Contract No:

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-08SR22470 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

Disclaimer:

Embedded Hardware Solution for Cybersecurity in Industrial Control Systems

Industrial Control Systems are the backbone of manufacturing, power, and critical infrastructure. These systems are made up of electronic and mechanical devices that operate on complex feedback systems that allow the production of consumer products, electricity, clean water, and nuclear industries. This broad reach of cybersecurity has earned it a place in the strategic roadmaps for many government agencies, including the Department of Energy. Their efforts stem from two general initiatives which are to improve cybersecurity in the energy sector and to strengthen effectiveness of Department of Energy incident management capabilities. Particular emphasis is in improving learning and preservations of knowledge at the labs, and to encourage collaboration between the labs.

This project aims to develop Savannah River National Laboratory's knowledge of industrial control systems cybersecurity by providing our engineers the opportunity to learn and execute advanced concepts in cybersecurity to real problems in industrial control systems. Successful execution of this project will enhance Savannah River National Laboratory's knowledge and capability in the realm of Industrial Control System and Operational Technology cybersecurity as well as advance understanding of defensive needs in these environments. This will directly impact Savannah River National Laboratory's capability to contribute and collaborate with Department of Energy, other Labs, and commercial partners in meeting Department of Energy national industrial control systems/Operations Technology cybersecurity goals.

Awards and Recognition

N/A

Intellectual Property Review

N/A

SRNL Legal Signature

Signature **Date**

Embedded Hardware Solution for Cybersecurity in Industrial Control Systems

Project Team: Robert Blair Barnett, Richard Poland, Ryan Cruz (Intern)

Subcontractor:

Thrust Area: Secure Energy Manufacturing

Project Start Date: October 1, 2017
Project End Date: September 30, 2018

Manufacturing and Utility companies utilize industrial controls systems (ICS) to automate their plants as a means of increasing efficiency and productivity. These environments consist of older ICS devices that have been networked, although they were never intended to have this functionality. To identify appropriate defensive characteristics needed to contribute to defense-in-depth of cyber-physical systems, we performed a survey of ICS environments and devices. A unique level of concern for ICS are levels one and zero (L1/L0). Devices at these levels are conducting physical activities (and thus considered cyber-physical systems). Our focus are gateway controllers which exist as the interface for L1/L0 devices to higher network controllers. Our strategy is to develop an authentication method using TLS without encryption enabled thus providing an authenticated channel of communication to a gateway device.

FY 2018 Objectives

- Categorize Vulnerability Concerns in ICS
  - Review ICS Architectures, Common Devices, and Protocols
  - Identify general or common weaknesses and vulnerabilities
- Stand Up ICS Testbed
  - Design a robust and flexible testing environment for ICS
- Develop Concept for mitigation of vulnerability at L1/L0
  - Leverage lessons learned from task 1 to devise a strategy for mitigating vulnerability that can be developed into a prototype for testing within the testbed environment

Introduction

Manufacturing and Utility companies utilize industrial controls systems (ICS) to automate their plants as a means of increasing efficiency and productivity. These environments consist of older ICS devices that have been networked, although they were never intended to have this functionality. More modern Industrial Internet of Things (IIOT) devices, that are rapidly developed with full suites of communication and intelligence features but not security, are also being deployed in these environments. This new interconnectedness on the production floor is being used to connect facilities across the internet to command and control centers. This state of highly interconnected computing capability leaves these systems vulnerable where once a true air-gap existed. In an unfortunate inability to learn from the general history of the internet the networking technologies for these environments are largely being developed on a model of trust. While this attitude is changing, improving ICS security it is a very slow process. The lifecycle for ICS devices can be 10-20 years in time making ICS enticing targets for adversaries looking to impact critical infrastructure [1].

A common topology of ICS networks is generalized by breaking the network into five standard levels. It starts with a Business/Enterprise center at the top (level 5) and ends with sensor or actuator devices at the bottom (level 0). Supervisory Control and Data Acquisition systems (SCADA) show up typically at level 3 in the model. It is this point in the model that communication technology transitions from Information Technology (IT) to Operations Technology (OT). With the shift in technology type comes changes in hardware and communication protocol usage. This shift in technology means there must also be changes in how security is conducted for OT systems as compared to standard IT security that accounts for the different nature of the OT environments and devices [2].

A unique level of concern for ICS are levels one and zero (L1/L0). Devices at these levels are conducting physical activities (and thus considered cyber-physical systems). These two levels are also the most different from IT in terms of behavior and considerations and suffer the most in terms of security. In order to raise the bar for security of these end devices, we have reviewed network architectures and device types, and engaged with industry to identify weaknesses and vulnerabilities which would benefit from tailored security for L1/L0 cyber-physical systems. Using this information, we have developed a plan for an ICS testbed, and the outline of a prototype device which will be developed in the second year to test security concepts for cyber-physical systems.

Approach

To identify appropriate defensive characteristics needed to contribute to defense-in-depth of cyber-physical systems, it was necessary to begin with a survey of ICS environments and devices. Engagement with the ICS community via conferences and workshops, as well as utilization of white papers provided by SANS and E-ISACs, and conversations with Fort Gordon cyber protection team personnel were used to discover contemporary issues with control systems. The results of this discovery phase were used to develop a plan for the development of an ICS-specific cybersecurity testbed, as well as development of specifications for a device that would allow implementation of security features at this low level.

Protocol usage for L1/L0 devices can vary greatly and any added security to existing systems must avoid interfering with this communication. Deep packet inspection is one established layer of security at this low level and anything added to defense-in-depth must compliment this technique. One initial constraint in our approach is to not use encryption as a means of security as to not interrupt this capability. To achieve this, novel forms of authentication were explored as a way of validating the communications without obscuring the traffic between points. The full development of this method is left for 2019.

Results/Discussion

We had three main objectives for this year: identify vulnerabilities in the ICS environment, develop a testbed that will allow us to conduct cybersecurity research on a range of ICS environments, and develop specifications for a prototype to address one of the identified vulnerabilities. We determined that a very common vulnerability in ICS systems is a lack of authentication. This exists at many levels, but our focus will be at the gateway controller level. This narrowed our focus to developing an authentication method using TLS without encryption enabled thus providing an authenticated channel of communication to a gateway device. For the end of the first-year goals, we thus began developing a lab environment and a

prototype device that would allow us to test this method of defense. The continuation of this will be discussed in the Future Directions section.

Initially we intended to produce a report classifying the vulnerabilities in ICS but the sheer volume proved overwhelming and ultimately distracting from the scope of this project ([3] as an example of the depth of this rabbit hole). The most discussed problem in person and at conferences was around gateway controllers and their lack of authentication [4] [5] [6]. More specifically, the conversation is about their inadequate authentication. Many of the devices that were explored by others contained some form of authentication – but with such poor implementation or easily accessed backdoors they were near useless. Many responses from vendors to this problem was to suggest disabling the security altogether. These devices typically control communication between L1/L0 devices and HMIs or RTUs at a higher level. This placed them at the level of interest, but also as a critical component to the security at the level of interest for us which made them prime candidates to be addressed by this project.

FY2018 Accomplishments

- Identified a critical problem affecting a class of devices – gateway controllers - at the low level on ICS networks in general
- Developed criteria to establish a working environment for ICS that will be used for this project but can be leveraged towards others and external customers
- Devised design specifications for a hardware device that can implement a security solution for the gateway controllers identified as suffering from critical security concerns.
- Established relationships with Fort Gordon and Florida International University
    - This project utilized a Cybersecurity graduate student from Florida International University via the DOE-Fellowship program

Future Directions

- Design and Develop Embedded Hardware
    - Apply specifications from FY18 to develop prototype hardware
    - Develop and Test an authentication method for the security hardware
- Test and Validate Authentication Method on ICS Testbed
    - Finish leftover tasks for completing the testbed construction
    - Deploy mock ICS network with security solution authenticating at the gateway controller
    - Verify the hardware provides tangible security benefit on the system

FY 2017 Publications/Presentations

N/A

References

[1] L. Obregon, "Secure Architecture for Industrial Control Systems," 23 September 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327. [Accessed 2018].

[2] G. Aydell, "The Perfect ICS Storm," 15 May 2015. [Online]. Available: https://www.giac.org/paper/gcia/10551/perfect-ics-storm/141222. [Accessed 2018].

[3] J. Z. Andrei Costin, "IoT Malware: Comprehensive Survey, Analysis Framerwork and Case Studies," 2018. [Online]. Available: http://i.blackhat.com/us-18/Thu-August-9/us-18-Costin-Zaddach-IoT-Malware-Comprehensive-Survey-Analysis-Framework-and-Case-Studies-wp.pdf. [Accessed 2018].

[4] T. Roth, "Breaking the IIOT: Hacking Industrial Control Gateways," in *Blackhat USA 2018*, Las Vegas, 2018.

[5] J. Shattuck, "Snooping on Cellular Gateways and Their Critical Role in ICS," in *BlackHat USA 2018*, Las Vegas, 2018.

[6] M. P. J. S. Daniel Crowley, "Outsmarting the Smart City," August 2018. [Online]. Available: http://i.blackhat.com/us-18/Thu-August-9/us-18-Crowley-Outsmarting-The-Smart-City-wp.pdf. [Accessed 2018].

Acronyms

- HMI – Human Machine Interface
- ICS – Industrial Control System
- IIOT – Industrial Internet of Things, category of industrial devices designed to allow control over either local or internet network connections
- IT – Information Technology
- L1/L0 – Level 1 and Level 0 of the Purdue ICS network model, lowest level where computer devices are performing physical activities.
- OT – Operations Technology
- RTU – Remote Terminal Unit
- SCADA – Supervisory Control and Data Acquisition

Intellectual Property

N/A

Total Number of Post-Doctoral Researchers

N/A