Evaluating Effectiveness of an Embedded System Endpoint Security Technology on EDS OT: Defeating the Hackers of IIoT Devices

Website: http://cred-c.org/researchactivity/iiotdeveval

Researchers (MIT): Michael Siegel, Stuart Madnick, Gregory Falco, Keman Huang, Weilian Chu, Elizabeth Reilly, Mayukha S. Vadari

Industry Collaboration:

- Siemens, Smart Transportation Group
- Schneider Electric, Security Group

Other Collaboration:

- NRECA, IIoT EDS Data Collection & Analytics
- Pacific Northwest National Laboratory, ICS testbed group
- University of Illinois Urbana Champlain, ICS testbed group

Description of research activity: Industrial control systems have been shown to be vulnerable to cyberattacks as seen in high profile attacks such as Stuxnet (Zetter 2014). Multiple security approaches have been proven to be ineffective for IIoT EDS devices. There are several reasons for this. One is that antivirus programs need to house gigabytes of data and malware memory signatures. Considering the low memory, low processing power for these devices, it is impossible to run such solutions. This research aims to study an embedded end-point security technology that was originally designed for the unique requirements of enterprise IoT devices and customize it for EDS.

To implement this research, we are planning to collaborate with NRECA who has established a solution for collecting and analyzing IIoT EDS data. The proposed agenda is entirely complementary considering we aim to focus on the ability to securely deliver and then make actual changes to the endpoint without impacting operations. Our endpoint security mechanism can provide updates based on the recommendations from NRECA's system (other data gathering approaches may be used as needed).

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
The intention of this study will be to address the roadmap area: Develop and Implement New Protective Measures to Reduce Risk. The technology to be developed will include a lightweight agent that could fit on the endpoint of an EDS. The agent will have command and control capabilities that will act in parallel to the EDS firmware so that security updates to the OS environment will be done without affecting operations.

Summary of EDS gap analysis: Current IIoT EDS security solutions are inadequate and do not meet the requirements set in the Energy Delivery Systems Cybersecurity roadmap. Specifically, current solutions do not address the unique nature of IIoT networks.

While some current solutions claim to be 'secure', they each have known flaws. Adding additional application-level security improves security but is still susceptible to attacks that distort control signals or timing-based attacks. Similarly, network listening via packet sniffing fails to protect against message tampering upstream on the network. Virtual machines and system-on-chip solutions are also hindered by performance issues and scalability problems respectively.

Other DOE-funded security research programs such as NRECA's work initially focuses on data collection and analytics for IIoT EDS. Complementary to these solutions we allow for command and control over the endpoint to securely deliver and implement security updates.

Full EDS gap analysis: There is a substantial body of work concerning firewalls and security monitors for traffic security. However, this work is largely focused on TCP/IP, which is not often applicable for IIoT due to the unique protocols that

industrial devices use. Existing research assumes IIoT has similar attack surfaces to traditional IT systems, which is not the case. This is further exemplified by work on attack planning for TCP/IP and its current failure to incorporate IIoT-unique attack vectors.

Some work in EDS security has been done that involves including an application-level module in existing security monitors to evaluate anomalous activity on the network1 (Giani et al. 2009). This leverages existing intrusion detection techniques and attempts to add a layer of scrutiny to the system. This, however, fails to address attacks involving distorting control signals or timing-based attacks (which would traditionally be authorized signals in an IT system).

Another security monitor was developed for PLCs that involves a network tap to monitor raw traffic packets at the PLC interface2 (Hadžiosmanović et al. 2014). The traffic monitor analyzes the packets to determine the system's state. Models are used to determine if an expected state determined from the traffic analysis deviates from the messages. This approach must assume that the messages were not tampered with over the network considering they are intercepted at the PLC interface. Further, it fails to account for semantic level analysis that is needed for critical embedded systems that require operational context to perform safely and efficiently.

Similarly, a system-on-chip (SoC) solution was created for PLCs to capture traffic and program updates3 (Franklin et al. 2014). It is installed between the serial controller and network. The intent of the SoC ensures in real time that malicious traffic does not violate safety rules. The embedded nature of this solution is not scalable as it would need to be installed on every PLC in a system.

An alternative monitoring technique proposed for embedded systems includes a Virtual Machine based Attack Detection Agent and Servers connected to infrastructure4 (Tupakula & Varadharajan 2014). The intent of this system would be to monitor for anomalies in control systems randomly. The challenges with such an approach is manifold: detection rules will need to be specific based on the infrastructure (thus, scale is impossible), random monitoring may miss anomalous behavior which can occur intermittently (e.g. Stuxnet), and the communication overhead to feed information to a remote VM could hinder system performance.

Solutions such as NRECA's network tapping and analysis for IIoT EDS are very effective at detecting system abnormalities without affecting typical operations. Our work is complementary in that it can used to control the endpoint abnormal activity is detected via a patch or security update as no command and control mechanism is in place. Such solutions rely on manual updates that could be costly and impact uptime operations that are particularly critical to IIoT EDS.

The Roadmap to Achieve Energy Delivery Systems Cybersecurity 2011 calls for the development and implementation of new protective measure to reduce risk of attack. In Long-term milestones to be completed by 2020, it requires the development of a secure wireless communication system and capabilities for automated response to cyberattacks. Given these goals and the inadequacy of current security solution for IIoT EDS there is a requirement for an end-point security solution with secure communication capabilities.

Bibliography:

Cardenas, Alvaro, et al. "Challenges for securing cyber physical systems." Workshop on future directions in cyber-physical systems security. 2009.

ESCSWG. 'Roadmap to Achieve Energy Delivery Systems Cybersecurity'. September 2011.

Hadžiosmanović, Dina, et al. "Through the eye of the PLC: semantic security monitoring for industrial processes." Proceedings of the 30th Annual Computer Security Applications Conference. ACM, 2014.

Lerner, Lee W., et al. "Application-level autonomic hardware to predict and preempt software attacks on industrial control systems." Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on. IEEE, 2014.

Varadharajan, Vijay, and Udaya Tupakula. "Security as a service model for cloud environment." IEEE Transactions on Network and Service Management 11.1 (2014): 60-75.