is essential that the proposed solution performs live forensics at run time with minimal impact on overall system performance.

PHASE I: The company will investigate and develop an architectural design of a forensic tool set for SCADA including identification of an Application Program Interface (API), for the plug in interface, and functional requirements. The company will define and develop a concept for forensic tools for SCADA that can meet the performance constraints listed in the description. They will perform modeling and simulation to provide initial assessment of concept performance and feasibility. Phase I Option, if awarded, would include the initial layout and capabilities description to build the system in Phase II.

PHASE II: Based on the results of Phase I and the Phase II Statement of Work (SOW), the company will develop and demonstrate a prototype forensic tool kit for SCADA based on the interface and functional requirements developed in Phase I. Testing will be conducted in a land based SCADA test facility. The prototype should be delivered at the end of Phase II, ready to be integrated by the government. The Phase II effort will likely require secure access.

PHASE III DUAL USE APPLICATIONS: The company will assist the Navy in transitioning the forensic tool set for SCADA specified in Phase I and prototyped in Phase II to a Navy lab for operational analysis. After Navy laboratory assessment, the company will assist with the integration of the forensic tool kit and demonstrate the complete system shipboard. The company will transition the technology to SCADA. The Cyber forensic tool kit will be applicable to control systems cyber analysis across the government. The cybersecurity tool will also be applicable to all manufacturing, energy production, and oil and mineral processing facility machinery and engine control systems.