A PHYSICAL OVERLAY FRAMEWORK FOR INSIDER THREAT MITIGATION OF POWER SYSTEM DEVICES

A Thesis
Presented to
The Academic Faculty

by

David Formby

In Partial Fulfillment
of the Requirements for the Degree
Masters of Science in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
December 2014

A PHYSICAL OVERLAY FRAMEWORK FOR INSIDER THREAT MITIGATION OF POWER SYSTEM DEVICES

Approved by:

Dr. Raheem Beyah, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. John Copeland
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Sakis Meliopoulos
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: 17 November 2014

ACKNOWLEDGEMENTS

Foremost, I would like to thank my advisor, Dr. Beyah, for his constant guidance and support over the long course of this research. I also thank the members of my thesis committee for the time they took to read my work and provide insightful comments.

I would like to express my gratitude to my lab mates, Sang Shin Jung and Chris Wampler, for providing valuable technical advice at various stages of my research when I hit road blocks and needed some assistance.

Finally, I could not have done any of this without the continued love and support from my caring family and friends.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

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 afterthought, 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.

CHAPTER 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 [8]. 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 [22].

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 [1].

In this thesis 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 thesis 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 thesis is organized as follows. In Chapter 2 we present related work in the area of securing power system networks, Chapter 3 describes the exact threat model addressed, and in Chapter 4 we present the architecture of our proposed overlay network and describe the details of our CILs. In Chapter 5 we evaluate the performance of our proposal, and finally discuss our conclusions and future work in Chapter 6.

CHAPTER 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 [10] 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 [18]. 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 [21]. 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, invasions of consumer privacy, and taking advantage of the remote control capabilities to conduct devastating terror attacks [13]. 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 [9].

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 [17]. 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 [14]. 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 [20].

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 [23]. 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 [6]. In similar works, proposals for IDS systems have focused on preventing the SCADA system from entering a dangerous state [5] [11]. 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 [3] and then proposed their own specification based IDS for AMI the next year [2].

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 [7] 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 [15]. However, the Gatekeeper was designed only for Internet traffic. The solutions that come closest to solving all of these problems are bump in the wire (BITW) devices, such as YASIR. In 2008, YASIR was proposed as a unique BITW solution that provided encryption and authentication to SCADA communication over time-sensitive serial links [19]. While this solution goes a long way towards protecting

legacy SCADA equipment, it does not clearly address the issue of open interfaces on SCADA equipment or how it can protect against insiders who are occasionally allowed to perform on-site maintenance. This thesis 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.

CHAPTER 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.

CHAPTER IV

OVERLAY FRAMEWORK

4.1 Network

A typical substation can have on the order of twenty-five IEDs with around four different interfaces on each device. We assume our locks could 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 need to 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. To prevent against a beacon spoofing attack, the CIL will include a signed time stamp in its beacon using a private key assigned to it at configuration. When the control center receives the beacon, it will verify that it is signed by the lock device and that the time stamp is recent. Additionally, deployment of such an overlay network 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. ZigBee is an entire protocol stack based on the IEEE 802.15.4 standard developed for low data rate, long battery life wireless personal area networks (WPAN), and is commonly used in building automation and sensor networks. The CILs would require very small data transfers at intermittent times, which fits well with the design goals of ZigBee. The low power aspect of ZigBee keeps the CILs to a small form factor and makes upkeep much easier. Another major advantage that ZigBee has over other wireless options is its reliability and robustness. According to Bhatti et al. [4], the 802.15.4 protocol was found to perform

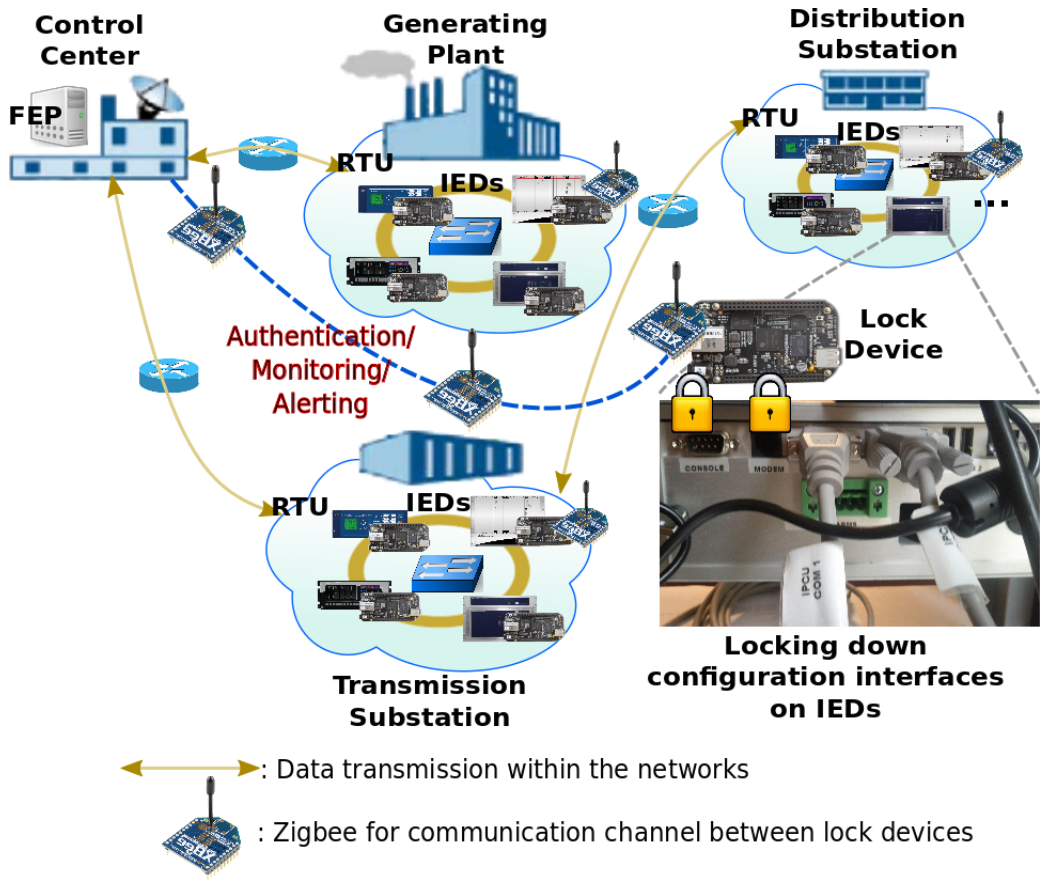


Figure 1: Deployment in Power System.

relatively well under the type of impulsive noise generated in the substation environment compared to the more common 802.11 standard. Finally, 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/TLS.

4.2 Interface Lock

4.2.1 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, and RJ-45 Ethernet 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

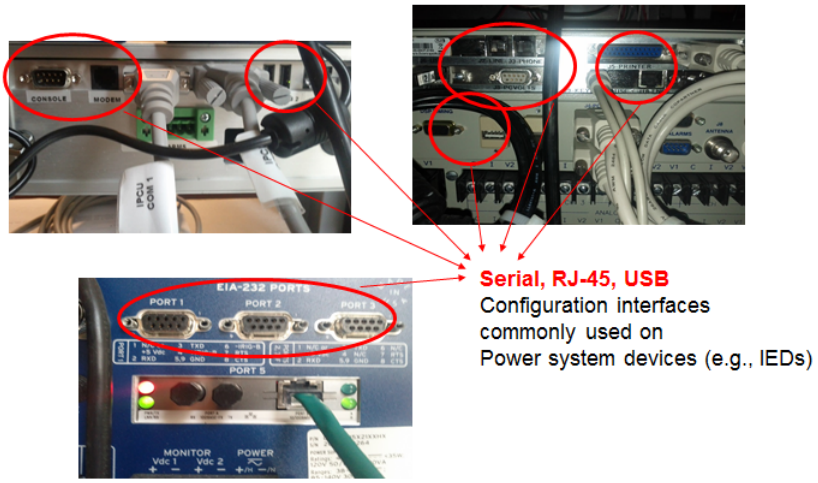


Figure 2: Variety of interfaces found on the back of an IED.

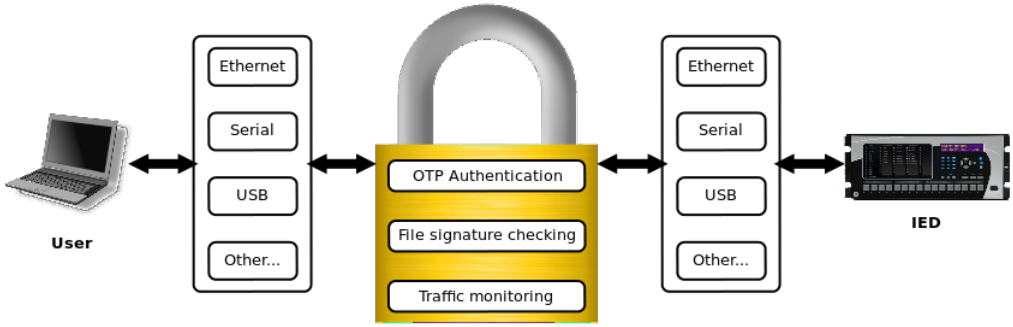


Figure 3: Modular design of CIL device.

interface. 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. When developing our overlay framework we assume that our CILs will be securely attached to every open interface on a device and enclosed in a tamper-resistant case. We acknowledge that these are no easy tasks to complete, but any attempt at retrofitting security onto legacy equipment in remote locations will have the same issues. We also believe that the keep-alive beacon feature of the CILs makes it much harder for adversaries to tamper with the device undetected. The security functions that our CILs provide for the vulnerable power system interfaces include authenticated access control with one time passwords (OTP), file signature checks to ensure that configuration files came from the control center without

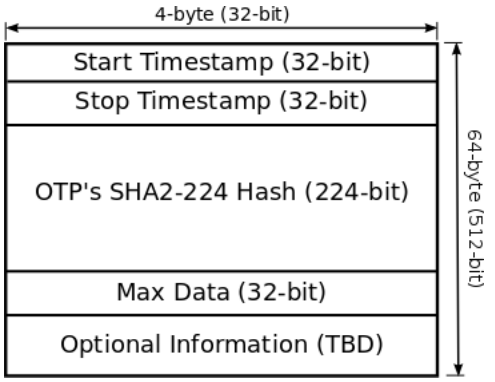


Figure 4: Maintenance Record Structure.

being modified, and monitoring for suspicious activity.

4.2.2 Security Services

4.2.2.1 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 hash of a randomly generated 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 a typical maintenance record is illustrated in Figure 4.

Authentication using randomly generated OTPs, instead of traditional long term passwords, was chosen for stronger security guarantees. Firstly, even if a traditional password scheme was used with "strong" passwords, it would provide no real improvement over the current situation in the case of insider threats. An insider entrusted with the long term password for legitimate work could return later to also use the password for illegitimate

activity. By using an OTP valid only during a specified time window, we can significantly reduce the chances of an insider performing unauthorized actions without being detected. Secondly, an OTP solution reduces the threat of compromised passwords. If an outside attacker manages to steal an OTP, he has a limited window of attack before the password expires. We propose that the OTP used be eight characters long as a compromise between difficulty in brute-forcing and ease of use.

While we assume that the communication between each CIL and the control center is protected through secure channels and that the CIL itself is relatively tamper proof, we provide additional protection when transporting the OTP in the rare chance that the adversary overhears the communication or is able to retrieve the stored OTP from the CIL. Instead of communicating or storing the clear-text of the OTP, we transmit and store the hash of the OTP. This way, if an attacker manages to overhear the hash, he must brute-force search through all possible passwords to find which one generated that specific hash. Given a long enough password and short enough time window, the time to find the correct OTP becomes greater than the time that the OTP is valid, giving the adversary no opportunity to use it. The specific hashing algorithm we propose to use in our framework is SHA2-224. This hashing algorithm was chosen because it is currently believed to be secure and the shorter hash length (224 bits) makes it easier to transport over the low data-rate ZigBee links.

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 SHA2-224 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.

4.2.2.2 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 the control center's private key: $Sign_{k_{priv}}(Hash(MTF))$. Again, the hash function that was decided on was SHA2-224 due to the current belief in the community that it is secure, and because the smaller size makes it slightly easier to handle with the limited resources available on the CIL. The public key cryptography algorithm that we propose to use is RSA with 2048 bit keys. As of now, there are no known efficient attacks against RSA and 2048 bit keys are the recommended length for strong security.

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

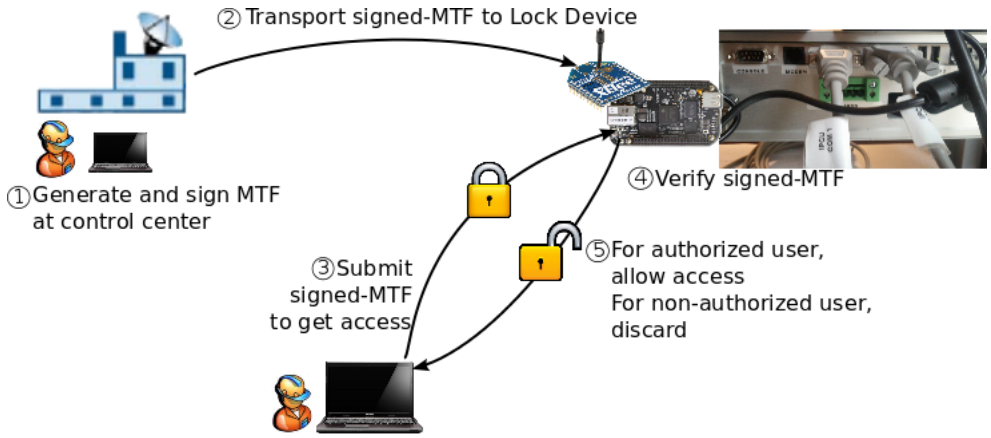


Figure 5: Procedure for loading a maintenance file (MTF) onto an IED.

guarantees and so this latter option was chosen.

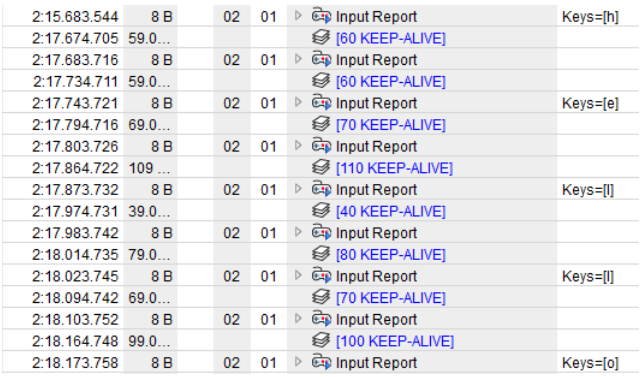
The overall procedure for loading a new configuration or maintenance file (MTF) onto an IED is illustrated in Figure 5.

4.2.2.3 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.

4.2.3 Implementation Details

The hardware used to build the prototype CIL device for this research was the Beagle-Bone Black loaded with the Debian operating system. The small form-factor, low power



2:15.683.544	8 B	02	01	Input Report	Keys=[h]
2:17.674.705	59.0...			[60 KEEP-ALIVE]	
2:17.683.716	8 B	02	01	Input Report	
2:17.734.711	59.0...			[60 KEEP-ALIVE]	
2:17.743.721	8 B	02	01	Input Report	Keys=[e]
2:17.794.716	69.0...			[70 KEEP-ALIVE]	
2:17.803.726	8 B	02	01	Input Report	
2:17.864.722	109 ...			[110 KEEP-ALIVE]	
2:17.873.732	8 B	02	01	Input Report	Keys=[l]
2:17.974.731	39.0...			[40 KEEP-ALIVE]	
2:17.983.742	8 B	02	01	Input Report	
2:18.014.735	79.0...			[80 KEEP-ALIVE]	
2:18.023.745	8 B	02	01	Input Report	Keys=[l]
2:18.094.742	69.0...			[70 KEEP-ALIVE]	
2:18.103.752	8 B	02	01	Input Report	
2:18.164.748	99.0...			[100 KEEP-ALIVE]	
2:18.173.758	8 B	02	01	Input Report	Keys=[o]

Figure 6: Example capture of USB keyboard traffic.

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 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. Another advantage of the BeagleBone Black is that it has both a host and client USB interface to enable the man-in-the-middle functionality necessary for implementing our CIL for USB communications.

Given the USB interfaces on the BeagleBone Black, we decided to initially implement our prototype only for USB communication. To study the way devices communicate over USB, we first used a commercial USB protocol analyzer to monitor traffic between common devices such as keyboards and mass storage devices. For example, Figure 6 illustrates the USB traffic that occurs when a user types the word “hello” on a USB keyboard. One important thing to note is the presence of keep-alive messages in the protocol, that significantly complicate the task of designing a USB man-in-the-middle monitor that can provide all the security services we propose for out CILs.

To perform the USB monitoring on our CIL device, we used the USBProxy Git Hub project developed by Dominic Spill [16]. The USBProxy project is a framework designed specifically 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

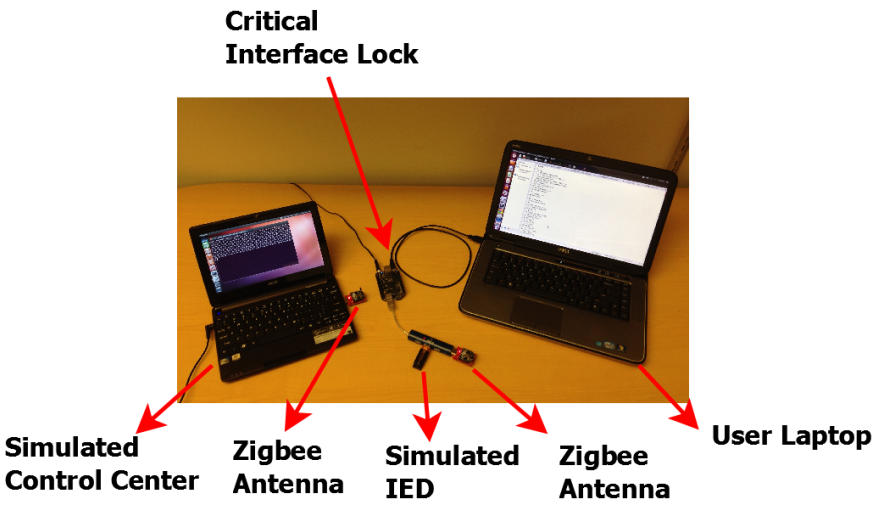


Figure 7: Current prototype being tested with USB flash drive and simulated control center.

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 Chapter 4.1, 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 7.

CHAPTER V

EVALUATION

5.1 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 performed simulations of different sized networks using the MiXiM framework developed for the Omnet++ modeling software under the worst case scenario where every CIL in the network tries to send an alert at the same time. We assume that each alert if 512 bits, there is no other interference, and the devices are randomly placed in a 30 meter by 30 meter area. 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 8 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.

5.2 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,

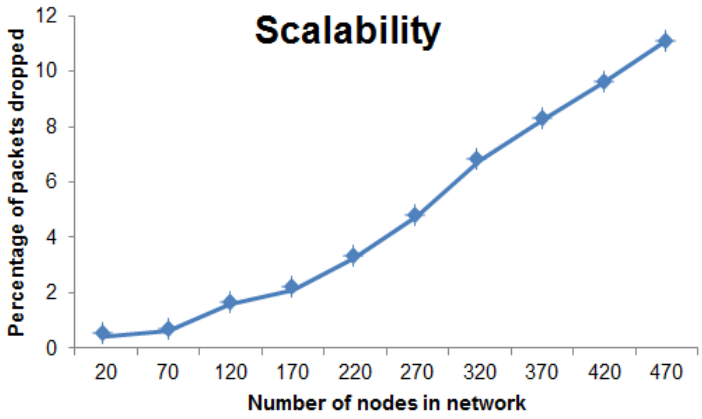


Figure 8: Scalability of Network Architecture.

Table 1: 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

check its signature, and read a typical file back was then estimated to take a total of 29 ms. While the signature validation may add too much latency for time-critical operations, 29 ms is completely unnoticeable to the typical user performing standard maintenance on the device. The results of these tests are summarized in Table 1.

Although we did not implement and test the framework for Ethernet or RS-232, we can make fairly accurate estimates as to how they would perform based on their standard speeds and the fact that the signature validation time will remain the same. Assuming the slowest Ethernet speed of 10 Mbps (1.25 MB/s) we can expect Ethernet to perform roughly the same as USB and even better if the faster standards of 100 Mbps or 1Gbps are used.

RS-232 supports a wide range of baud rates, but assuming the most common speed of

9600 bps, we can estimate that the read and write speeds will be about 1000 times slower than USB. Since buffering the file on the CIL introduces an extra write or read time in the process, we can expect that the total time would roughly double. In our example writing a 6.4 KB file would normally take 0.68 seconds over a 9600 bps link, but would instead take (0.683s * 2 + 17ms) 1.383 seconds going through the CIL. While this may be slightly noticeable to a user, it would not significantly hinder his ability to perform the required maintenance task.

5.3 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.

CHAPTER VI

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] Abrams, M. and Weiss, J., "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.

[2] Berthier, R. and Sanders, W., "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.

[3] Berthier, R., Sanders, W., and Khurana, H., "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.

[4] Bhatti, S., Shan, Q., Atkinson, R., and Glover, I., "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.

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

[6] Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., and Sastry, S., "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.

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

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

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

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

[11] Lin, H., Slagell, A., Kalbarczyk, Z., Sauer, P. W., and Iyer, R. K., "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.

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

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

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

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

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

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

[19] Tsang, P. and Smith, S., "Yasir: A low-latency, high-integrity security retrofit for legacy scada systems," in *23rd International Information Security Conference (SEC 2008)*, August 2008.

[20] Verba, J. and Milvich, M., "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.

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

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

[23] Zhang, Y., Wang, L., Sun, W., Green, R., and Alam, M., "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.