A Physical Overlay Framework for Insider Threat Mitigation of Power System Devices

David Formby†, Sang Shin Jung†, Seth Walters‡, and Raheem Beyah†
Communications Assurance and Performance (CAP) Group†
Georgia Tech Research Institute (GTRI)‡
School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, GA 30332
Email: {djformby, sangsin}@gatech.edu, seth.walters@gtri.gatech.edu, raheem.beyah@ece.gatech.edu

***Abstract*—Nearly every aspect of modern life today, from businesses, transportation, and healthcare, depends on the power grid operating safely and reliably. While the recent push for a "Smart Grid" has shown promise for increased efficiency, security has often been an after-thought, leaving this critical infrastructure vulnerable to a variety of cyber attacks. For instance, devices crucial to the safe operation of the power grid are left in remote substations with their configuration interfaces completely open, providing a vector for outsiders as well as insiders to launch an attack. This paper develops the framework for an overlay network of gateway devices that provide authenticated access control and security monitoring for these vulnerable interfaces. We develop a working prototype of such a device and simulate the performance of deployment throughout a substation. Our results suggest that such a system can be deployed with negligible impact on normal operations, while providing important security mechanisms. By doing so, we demonstrate that our proposal is a practical and efficient solution for retro-fitting security onto crucial power system devices.**

I. Introduction

Due to a variety of pressures, ranging from environmental to economic, America's power grid is currently undergoing a transformation made possible by the continuing advances in computing and communication technologies. This new "Smart Grid" makes use of ubiquitous sensors and high-speed data networks to integrate renewable energy sources into the power grid while increasing overall efficiency and reliability of operations. A core piece of technology at the center of the power grid that enables all of this is supervisory control and data acquisition (SCADA) systems that allow efficient and intelligent control over wide areas [1]. Although the benefits of these two technologies are numerous, they bring with them several alarming security concerns.

The traditional power grid is separated into power generation, transmission across long distances, and distribution among end users. SCADA systems are deployed at various points throughout this network with remote terminal units (RTUs) collecting power and voltage measurements from, and issuing commands to intelligent electronic devices (IEDs). These measurements are then used to estimate the current state of the grid, perform optimal power flow calculations, and automatically send control signals to breakers and generators to match power generation with current consumption [2].

As the grid has transformed, the use of SCADA systems has changed as well. SCADA systems are relied upon to take even more fine-grained measurements and are being implemented over long-distance IP networks. This change has made it easier for outside attackers and insiders to compromise outdated and poorly protected equipment located in remote substations, and arguably wreak more havoc on the power system than was possible in the past.

One of the most well known examples of the kind of damage an insider attack can cause a cyber-physical control system occurred in the year 2001. A disgruntled ex-employee who had installed the SCADA system for the Maroochy water services in Australia drove around sending control signals to various pumps in the system. As a result, thousands of gallons of sewage was spilled into the surrounding area causing significant environmental and economic damages. Afterwards, forensic analysis concluded that proper use of access control and cryptography could have helped prevent the attack [3].

In this paper we develop a framework for a physical overlay network of critical interface locks (CILs) to mitigate the threat of insider attacks against remote power substation devices. These CILs provide access control to critical device interfaces, check the authenticity and integrity of configuration files, and provide monitoring of any communication with the critical device. The major contributions of this paper are:

- A flexible, modular design for a physical interface lock (i.e., CIL) for power system devices
- An overlay network architecture for interface locks that is efficient and scalable
- Evaluation of our proposal analyzing the effect of deploying such a system in a substation environment

The rest of this paper is organized as follows. In Section II we present related work in the area of securing power system networks, Section III describes the exact threat model addressed, and in Section IV we present the architecture of our proposed overlay network. Section V describes the details of our CILs, in Section VI we evaluate the performance of our proposal, and finally discuss our conclusions and future work in Section VII.

II. Related Work

The power grid, and control system networks in general, have unique security challenges that differentiate them from more traditional networks. Until recently, information security was not a primary concern in this area and as a result poor security practices and misconceptions, such as "security through obscurity" and misplaced confidence in air-gaps, were widespread.

To complicate these issues, due to the nature of these systems it is also often very difficult to keep equipment patched and up-to-date in order to protect against software vulnerabilities. Furthermore, as the Stuxnet attack [4] clearly illustrated, these weaknesses can be used to cause physical damage and achieve military-like goals. The abundance of security issues and their alarming consequences has led to a recent surge in research activity in this area.

In one of the first papers to really highlight the importance of the security of critical systems such as these, Ten et al. proposed a framework in 2008 for assessing the vulnerability of SCADA systems and suggested means of hardening them against various attacks [5]. Although this paper warned of the security threats faced by SCADA systems, it was not until a Chinese student in 2009 published a paper describing how vulnerable the US power grid was to cascading failure attacks, that this area of research finally started to get the attention it deserved [6]. That same year an article was published in the popular IEEE Security & Privacy magazine that gave a broad overview of the issues associated with the use of smart meters in the power grid to provide fine-grained power measurements and remote control of power consumption even at the electrical appliance level. The issues highlighted here included falsifying meter readings for financial gain, taking advantage of the remote control capabilities to conduct devastating terror attacks, and invasions of consumer privacy [7]. Another article was published in the IEEE Security & Privacy magazine the next year that covered the issues in more technical detail and explained the difficulties with applying current security technologies to the domain of the Smart Grid. The article argued that practical security solutions to the Smart Grid must be built in, scalable, designed to work on low-powered devices, and provide availability, integrity, confidentiality, and consumer privacy [8].

The communications aspect of the Smart Grid and its importance to the proper operation of the power system has been a significant area of research itself. In a 2012 paper by Sridhar et al. that discussed the security issues with cyber-physical systems, one of the key points argued was that cyber-physical systems, such as the Smart Grid, need to apply a defense-in-depth approach to security by focusing on how the control system relies on the underlying communications infrastructure [9]. Due to their flexibility and low cost implementation, the Smart Grid, and many other critical control systems, rely on wireless sensor devices to provide important real-time measurements over a wide area. The security strengths and weaknesses of the most commonly used protocols were analyzed in 2010, and suggestions were made for improvements.

Now that the myriad of security issues associated with the Smart Grid has been brought to light through several papers and studies, recent research has been focused on developing techniques and tools to address them. Metke et al. proposed methods of improving the security of the Smart Grid by building in security from the ground up and by implementing a Smart Grid PKI, but with so many legacy devices in the field, it is not very practical to deploy such a scheme any time soon [10]. With this in mind, most of the recent attempts to address critical infrastructure security has been to develop intrusion detection tools that could be deployed in current wide area control systems. In 2008, the Idaho National Laboratory published a paper describing how traditional Intrusion Detection Systems (IDS) fail to translate well to SCADA systems and proposed certain properties that a good SCADA-specific IDS should have, including deep packet inspection of SCADA protocols, having rules for which devices should communicate with each other, and having a basic understanding of which commands make sense for a given state of the system [11].

In 2009, although it did not perform SCADA specific protocol inspection, an IDS was developed using Artificial Neural Networks to learn what normal traffic looked like for an example control system and then was able to accurately detect various attacks on the system [12]. Another paper proposed deploying IDS modules trained by Machine Learning techniques at every layer of the Smart Grid to detect anomalous traffic [13]. Other proposed ideas for SCADA specific IDS have focused on understanding the underlying physical processes that the SCADA system is controlling. Cardenas et al. developed a model for a typical SCADA controlled physical process and then proposed means of detecting intrusions based on how anomalous behavior affected that model [14]. In similar works, proposals for IDS systems have focused on preventing the SCADA system from entering a dangerous state [15] [16]. Focusing on the Advanced Metering Infrastructure (AMI) component of the Smart Grid, Berthier et al. explained the requirements for designing an effective AMI IDS in a 2010 paper [17] and then proposed their own specification based IDS for AMI the next year [18].

While all of these ideas show promise for detecting intrusions at the network level, little work has been done to prevent attackers from accessing critical devices in the first place. Even if basic authentication is implemented on these devices, *there is no protection against an insider threat or an attempted exploit on an unpatched device*. A defense-in-depth approach to Smart Grid security that uses intrusion detection at the network level all the way down to the device level could significantly decrease chances of an attacker causing any harm to the system. Since it is impractical for companies to deploy physical locks on all critical device interfaces and keep track of physical keys, a scalable software based solution could be preferable. Commercial software is available [19] to lock down USB ports on a corporate network, but since most devices throughout the power grid are outdated and difficult to upgrade, this does not present a feasible solution. A more practical approach would be to deploy small, portable monitoring devices on all of the interfaces, such as the Israeli company Yoggie's Gatekeeper device [20]. However, the Gatekeeper was designed only for Internet traffic. This paper proposes to address these issues by developing the framework for an overlay network of lock devices that provide authenticated access control to the physical interfaces of critical power system devices and monitoring services for suspicious activity.

III. Threat Model

The threat model that our proposed solution addresses is one of an insider attack. The power system devices that this framework is designed to protect are assumed to be located in remote substations where a determined adversary or insider can

gain physical access with little chance of detection. Furthermore, although some power system devices do have basic password authentication, we assume that the attacker is an insider trusted with the password. Additionally, since it is common for these devices to have unpatched vulnerabilities, default passwords, or a poor choice of password, it is quite feasible for an outside attacker to bypass this basic authentication as well.

Once the adversary gains access to these devices, there are a variety of malicious actions he could take. For one, he could perform reconnaissance for a future attack by grabbing configuration files or data history logs to gain a better understanding of the power grid. He could also reconfigure the device to report data differently or trip a breaker under different conditions, potentially causing harm to the rest of the grid due to the unexpected behavior. Finally, in the worst case an attacker could gain complete control of the device and inject false data and commands into the network with disastrous results. We also assume that an adversary is limited to the computing power found on a typical laptop.

IV. Overlay Network

A typical substation can have on the order of twenty-five IEDs with around four different interfaces on each device. Our locks would be deployed on every interface and need to be able to reliably and securely communicate with the control center. The control center needs to be able to send maintenance records and software patches to the CILs and the CILs need to be able to send alerts and logging information back. The CILs will also transmit a periodic keep-alive beacon to the control center informing operators that the CIL is still online. If an adversary detaches the CIL, the device will power down and the beacon will cease. The control center will then know that the device has gone offline and that someone should check on the device in person. Additionally, deployment of such a system should have as little impact on the current infrastructure as possible and be able to operate reliably in a noisy substation environment.

With all of these factors taken into consideration, it was decided that the CILs would be deployed in a sensor network architecture using the Zigbee protocol, as illustrated in Figure 1. The low power wireless communication makes the CILs easy to deploy, and according to [21], the 802.15.4 protocol performs well in the substation environment compared to 802.11. Additionally, Zigbee supports encryption between links to ensure a secure connection with a gateway in the substation, which would then communicate with the control center through a secure channel such as SSL.

V. Critical Interface Lock

A. Modular Design

Devices found in the power system network today have several different physical interfaces available to communicate data and configuration settings. These include USB, Serial, Ethernet, and RJ-45 interfaces as can be seen from the back of an IED in Figure 2.

To make the deployment of our solution practical, it was developed with a modular design in mind that can provide the same security services to the device regardless of the interface.

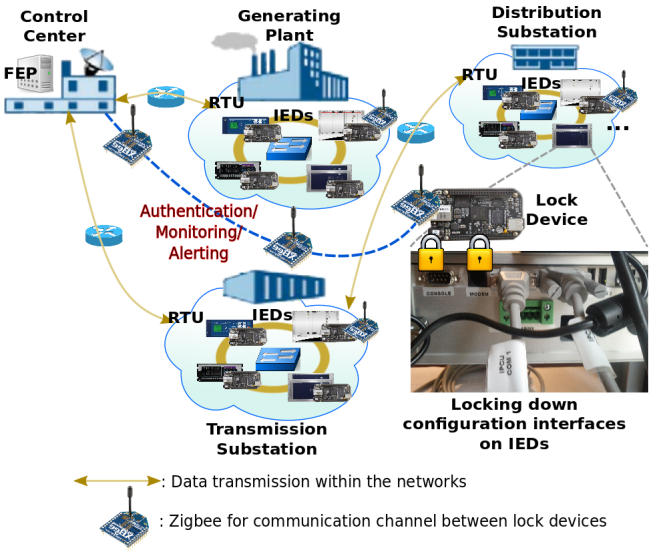

Fig. 1: Deployment in Power System.

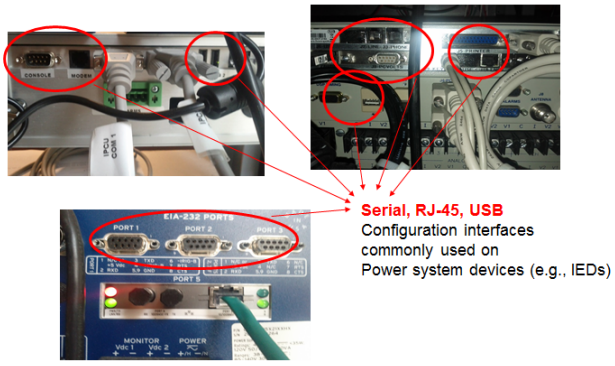

Fig. 2: Variety of interfaces found on the back of an IED.

For our prototype the USB interface was used, but a module could be developed for any interface and inserted into the framework for our CIL device as illustrated in Figure 3. We assume that our CILs will be securely attached to every interface on a device and enclosed in a tamper-resistant case. The security functions that our CILs provide for these interfaces include authenticated access control with one time passwords (OTP), file signature checks to ensure that configuration files came from the control center without being modified, and monitoring for suspicious activity.

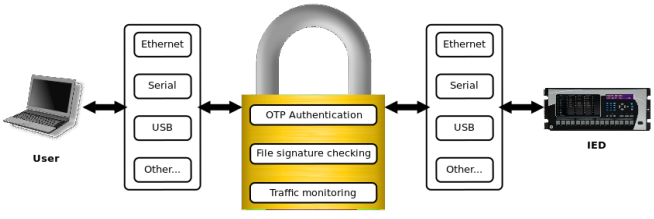

Fig. 3: Modular design of CIL device.

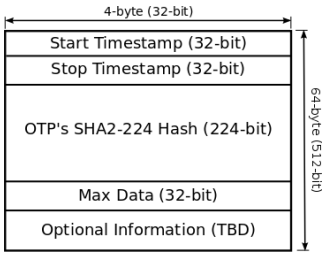

Fig. 4: Maintenance Record Structure.

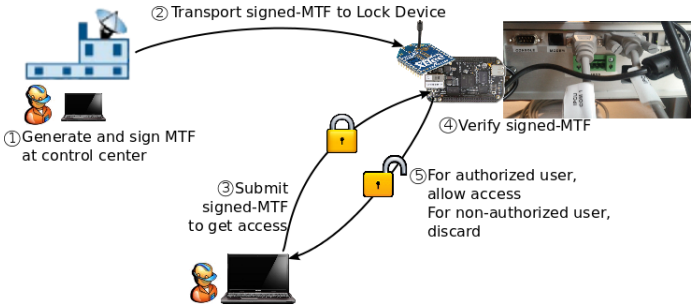

Fig. 5: Procedure for loading a maintenance file (MTF) onto an IED.

B. Security Services

1) OTP Authentication: The primary function of our solution is to provide improved access control over the weak, or non-existent, mechanisms in place in current substations. Maintenance on these critical devices happens fairly infrequently and is usually planned far in advance to ensure that consumers see no interruption in their power. We leverage this fact in the implementation of our solution by requiring that maintenance windows for every device also be scheduled in advance at the control center. Specifically, we propose that a maintenance "record" be created that includes the start and stop times for the maintenance window, the SHA224 hash of a randomly generated eight character OTP, and an estimate of the maximum data that a user is allowed to read from the device. We also allow for additional information to be included in such a record for extending the functionality to provide more fine-grained control of the user's connection, such as specifying exactly what files can be loaded. The structure of such a record is illustrated in Figure 4. When maintenance must be performed on a device, a trusted individual at the control center creates a record as described above and sends it to the corresponding CIL. The CIL will then only allow a complete connection to be made if the user provides a password that has the same SHA224 hash as the one in the record, and if the user does this during the specified time window. Once a user passes this authentication mechanism, the CIL will begin to act as a man-in-the-middle device, allowing communication between the user and the power device, but monitoring everything that happens.

2) File Signature Checking: We again leverage the fact that maintenance happens infrequently and must be scheduled in advance at the control center in order to provide integrity checks for important configuration files. To accomplish this, we assume that a trusted individual creates the configuration or maintenance file (MTF) ahead of time at the control center and signs it with a 2048 bit RSA secret key: $Sign_{k_{priv}}(Hash(MTF))$.

As explained above, after a user passes the OTP authentication the CIL acts as a man-in-the-middle device and is able to monitor the communication. When the CIL sees a maintenance file being loaded onto a power system device, it will verify that the signature matches with the control center's public key: $Verify_{k_{pub}}(Hash(MTF))$. If the signature is verified, then the file passes through without any further action taken. However, we considered two choices for what actions to take if the signature verification failed.

Alert and Drop: With this option, the CIL would send an alert back to the control center and prevent the file from being loaded onto the device. This option provides better security guarantees by ensuring that malicious configuration files do not get loaded onto critical devices, but does so at the cost of availability. In the real world, it might not always be practical to have the exact configuration file created beforehand at the control center and small changes might have to be made at the remote substation. Therefore this option might cause too many problems to allow for practical deployment.

Alert and Pass: Under this policy the CIL device would send an alert back to the control center letting the operators know that a different configuration file was loaded than the one that was signed. However, to accommodate for the real world scenario where small changes might need to be made at the last minute, the CIL device will still allow the file to be loaded. It was eventually decided that practicality outweighed the extra security guarantees and so this latter option was chosen.

The overall procedure for loading a new configuration or maintenance file (MTF) onto an IED is illustrated in Figure 5.

3) Traffic Monitoring and Alerts: Since our proposed CILs are able to monitor all of the communication between the user and the power system device, they can be used as an intrusion detection system to look for signs of malicious activity. As described above, one of the uses for this functionality is sending alerts back to the control center if a configuration file signature does not match with the control center's public key. Another case in which the CIL device will send an alert to the control center is if a user attempts to read more data from the IED than was allowed in the maintenance record. Although our current prototype only checks the integrity of files and measures how much data is being read from the IED, it can also be extended further to perform even more complex intrusion detection functions. Examples of this could include creating models of behavior for certain types of maintenance or devices and alerting if observed behavior falls outside these models.

C. Implementation Details

The hardware used to build the prototype CIL device for this research was the BeagleBone Black loaded with the Debian operating system. The small form-factor, low power requirements, and limited resources all made it suitable for the application of a distributed network of CIL devices. Specifically, this board can be powered over USB, has a 1GHz ARM processor with

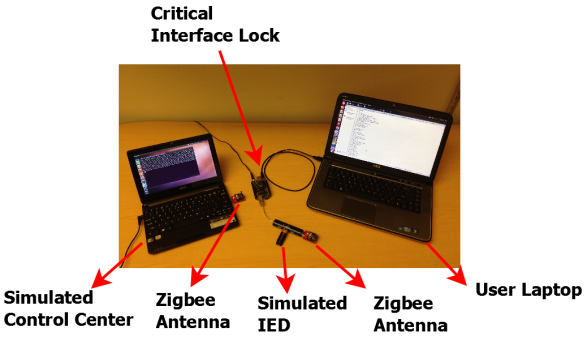

Fig. 6: Current prototype being tested with USB flash drive and simulated control center.

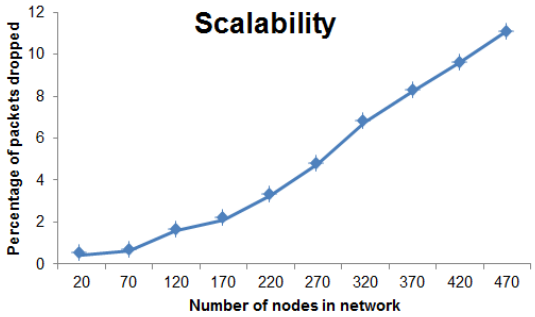

Fig. 7: Scalability of Network Architecture.

512MB of RAM, and is extremely flexible. In addition to the custom security mechanisms described in the previous section, we were able to load other popular security software including Snort network IDS, Clam Antivirus, and Tripwire host IDS.

To perform the USB monitoring on our CIL device, we used the USBProxy Git Hub project developed by Dominic Spill [22]. The USBProxy project is a framework designed for the BeagleBone Black to enable the board to act as a USB man-in-the-middle. Although this project is still in its early stages of development, we modified the basic logging filter provided by the project to also check for the OTP and digital signature of configuration files.

To test our implementation we modeled a generic power system device by using a USB storage device and writing an actual IED configuration file to it. Since these CILs would be deployed in a sensor network architecture as described in section IV, we also used Zigbee USB dongles to model communication between our device and a control center. The modified USBProxy code on the BeagleBone Black was able to operate on the targeted USB storage device while still being able to communicate with our stand-in control center. The setup for these experiments can be seen in Figure 6.

VI. Evaluation

A. Scalability

Since our CILs would be used to protect every interface in a substation, it is necessary that the sensor network architecture we use be able to scale and perform well in a typical substation. As mentioned above, an average substation was estimated to have about twenty-five IEDs with about four interfaces each, coming to a total of 100 devices. To measure how well our system would scale, we assumed a worst case scenario where every CIL in the network tries to send a 512-bit alert back to the control center and simulated the packet loss percentage with an increasing number of nodes in the network using the MiXiM framework developed for the Omnet++ modeling software. For each network size, we ran a twenty second simulation where each node generates a 512-bit packet every second and used the MiXiM framework to estimate the packet loss. The graph in Figure 7 shows that using the estimate of 100 nodes in the substation network, less than two percent of the packets are expected to be dropped, which was deemed an acceptable rate. The figure also illustrates that the network could be scaled to bigger sizes as well, with a trade-off in performance.

TABLE I: Performance of USB man-in-the-middle device.

Measurements	Performance
Size of config file	6.4 KB
Time for signature validation	17 ms
Read speed for USB drive	1.2 MB/s
Write speed for USB drive	1.0 MB/s
Combined read/write time	12 ms
Total	29 ms

B. Performance

Another important measurement when evaluating the effectiveness of our solution was the added latency and computation time that our man-in-the-middle device introduces to the normal interaction between a user and an IED. It is necessary that we keep this low enough that the user is still able to perform everything he would normally do without any noticeable changes. To do this we performed the signature validation of an actual configuration file one hundred times on the BeagleBone Black to get an estimate of the time it takes. We then used the Linux disk utility to benchmark the read and write speeds for the USB drive that was connected through our CIL device in the middle. The total time to write a file, check its signature, and read a typical file back was then estimated to take a total of 29 ms, which is unnoticeable to the typical user. The results of these tests are summarized in Table I.

C. Security

Finally, we performed some basic estimates of the strength that the OTP time window authentication scheme provides for critical power system devices. We assume that maintenance windows will be scheduled for a range of a few hours, or in the worst case the range of a whole day. This means that we assume that a randomly generated OTP will be valid for an entire day at the most, so an adversary has roughly 24 hours to guess the password. Assuming a threat model where an adversary was able to overhear the SHA224 hash of the OTP and has the computing power of a standard laptop, we estimated how long it would take

to crack. Assuming that the OTPs are alphanumeric passwords generated with strong randomness, the adversary would have to brute force guess every possibility to find the correct password. For each guess he would have to take the SHA224 hash of the password and compare it with the one he overheard. After performing 1000 sample of hashing and comparing the hash on a 2.2 GHz quad core 8GB RAM laptop, it was estimated that each guess would take about 4 microseconds. With an OTP of eight characters, this means that it would take more than 7 years for an adversary to guess it, which is well beyond any reasonable maintenance window. Considering a stronger threat model where an adversary is able to efficiently offload and parallelize this calculation onto a botnet or cloud of 1000 such laptops, it would still take weeks to crack, which is longer than any reasonable maintenance window.

VII. Conclusion and Future Work

Many devices critical to the safe operation of the power grid are left virtually unprotected in remote substations with their configuration interfaces completely exposed. These open interfaces provide adversaries with an alarming attack vector which they can use to cause damage to the grid or steal sensitive information. To address this problem, a framework for a physical overlay network of modular critical interface lock devices was developed that provides access control, integrity checking, and security monitoring. When used properly, the access control and integrity check schemes were shown to provide strong security for the vulnerable interfaces while adding a negligible amount of latency in the communication. Additionally, a network of such devices was simulated and estimated to scale well beyond the required size with no significant decrease in performance. Our results show that the proposed framework is a practical solution for providing important security mechanisms to critical power system devices.

For future work, the monitoring and intrusion detection features of our CIL network can be extended in a variety of ways. For example, it may be desirable to implement some intelligent combination of the "Alert and Drop" and the "Alert and Pass" policies depending on the type of device being configured or the type of file being loaded. The complexity of the intrusion detection algorithms could also be extended by developing models of behavior for different types of maintenance procedures or by developing algorithms to understand the syntax of configuration files and try to determine if a file is "safe" or not before loading it.

References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power and Energy Magazine*, vol. 7, pp. 52–62, March 2009.

[2] F. Wu, K. Moslehi, and A. Bose, "Power system control centers: Past, present, and future," *Proceedings of the IEEE*, vol. 93, pp. 1890–1908, Nov 2005.

[3] M. Abrams and J. Weiss, "Malicious control system cyber security attack case studymaroochy water services, australia." http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf, 2008.

[4] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, pp. 49–51, May 2011.

[5] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Transactions on Power Systems*, vol. 23, pp. 1836–1846, Nov 2008.

[6] J.-W. Wang and L.-L. Rong, ""cascade-based attack vulnerability on the us power grid "," *Safety Science*, vol. 47, no. 10, pp. 1332 – 1336, 2009.

[7] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, pp. 75–77, May 2009.

[8] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[9] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, pp. 210–224, Jan 2012.

[10] A. Metke and R. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, pp. 99–107, June 2010.

[11] J. Verba and M. Milvich, "Idaho national laboratory supervisory control and data acquisition intrusion detection system (scada ids)," in *2008 IEEE Conference on Technologies for Homeland Security*, pp. 469–473, May 2008.

[12] O. Linda, T. Vollmer, and M. Manic, "Neural network based intrusion detection system for critical infrastructures," in *Proceedings of the 2009 International Joint Conference on Neural Networks*, IJCNN'09, (Piscataway, NJ, USA), pp. 102–109, IEEE Press, 2009.

[13] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Transactions on Smart Grid*, vol. 2, pp. 796–808, Dec 2011.

[14] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, (New York, NY, USA), pp. 355–366, ACM, 2011.

[15] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in scada systems," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 2, pp. 179–186, 2011.

[16] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Semantic security analysis of scada networks to detect malicious control commands in power grids," in *Proceedings of the First ACM Workshop on Smart Energy Grid Security*, SEGS '13, (New York, NY, USA), pp. 29–34, ACM, 2013.

[17] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 350–355, Oct 2010.

[18] R. Berthier and W. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 184–193, Dec 2011.

[19] A. S. International, "Usb lock rp." https://usb-lock-rp.com/.

[20] P. Miller, "Yoggie's mini-computer offloads security duties." http://www.engadget.com/2006/09/26/yoggies-mini-computer-offloads-security-duties/, 2006.

[21] S. Bhatti, Q. Shan, R. Atkinson, and I. Glover, "Performance simulations of wlan and zigbee in electricity substation impulsive noise environments," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, pp. 675–679, Nov 2012.

[22] D. Spill, "Usbproxy." https://github.com/dominicgs/USBProxy, 2014.