2016

Cybersecurity Framework for Ship Industrial Control System

Maule, R. William; Hake, Joseph

Monterey, California. Naval Postgraduate School

MONTEREY, CALIFORNIA

Cybersecurity Framework for Ship Industrial Control Systems

Report Type: Final Report
Period of Performance: 10/01/2015-01/30/2017

Project PI: Dr. R. William Maule, Research Associate Professor, Graduate School of Operational and Information Sciences, Naval Postgraduate School
Student Participation: Joseph Hake, Lieutenant Commander, U.S. Navy, Cyber Systems & Operations

Prepared for:
Topic Sponsor: SPAWAR 58000
Research POC Name: CAPT Brian Erickson
Research POC Contact Information: brian.g.erickson@navy.mil, 619-524-3271

Title: Cybersecurity Framework for Ship Industrial Control Systems (ICS)
Report Date: 30/01/2017 Project Number (IREF ID): NPS-N16-N282-B
Naval Postgraduate School / GSOIS / Information Sciences

EXECUTIVE SUMMARY

Project Summary
Ship mechanical and electrical control systems, and the communications grid through which these devices operate, are a high priority concern for Navy leadership. Ship systems use microprocessor-based controls to interface with physical objects, and Programmable Logic Controllers (PLCs) to automate ship electromechanical processes. Ship operations are completely dependent on these devices. The commercial security products upon which ships depend do not work on ICS, leaving ships vulnerable.

The ICS research framework advanced in this project provide metrics for ship ICS cyber-physical infrastructure evaluation, and analytic techniques based on industry best practices. Component test and measurement workflows were developed to apply test procedures and metrics to ship industrial controls. Ship ICS audit processes and decision support workflows will help watchstanders address and counter cyber-physical infrastructure vulnerabilities.

Keywords: Cybersecurity, cyber-physical infrastructure, industrial control systems, supervisory control and data acquisition, programmable logic controllers

Background
Modern warship designs have evolved toward distributed, network-enabled automation architecture to improve operational awareness for Hull, Mechanical and Electrical (HM&E) systems. Automation enhances battlespace awareness and mission-readiness, and supports systems designed for reliability under random failure (e.g., link outages) or correlated failure under duress (e.g., fire, physical damage). HM&E and Machinery Control Systems (MCS) engineering has not prioritized cybersecurity, leaving ships in a vulnerable cyber posture.

Some work has been devoted to clean-slate design approaches for control systems (Velagapalli, 2011; Hieb, 2009; Chavez, 2009) but to date these and similar efforts have not been implemented in a manner sufficient to address Navy security needs. Nor does this approach address the large installed base of legacy control systems (Lindqvist, 1998; Federal Times, 2014) which may be subject to compromise during original equipment

manufacturing, systems integration, daily operations or maintenance (Collado, 2016; DuHarte, 2016).

There are over 250 industrial control technologies, with most using protocols not detected by legacy ship cybersecurity. These devices and their controls are the target of cyberattacks since security is minimal and they provide access to infrastructure (Sands, 2016). These devices control ship mechanical, electrical and power systems—which are additionally subject to component-specific attacks against embedded devices, such as electrical relays or gates (Bruggermann, 2016). Vulnerabilities exist in end-point devices such as sensor interfaces, analog to digital conversion gates, and motor controls and actuators (Grow, 2008).

Programmable Logic Controllers (PLCs) are embedded within MCS to automate processes. Supervisory Control and Data Acquisition (SCADA) controls supervise the PLCs. Both can be exploited by adversaries seeking to disrupt electrical or mechanical operations, or control cyber-physical infrastructure (Koscher, 2015). Fault handlers neither protect systems whose control logic has been compromised, nor protect against attacks where damage is caused in aggregate—not detected from the perspective of any single system. Ship Electric Management Systems (EMS), Distribution Control Systems (DCS), and Process Control Systems (PCS) are impacted (Duggan, 2005). Cyber intrusion of mission critical controls may impact command decisions (Maule, 2015).

Findings and Conclusions

This report developed research frameworks, metrics and workflows for the analysis of ship ICS infrastructure to help assess the degree to which ship cyber-physical systems can be protected from cyberattacks and external control. This included a discussion of methods through which adversaries can enter cyber-physical infrastructure through conventional cyberattacks, and conversely compromise ship systems and networks through ICS devices and controls.

Discussion of ICS cyberattack methods that may impact ship cyber-physical infrastructure were integrated with analysis metrics, supporting audit processes and decision workflows. Research frameworks to assess ICS infrastructure included a discussion of ICS devices, their protocols and metrics, and interfaces to legacy IT/network security systems.

In addition to traditional IT and network cybersecurity, successful ICS defense requires familiarity with the specialized equipment that will be attacked, and with the cybersecurity tooling required to assess that equipment. This includes proprietary integrated circuits and firmware. The auditor needs to be versed in traditional IT/network cybersecurity and tooling, and in the engineering specializations required for assessment of the specialized ICS components. The learning curve and tooling requirements are significant.

Recommendations for Further Research

Future research may apply the ICS research frameworks, audit processes and decision workflows for ship ICS cyber assessment and defense. ICS cybersecurity audits require up-to-date reference databases to adequately protect ICS infrastructure. Future research may develop databases which contain component specifications, ship architecture models, control and device measurement results, and vulnerability maps for ship ICS configurations.

In a prolonged cyber conflict ship watchstanders may be overwhelmed with ICS problems, and in A2AD and D-DIL conditions without reach-back for technical support. Future research may develop architecture for ICS cybersecurity automation to help protect ship cyber-physical infrastructure. New advances in artificial intelligence, cognitive computing, and machine learning provide viable options for ship ICS cybersecurity automation.

References

Bruggermann, M., Schwartke, H., and Spenneberg, R. (2016). PLC-Blaster: A Worm Living in your PLC," *BlackHat USA 2016*, Las Vegas, NV: Blackhat.

Chavez, A. (2009). Protecting Process Control Systems Against Lifecycle Attacks Using Trust Anchors. *DHS Workshop on Future Directions in Cyber-Physical Systems Security,* Washington, DC: Department of Homeland Security.

Collado, E. (2016). Reversing and Exploiting Embedded Devices. *DEFCON 24.* Las Vegas, NV: DEFCON.

Duggan, D. (2005). *Penetration Testing of Industrial Control Systems.* Albuquerque, NM: Sandia National Laboratories.

DuHarte, M. (2016). Basic Firmware Extraction. *DEFCON 24.* Las Vegas, NV: DEFCON.

Federal Times. (2014, January 29). How COTS Endangers National Security. *Federal Times*.

Grow, B., Tschang, C., Edwards, C., and Burnsed, B. (2008, October 1). Dangerous Fakes: How Counterfeit, Defective Computer Components from China are getting into U.S. Warplanes and Ships. *Business Week*.

Hieb, J., and Graham, J. (2009). Designing Security-Hardened Microkernels for Field Devices. *Critical Infrastructure Protection II* (pp. 129–140). NY: Springer.

Koscher, K. (2015). Sniffing SCADA. *DEFCON 23.* Las Vegas, NV: DEFCON.

Lindqvist, U., and Jonsson, E. (1998). A Map of Security Risk Associated with Using COTS. *IEEE Computer, Vol. 31, No. 6*, 60-66.

Maule, R., Goldberg, J., Baker, B., McElvain, L., and Sinopoli, J. (2015). Integrated Air and Missile Defense (IAMD) Multi-Tactical Data Link (M-TDL) Network (MTN). *Valiant Shield 2014 Analysis Report*, Norfolk, VA: Navy Warfare Development Command.

Sands, F., and Gorenc, B. (2016). Hacker-Machine Interface. *DEFCON 24.* Las Vegas, NV: DEFCON.

Velagapalli, A., and Ramkumar, M. (2011). Minimizing the TCB for Securing SCADA Systems. *Seventh Annual Workshop on Cyber Security and Information Intelligence Research.* Oakridge, TN: Oakridge National Laboratory.