5-2014

Electric Power Synchrophasor Network Cyber Security Vulnerabilities

Christopher Beasley
Clemson University, beasle6@g.clemson.edu

Electric Power Synchrophasor Network Cyber Security Vulnerabilities

---

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Computer Engineering

---

by
Christopher T. Beasley
May 2014

Accepted by:
Dr. Richard Brooks, Committee Chair
Dr. G. Kumar Venayagamoorthy, Committe Co-Chair
Dr. Kuang-Ching Wang

Abstract

Smart grid technologies such as synchrophasor devices (Phasor Measurement Units (PMUs)), make real-time monitoring, control, and analysis of the electric power grid possible. PMUs measure voltage and current phasors across the electrical power grid, add a GPS time stamps to measurements, and sends reports to the Phasor Data Concentrators (PDCs) in the control centers. Reports are used to make decisions about the condition and state of the power grid. Since this approach relies on Internet Protocol (IP) network infrastructure, possible cybersecurity vulnerabilities have to be addressed to ensure that it is stable, secure, and reliable.

In literature, attacks that are relevant to PMUs, are discussed. The system modeled is the benchmark IEEE 68 bus (New England/New York) power system. This document details vulnerability testing performed on a network implemented with a real-time grid simulator, the Real Time Digital Simulator (RTDS), with SEL PMU devices monitoring several bases. The first set of security vulnerabilities were found when running traffic analysis of the network. In using this approach it was found that the system was susceptible to Address Resolution Protocol (ARP) poisoning. This allowed the switch to be tricked so that all network traffic was rerouted through the attack computer. This technique allowed for packet analysis, man-in-the-middle, and denial of service (DOS) attacks.

Side channel analysis was used to distinguish PMU traffic across the virtual

private network (VPN) established by the security gateways. After the traffic was collected, the inter-packet delays were used to construct a Hidden Markov Model. This model was used to distinguish measurement packets being transported across the VPN. Once the measurements are identified, a DOS attack can be performed on the network.

While this document unveils certain security vulnerabilities within the PMU network, further testing is needed to provide a full security vulnerability analysis. A future security agenda is proposed.

Acknowledgments

First, I would like to thank my advisor Dr. Richard Brooks and my co-advisor Dr. G. Kumar Venayagamoorthy. Without their knowledge, guidance, and support this thesis could not have been written. I would also like to thank you for your unending patience and dedication of time. Additionally, I would like to thank Dr. Kuang-Ching Wang for serving on my committee.

Second, I would like to thank my family. Without your love, dedication, and support none of this would have been possible.

I would like to thank all of the members of Dr. Richard Brooks' research group for their support and guidance during the course of this project.

I would like to thank the Real-Time Power and Intelligent Systems (RTPIS) Laboratory (http://rtpis.org/) for allowing me to work in the facilities used to perform the experiments.

Last but not least, I would like to acknowledge the National Science Foundation for providing the financial support. This work is supported by the National Science Foundation contract/grant number 1312260. The views and conclusions herein are those of the authors and not the National Science Foundation.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Electricity is essential to maintaining the standard of living in North America and globally. Citizens need the electrical infrastructure to be reliable. Increasing consumption requires that either more energy be produced or energy generation be increasingly efficient. The smart grid is a modern power system that uses information and communication technologies to provide efficient, reliable, and sustainable energy [34]. A smart grid allows for bidirectional flow of information and energy in the transmission and distribution systems [22]. Real-time monitoring provides situational awareness, and ensures that power is continuously available to consumers. Although, real-time feedback is critical to power system operations, communications are susceptible to cyber-attack.

Previous research has investigated PMU vulnerabilities to Denial of Service (DOS), malicious code injection, packet analysis, physical damage, Man-in-the-Middle, and data spoofing attacks. Each attack affects the network in different ways. Each attack can be put into attack classes: interruption, interception, modification, and fabrication [31]. Each attack class effects the network in a different manner.

Although, there are some documented attacks, little research has been done

on addressing known network vulnerabilities with regard to PMU networks. Further research will need to be applied, to evaluate their affects.

This thesis discusses previously documented attacks as well as the evaluation of the security vulnerabilities found. The goal is to provide details of possible attacks so that possible countermeasures can be found. Documented attacks give a background knowledge of current vulnerabilities. The security vulnerability testing based on traffic analysis and side-channel attacks is documented. Before presenting the methods, background on the previously researched attacks is given in Chapter 2. The remainder of this Chapter details the organization of this thesis.

1.1 Organization

This thesis is organized as follows.

- Chapter 2 presents background information. PMU networks, the security gateway, Documented Attacks on PMU networks, DOS countermeasures, malicious code injection countermeasures, and data spoofing countermeasures are presented.
- Chapter 3 describes ARP poisoning to perform a Man-in-the-Middle and DOS attack. Packet analysis performed on the network is also discussed with recommendations on how to make the network less vulnerable.
- In Chapter 4, introduces the side channel analysis performed. Hidden Markov Models were used to recognize traffic across the VPN.
- The thesis concludes in Chapter 5. A summary of the thesis and proposed future work will be introduced.

1.2 Contributions

This thesis contributes to the area of PMU network security. Specifically, it introduces documented attacks found through literature review, exposes vulnerabilities found during traffic analysis and side channel analysis, and provides a direction for future vulnerability testing. The primary objective of this thesis is to address security vulnerabilities so that possible countermeasures can be found.

Part of this thesis work has been published in the 2014 Clemson University Power Systems Conference "Cyber Security Evaluation of Synchrophasors in a Power System".

Chapter 2

Background

This Chapter provides background on the PMU network and researched attacks. We begin by presenting PMU network basics, the protocol used, and the GPS synchronized time stamp. Then details of the security gateway and VPN are provided. Following the discussion of the security gateway, the documented attacks and counter measures are discussed. A brief summary concludes this chapter.

2.1 PMU Network

Phasor measurement units measure bus voltages, line currents, and frequency of real-time power systems. Each measurement is tagged with a global positioning system (GPS) time stamp [23]. PMU readings with time stamps let the system operators diagnose problems and evaluate changing power conditions. Data is usually reported to the Phasor Data Collector (PDC) via TCP/IP and stored for analysis [35]. Global Positioning System (GPS) time stamps allow measurements to be synchronized so the network can be analyzed as a whole [4].

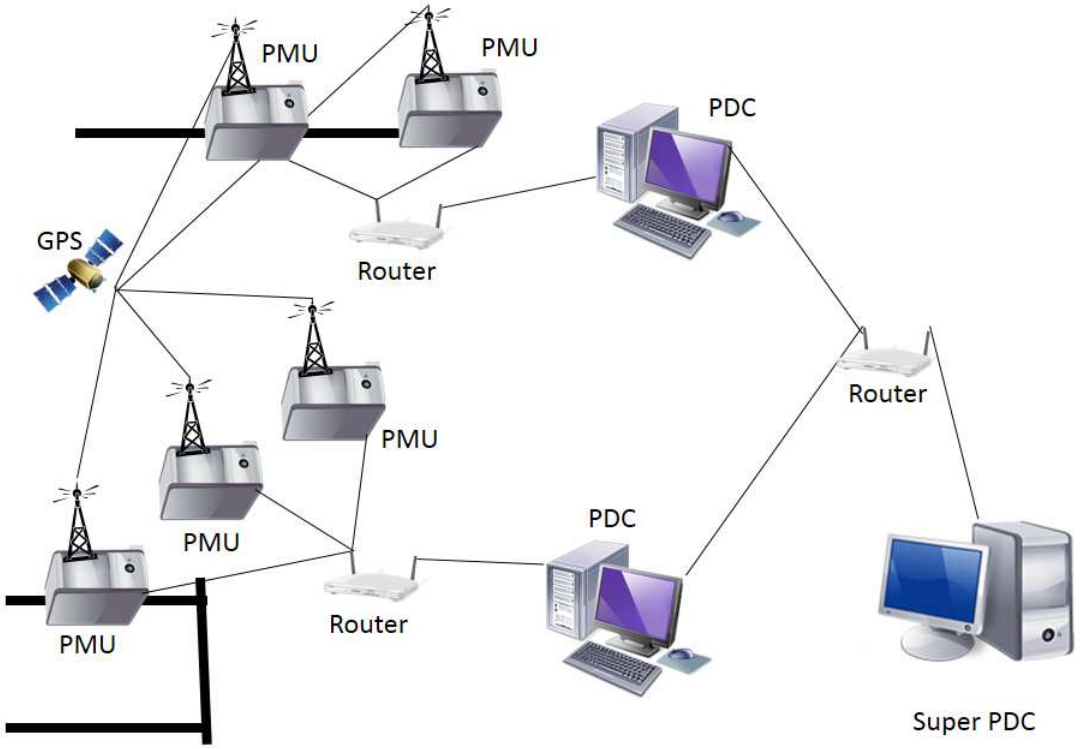

Figure 2.1: Typical PMU Network Architecture

Figure 2.1 shows the structure of a typical PMU network. Once synchrophasors synchronize with the GPS, each measurement they send across the network includes a time stamp. Electrical distribution line measurements are sent by PMUs over a network connection to a PDC. The PDC is a regional command station for the grid [18]. The PDC stores measurements for additional processing.

2.1.1 PMU Protocol

Since PMUs are widely distributed and used by many electric power utilities, a standard protocol ensures consistent data storage and network communications between PMU networks. The current PMU communications standard is the IEEE

C37.118 protocol, which defines synchrophasor data conventions, measurement accuracies, and communications formats [20]. To adhere to the IEEE C37.118 protocol, the synchrophasor has to recognize five frame types [20]:

- Data frame (binary),
- Two configuration frames (binary),
- Header frame (ASCII),
- And command frame (binary).

The configuration and header frames describe the synchrophasor configuration, the data frame contains measurements, and the command frame tells the PMU when to start and stop taking measurements [20]. Once measurements have been collected, they are processed using a phasor data concentrator (PDC) such as the open-source OpenPDC [1]. OpenPDC takes measurements and sorts them by their time stamps. The measurements are archived in a database using their time stamps.

2.2 Security Gateway

PMUs and PDCs need to be shielded from the larger network. The security gateway provides a interface between the critical network components and the internet. Security gateways provide the network with a firewall [32]. In [3] the authors suggest firewalls should have three main properties: all traffic must enter, only trusted traffic may pass, and the firewall is immune to penetration. All traffic from the PMU to the PDC, or from PDC to PMU, needs to pass through the security gateway to

improve security. It generally uses a deny by default approach (also known as white-list) to filter traffic. If the component trying to connect to the PMU or PDC is not on the trusted list for the security gateway, then it is not allowed to pass. So, if the security gateway is configured and setup correctly, only traffic from the trusted list may pass. Although, this provides some security, data spoofing still remains a threat to the system.

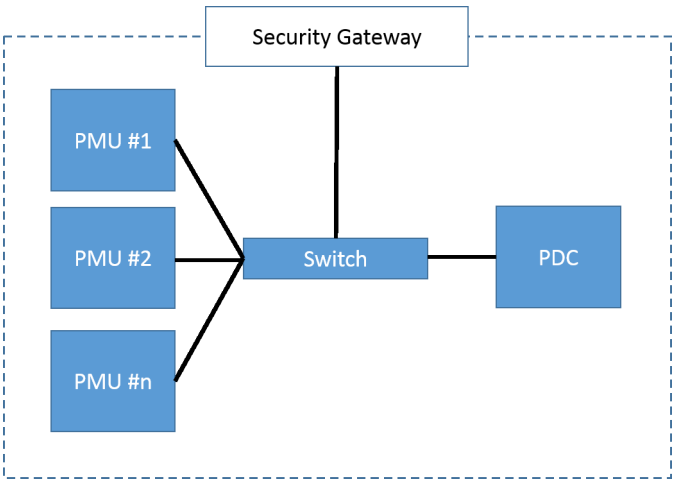

Figure 2.2: Security Gateway as a Firewall

Figure 2.2 shows the PMU and PDC being shielded from the wider network by the security gateway. It can be a local area network behind the security gateway.

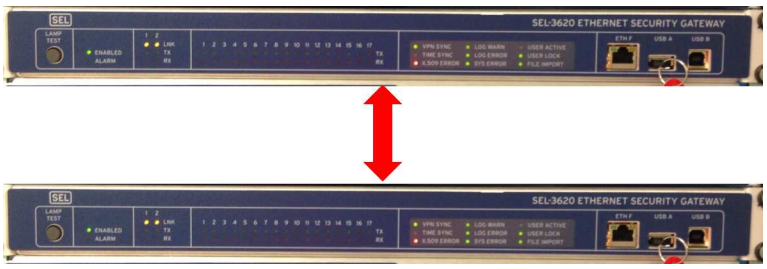

Figure 2.3: Security Gateway VPN

The other job of the security gateway within the network is to establish a VPN [32]. Establishing a VPN between substations allows measurement and configuration data to be sent securely between substations. The security gateway uses the IPsec protocol to establish VPN connections. IPsec uses Encapsulated Security Payload (ESP) and Authentication Header (AH) protocols to secure data [25]. Once the payload is encrypted, it is sent across the network. When it reaches the designated security gateway, the gateway will check to see if the packets were delayed or replayed and decipher the packet [25]. The measurements are then recorded in the PDCs' database.

2.3 Denial of Service

Denial of Service (DOS) attackers attempt to consume systems resources, such as bandwidth, to prevent users from accessing the system. One common type of DOS attack is an Internet Control Message Protocol (ICMP) Smurf attack. The attacker sends an ICMP echo packet with the victims IP address, all the hosts accept the ICMP echo packet and reply to the victim computer [37].

In a Distributed Denial of Service (DDOS) attack, the attacker takes control of multiple machines called bots. Bots can be used to perform malicious activities such as DDOS attacks. While DOS attacks on traditional IP networks are well studied, DOS attacks could also be performed on PMU networks. Researchers [21], tested DOS attacks such as network layer attacks, Internet Control Message Protocol (ICMP) attacks, transport layer attacks, Local Area Network Denial (LAND) attacks, and teardrop attacks on a PMU network. These attacks take advantage of weaknesses in network protocols. PMU networks dependence on real-time measurement data, makes them vulnerable to this attack. If a malicious person were to attack multiple

PMUs, all measurements from those PMUs would be dropped or delayed. This could cause inaccurate predictions about the status of the transmission system, delayed mitigation of power system problems, or total failure of measurement devices along the network.

2.4 Denial of Service Countermeasures

Though DOS attacks remain a serious threat to power grids that include PMUs, there are ways to prevent or mitigate the damage caused by an attacker. One possible solution to DOS attacks on PMU networks would be to use an "air gap". An air gap physically isolates the network. Air gapped networks have no physical connection to the larger internet. This isolation is costly.

Some common DOS countermeasures are large bandwidth connections to insure the network can handle the traffic. DOS traffic can also be mitigated using distributed or redundant infrastructure. Researchers [17] discuss existing DDOS countermeasures. Countermeasures include filtering routers, disabling IP broadcasts, applying security patches, disabling unused ports, and performing intrusion detection [17].

2.5 Physical Attacks

A PMU can be isolated from the network using physical attacks that damage hardware or infrastructure. This includes cutting a network connection between the PMU and PDC or sabotaging the PMU. Limiting access to critical infrastructure can mitigate this type of attack.

2.6 Man-in-the-Middle Attack

Man-in-the-Middle attacks are an (active) interception attack. Man-in-the-Middle attacks occur when an attacker poses as the other side of a legitimate protocol session to both the legitimate client and server. For example, if B and A communicate, the intruder I replaces the BA link with two links BI and IA. An example of this is shown in Figure 2.4.

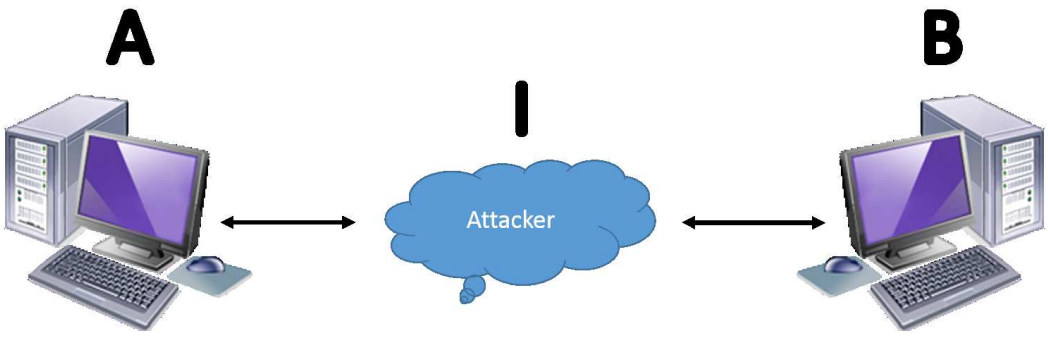

Figure 2.4: Example of a Man-in-the-Middle Attack

In a PMU network the Man-in-the-Middle attack occurs between the PMU and the PDC. The attacker disguises themselves as the PDC to the PMU and as the PMU to the PDC. Man-in-the-Middle attacks can use route table poisoning and compromised certificates. Researchers [6] discuss using false certificates to conduct a Man-in-the-Middle attack. The paper discusses the false certificate vulnerability for a HTTPS connection. But, this method could be used in any system that uses certificates to secure connections. If the PDC uses X.509 certificates for authentication then a man-in-the-middle attack between the PDC and the PMU would be possible. To prevent this type of attack clients need to authenticate the server they connect to [24].

2.7 Packet Analysis

Contents of the PMU TCP/IP packets are susceptible to packet analysis (sniffing). Programs such as Wireshark [11] allow attackers to look at traffic sent across the network. If encryption is not used, all information communicated can be seen by the attacker. In [32] researchers used Wireshark [11] to analyze the synchrophasor network. They found the packets were in clear text. This makes it possible for an attacker to get passwords and other information sent across the network.

To further evaluate the network, researchers [32] added a security gateway to the network. The packets are then sent through a virtual private network (VPN) tunnel. Since all of the packets are sent over a VPN, the traffic is encrypted. VPNs create a virtual network that connects two trusted sub-networks. The packets sent within the VPN are in a secure tunnel between clients. To secure communications, VPN tunnels commonly use the Secure Socket Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH) protocols. To insure a secure connection the parties on the network use X.509 certificates to authenticate users and then exchange symmetric keys. This process is supposed to provide the system with security, but may have implementation and design errors. Known attacks on SSL/TLS include [5]:

- DNS Cache Poisoning is where the attackers sends spoofed responses to the DNS server, instead of the user. This causes the DNS to retain faulty information and return wrong IP addresses when queried.

- ARP Poisoning is when the attacker broadcasts an ARP packet containing the desired IP and their MAC address. Computers then cache that IP for the attackers MAC address. All information sent to the desired IP will be routed through the attackers computer.

- Man-in-the-Middle Attacks occur when attackers make independent connections with victims and relays messages between them.

- TLS/SSL Certificate Attacks occur when attackers authenticate themselves on the network using compromised or faulty certificates.

VPNs are essential for securing traffic, but need to be carefully implemented and their security verified. These attacks have been shown to work on networks, research still needs to be conducted to see their impacts on PMU networks.

2.8 Malicious Code Injection

An example of a modification attack is malicious code injection. In malicious code injection, the attacker inserts new instructions into code to alter its execution. One common modification attack is Structured Query Language (SQL) injection. SQL is a standardized language for managing databases. Commonly SQL injection attacks occur when queries are generated using user input [5].

In PMU networks, the measurements are continuously sent across the network so that the power system can be measured in real-time. Since the data sent to the PDC is stored in a database, PMUs are particularly susceptible to SQL injection attacks [7]. Before measurements are sent, the PMU sends a configuration message to the PDC to specify the data table structure to be defined in the database [32]. The PDC does not authenticate the configuration message. Instead, it creates the new tables specified in the configuration message. This leaves the system vulnerable to code injection.

The SQL injection vulnerability most frequently comes when queries are formulated occur if user input is not properly validated before inclusion in an SQL

query [9]. The attacker can make the transmission system state appear to be the opposite of reality. For example, if there is an issue with a transmission bus or line, an attacker can modify measurements to indicate it is normal, which could put the power system at risk of an outage.

Researchers in [36], describe two insertion attacks: code-injection and return-oriented programming. In code-injection, the attacker directly inserts shell code (a set of malicious instructions) into the program. Return-oriented programming reuses binary code already present in the system as shell code. Shell code is the software exploit payload. Either attack can send malicious instructions to the database management system, to add, delete, or modify the database, or take control of the system.

2.9 Malicious Code Injection Countermeasures

Authors [10] show the security gateway using encryption and decryption to send packets across the internet. One security gateway encrypts measurement packets from the PMU. The other security gateway decrypts them before sending to the PDC. Since packets are encrypted before crossing the network, the attacker should be unable to decipher them. In modern operating systems, code injection is made difficult by randomizing the system address space, separating code and data, and monitoring the stack to detect buffer overflows [5]. The PMU and PDC should use operating systems that have these countermeasures.

To counteract SQL injection attacks: either check inputs for characters that can be abused, or use parameterized statements that force user inputs to follow a static template [8]. These templates only allow certain inputs to be translated into queries. For further prevention, databases should also have strict access controls for allowing users to modify or manipulate data [5]. In [8] authors also discuss using

static analysis and run-time monitoring, proxy filters, intrusion detection systems, and encapsulating database queries to provide safe and effective ways to access databases.

2.10 Data Spoofing

Data spoofing occurs when attackers falsify data. The PMUs continuously send data to the PDC. Instructions on how to set up database tables are included. If the PDC does not authenticate PMU connections, the PDC may accept fabricated data.

PMU data gives operators information so they can be aware of the condition of the electric grid. Data accuracy is important. Data spoofing gives the program forged data instead of actual data. This can be detrimental to grid stability and reliability. In [30] researchers inject false data into the system. This data can either be PMU measurements or time stamps. In [29] authors spoof GPS measurement time stamps. Altering measurement times can render measurements useless. For example, readings can be reordered to make capacity reduction seem to be capacity increase, etc.

2.11 Data Spoofing Countermeasures

Data spoofing has little effect when it is limited to a single data feed [18]. To mitigate data spoofing, the grid can use multiple PMUs to monitor the same transmission bus or line, which makes spoofing more complicated. The use of redundant measuring devices is suggested in [2], where the authors use redundant smart meters. The same idea is relevant to PMUs.

2.12 Summary

This Chapter detailed PMU networks. This includes PMU protocols, and the security gateway. Vulnerabilities common to PMU networks were discussed. The common vulnerabilities were DOS, physical attacks, man-in-the-middle, packet analysis, malicious code injection, and data spoofing.

Chapter 3

Traffic Analysis

PMUs and PDCs communicate over the network. To perform traffic analysis, attackers just need access to the connection. In this Chapter we present PMU traffic analysis tests. We begin by describing the laboratory setup. Then we show the network is vulnerable to DOS, man-in-the-middle, and packet analysis attacks. Finally, we summarize our results and give recommendations for fixing discovered vulnerabilities.

3.1 Experimental Setup

The laboratory used in this research contained a benchmark IEEE 68 bus (New England/New York) power system simulated using the Real-Time Digital Simulator (RTDS) [16]. The RTDS can simulate scenarios such as substation failures or disturbances that reflect conditions based on real world scenarios. All measurements produced by RTDS are collected by the PMU, and given time stamps [23].

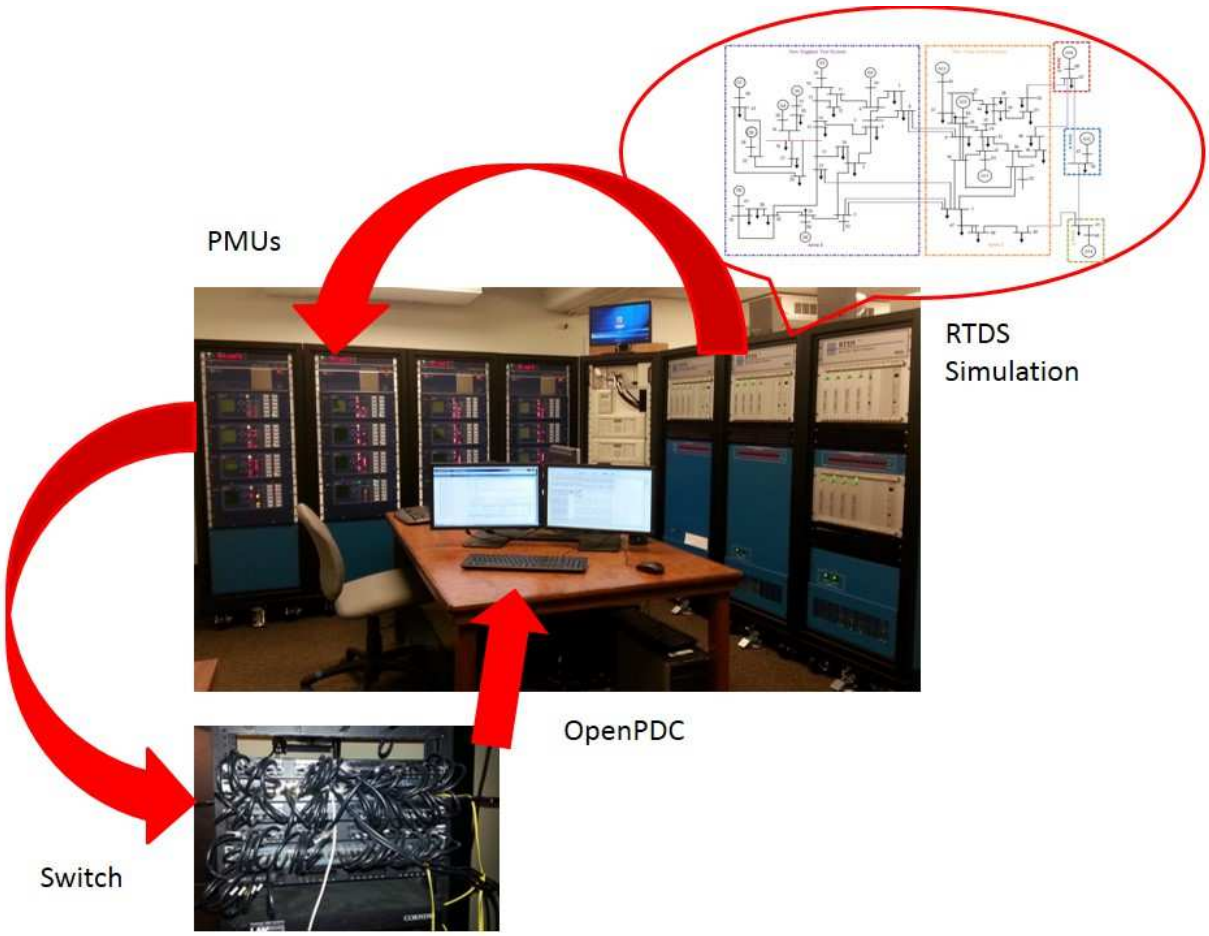

Figure 3.1: Laboratory Setup

Figure 3.1 shows the current laboratory setup. Each measurement is encapsulated in a data frame and sent through the network. The header includes the packet destination and source address. The switch reads the header and delivers the measurements to the PDC. The PDC could be located at a regional control center in the actual electric grid [18]. A super PDC could be located at independent system operators monitoring control center. The super PDC would collect data from all regional control centers. All measurements are stored in a database, such as a MySQL database, for further processing. The PDC runs open source openPDC software [1].

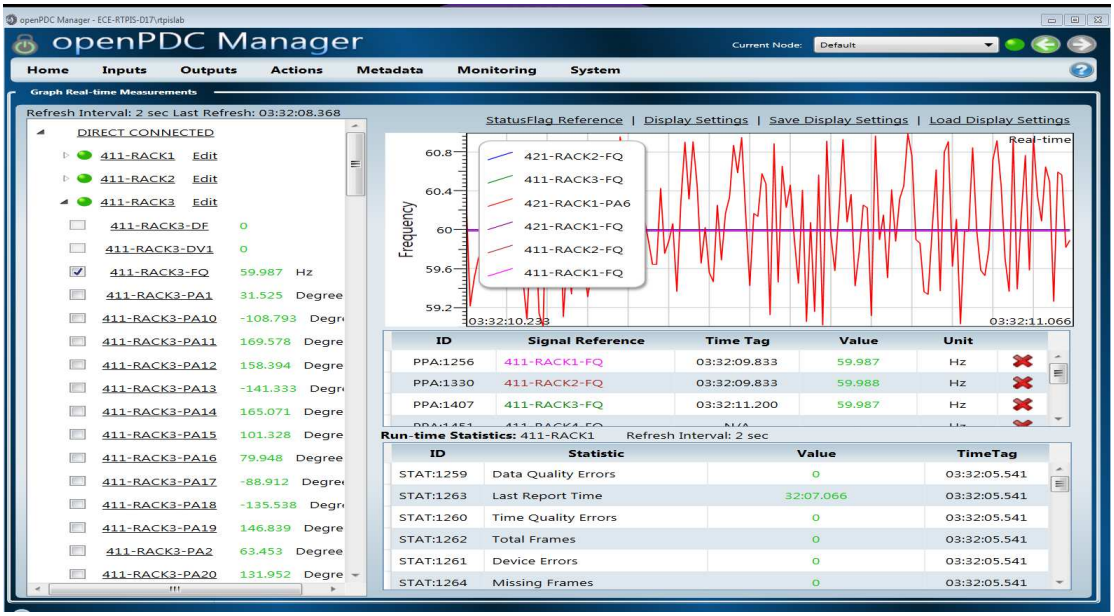

Figure 3.2: OpenPDC Interface

An example openPDC interface is in Figure 3.2. The openPDC software allows the controller to view all the packet information being sent from the PMUs. This would include data such as phasor measurements, PMU ID, and information whether the PMU is currently online.

3.2 Address Resolution Protocol (ARP) Poisoning

To analyze packets an Address Resolution Protocol (ARP) cache poisoning attack was used. Using Kali Linux [12], ARP packets associating the victim's IP and the Kali Linux computer's MAC address were broadcast. Local network machines then cache this information. This ensured that PMU network traffic would be routed through the attack computer. The attack computer can then forward them to the PDC. This enables packet analysis and man-in-the-middle attacks. All data sent from

the PMU to the PDC can easily be viewed and modified.

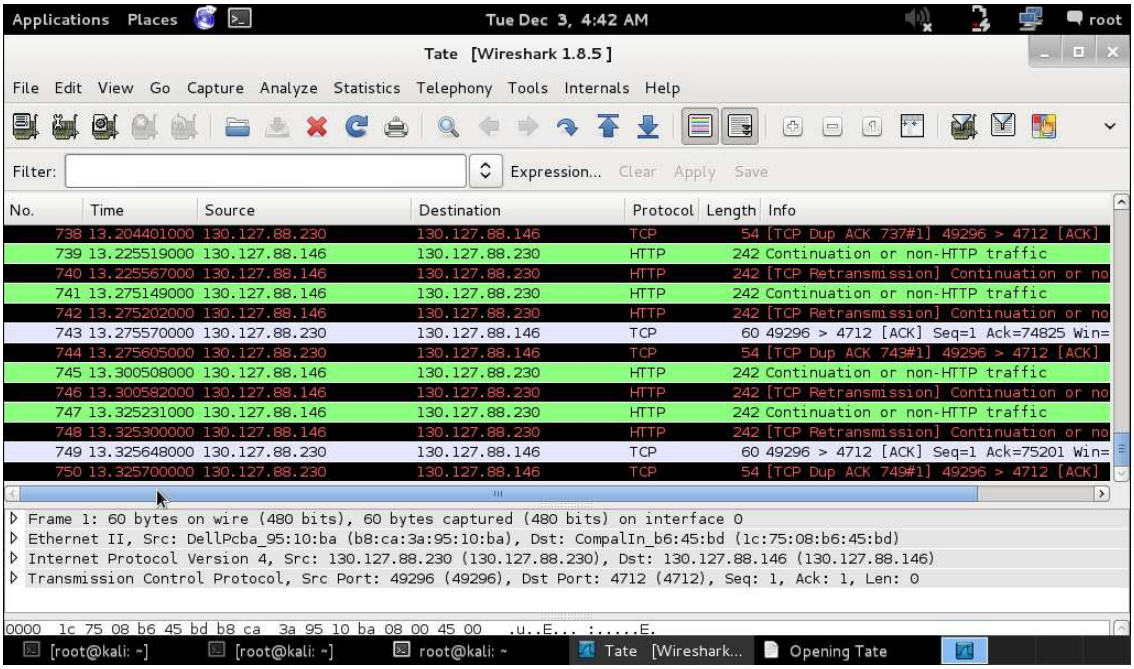

Figure 3.3: Wireshark Screen Capture

Figure 3.3 shows a Wireshark [11] capture of the network traffic. It shows data packets being sent from one PMU to the PDC. The figure shows the source IP address, the destination IP address, protocol, and data. Since the packets are sent across the network without the security gateway, all information is in clear text. This lets us view information such as passwords, measurement data, and configuration information.

Since the packets are routed through our computer we can perform a replay attack. By recording data and resubmitting it later. Man-in-the-middle attacks modify the measurements.

Rerouting traffic through an attack computer can also enable DOS attacks. If the PMU discards packets on the way to the PDC, it appears as if the PMU is offline.

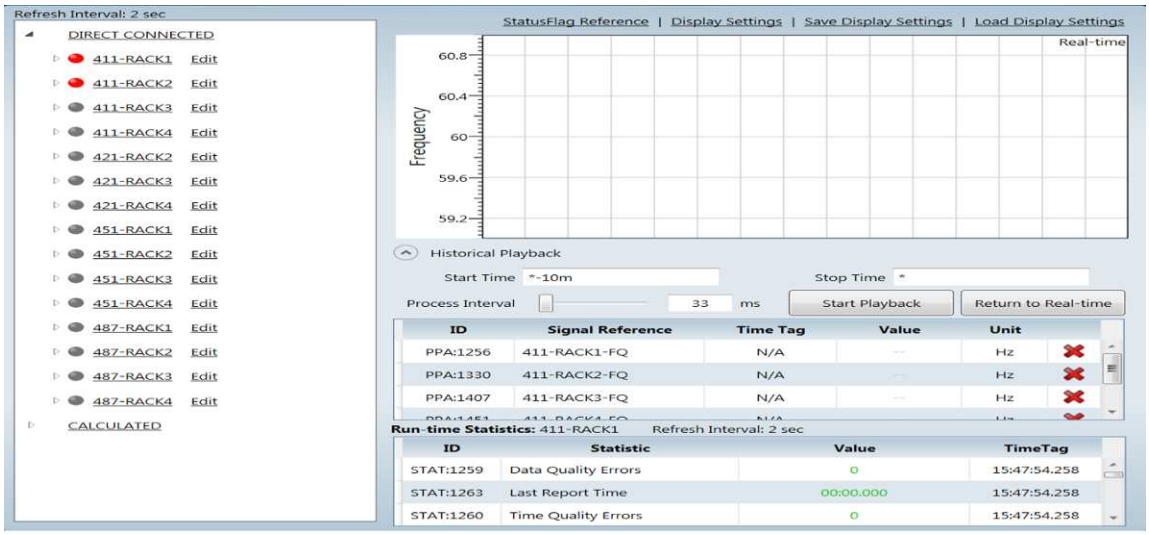

Figure 3.4: Denial of Service Attack

Figure 3.4 shows a DOS attack convincing the PDC that the PMUs are offline. Using this technique, it is possible to take PMUs offline using a simple script.

The PMUs have to be configured. To configure the PMU, the system administrator must enter passwords. After three incorrect password entry's, the system administrator is locked out for sixty seconds. An attacker can perform a DOS attack by repeatedly entering incorrect passwords to lock operators out of the system.

When configuring the PMUs, one available option is the Telnet network service. Telnet is a terminal based text-oriented communication protocol. Telnet sends messages in clear text. Each password allows different access to the PMU. For example, access level 1 allows viewing but not changing settings. Access level 2, gives full access over the system. Telnet allows the entire configuration session to be seen, including the passwords.

Figure 3.5 shows a Wireshark [11] capture screen shot of a PMU configuration

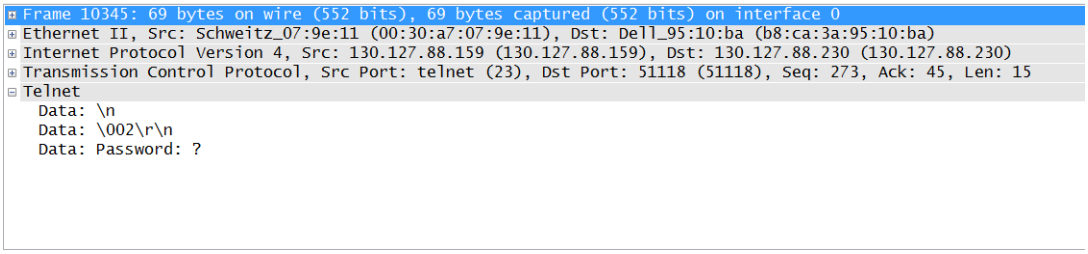

Figure 3.5: Prompting for Password over Telnet

over Telnet where the system is prompting the user for a password. Figures 3.6 - 3.9, show the packets containing the password information.

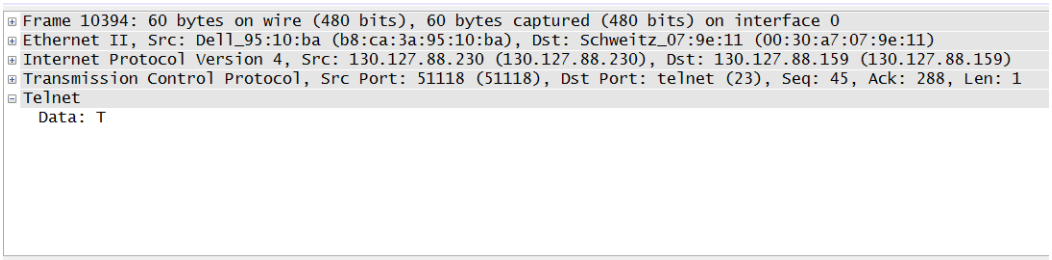

Figure 3.6: First Letter of the Password

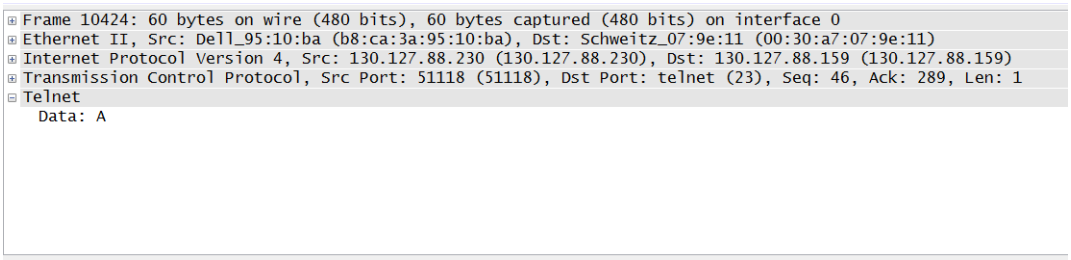

Figure 3.7: Second Letter of the Password

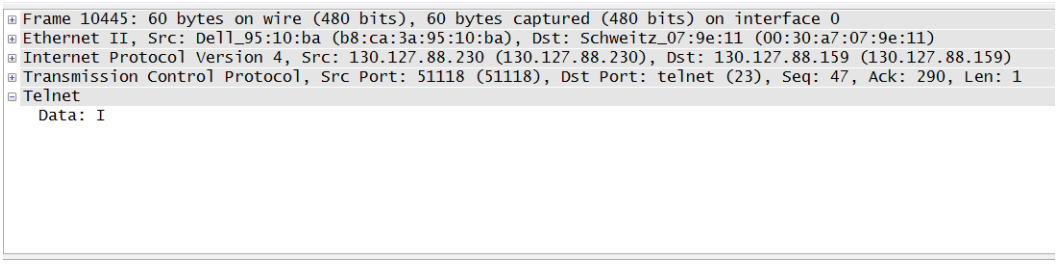

Figure 3.8: Third Letter of the Password

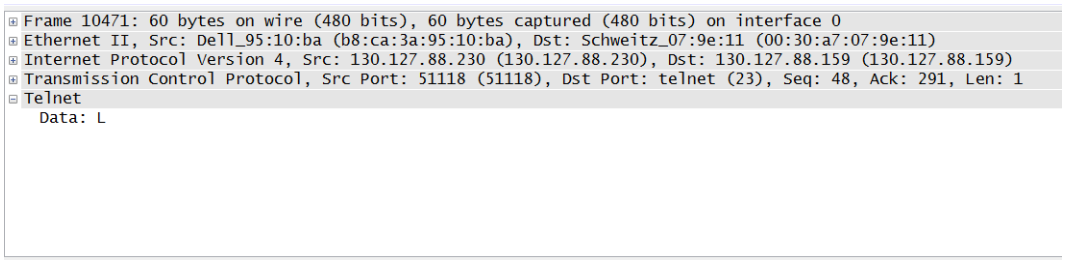

Figure 3.9: Final Letter of the Password

The data shows that the password is TAIL. This is the level 2 access password for the PMUs. Once I have level 2 access, I have full control over the PMU. This is problematic for the power industry. It is our recommendation when configuring the PMUs that the operators not be able to use Telnet.

3.3 Summary

This Chapter describes traffic analysis of a PMU network. Using an ARP poisoning attack, we found that several security vulnerabilities exist. These include packet analysis, DOS, and man-in-the-middle. These attacks were carried out on a local area network but, the same attack can be carried out over a wide area network, such as the Internet. Researchers [13] have found that due to a flaw in the design of the Border Gate Protocol (BGP), attackers can route packets through any path they choose. While building a separate network infrastructure is costly, it removes this vulnerability.

While the system allows the user to change the default access level passwords, it is not required. It is recommended that the system administrator be forced to change the default passwords. This would help prevent attackers from gaining access.

Chapter 4

Side Channel Analysis

In Chapter 3, we discussed the vulnerabilities associated with PMUs sending measurements through the network in clear text. To send encrypted data, PMU networks can use security gateways. While encrypting data via a VPN hardens security, further investigation of remaining vulnerabilities needs to be conducted. In this Chapter, we detail a side channel analysis of VPN traffic through the security gateways. The results of this attack are then summarized.

4.1 Detection of PMUs across the VPN

Side channel attacks take advantage of information leaked by the physical implementation of the cryptosystem. We use timing patterns. Although, information is encrypted, the timing pattern remains. Removing timing patterns requires significant performance impact.

4.1.1 Hidden Markov Models

Hidden Markov Models (HMM) model stochastic processes that are difficult to observe. Unlike the standard HMM [26] that uses two sets of random processes: states and outputs, our model uses a single set of random processes: the state transitions. This model is equivalent to classical models [26].

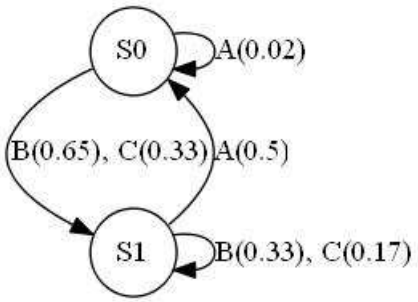

Figure 4.1: HMM with States and Transitions

Figure 4.1 shows an example HMM with two states and 6 transitions. Each state has outgoing transitions. Each transition has a transition probability. The sum of the outgoing transition probabilities for any state has to equal 1.

Traditionally the Baum-Welch algorithm is used to infer the state transition matrix and symbol output possibilities [26]. In [28] HMMS are inferred using the Causal State Splitting and Reconstruction (CSSR) algorithm. The CSSR algorithm is dependent on input data in the form of sequences of characters with length L. The history sequence L has to be sufficient in length to indicate the state. All sequences with length less than or equal to L are merged into alike states.

In [27] the HMM is derived without a priori information. Our approach follows the HMM inference in [19]. The HMM is inferred using an initial L. Then the training data is traced through the model. The L is increased until the structure of the HMM remains constant. When the structure stabilizes, no additional information can be gained from increasing L [27].

4.1.2 Hidden Markov Model Generation

HMMs can be generated directly from timing data [5]. This application uses inter-packet delays of data sent between security gateways. The inter-packet delays provide information of the underlying processes [33]. To find the inter-packet delays, we observe the packets using Wireshark [11]. Wireshark directly displays inter-packet delays. As mentioned in Chapter 2, the HMM is a stochastic process. The inter-packet delays need to be converted from analog to digital symbolized data, to generate the HMM. To convert the inter-packet delays into symbols, we make a histogram.

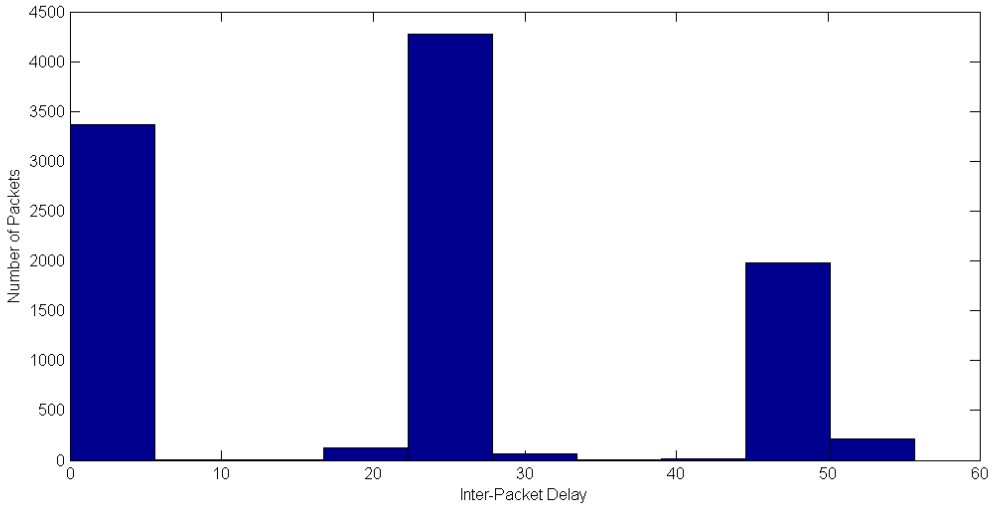

Figure 4.2: Histogram of inter-Packet Delays

Figure 4.2 shows a histogram of the the number of packets versus the inter-packet delays (in milliseconds) of one PMU being sent across the VPN by the security gateways. Each inter-packet delay was multiplied by a scaling factor to make them easier to read. The histogram contains approximately 10,000 packets. Using this graph, the packets can be grouped into 3 distinct symbols.

Table 4.1 shows the translation between the symbol and the associated inter-

Table 4.1: HMM Symbols from inter-packet Delay

Symbol	Delay Time (Milliseconds)
A	0-20
B	20-40
C	40-60

packet delay. After symbolizing the inter-packet delay the HMM is built using the HMM inference algorithm [27] [28]. Figure 4.3 is an HMM of the data.

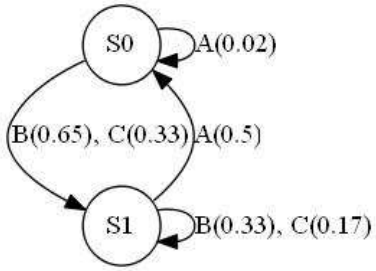

Figure 4.3: HMM of the inter-packet Delays Inside VPN

4.1.3 Experimental Results

After inferring the model of measurement traffic through the VPN, we detect whether the model can distinguish measurement traffic from random traffic. There were 10,000 packets of measurement traffic and 3,000 packets of random traffic. They were broken down into sequences of 24 symbols each. If the measurement traffic was identified correctly, it was defined as a true positive. If the random traffic was identified as a measurement packet, it was defined as a false positive. A ROC detection curve was then drown using the confidence interval approach. Figure 4.4 shows the ROC curve.

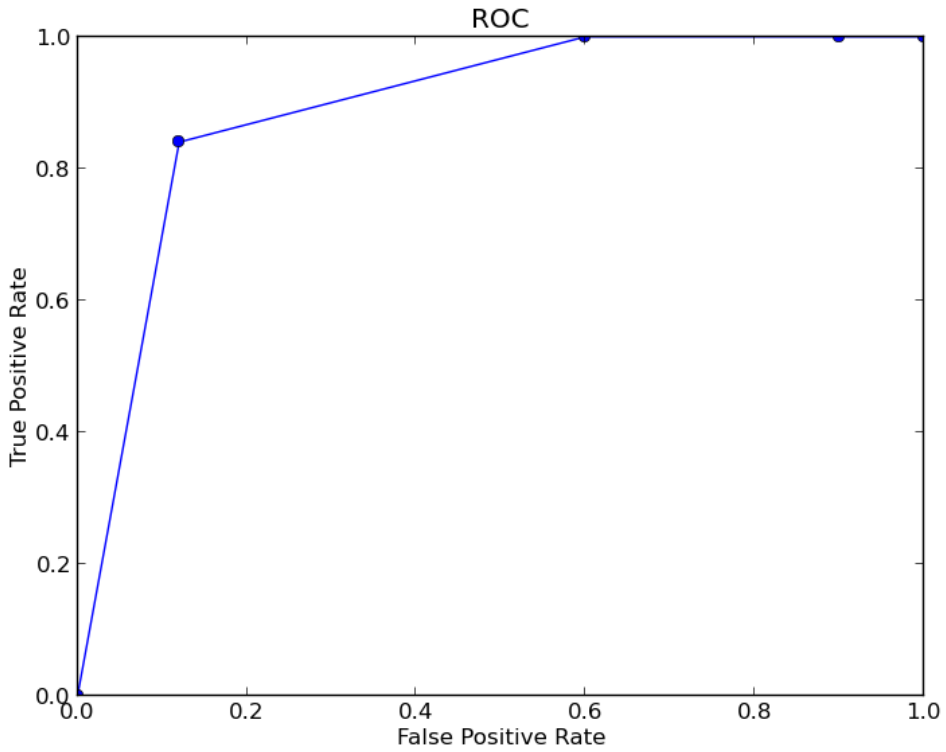

Figure 4.4: ROC of Detection

Figure 4.4 shows the true positive versus false positive rate of detecting the measurement data sent from one PMU through the VPN. The results give a 84'%' true positive versus 12'%' false positive rate. Thus, we can positively identify the measurement traffic sent from one PMU through the VPN.

4.2 Summary

While using security gateways to send measurements packets through VPN's can be used to encrypt network traffic, the system still remains vulnerable to side channel analysis. In this Chapter we discussed using the inter-packet delays between

packets across the VPN to detect measurement data. Once the inter-packet delays have been collected using a packet analysis tool, a hidden Markov model can detect measurement packets. Once, these packets are identified, an attacker can reroute and drop packets. This attack could be detrimental in monitoring the condition of the power grid. One possible solution to this problem, would be to build a separate infrastructure for communicating data.

Chapter 5

Conclusion

5.1 Summary

With the addition of PMUs to the existing electrical power grid, information exchange about the power grid has become possible. This allows for efficient, reliable, and cost effective power generation. However, the added networking brings further security concerns. The lab is modeled after the IEEE 68 bus (New England/New York) power system. It has been shown that packet analysis, man-in-the-middle, and DOS attacks are possible using ARP poisoning. Additionally, it has be shown that packets sent across the VPN are susceptible to side channel analysis.

In Chapter 1, gives an introduction on why security research on PMUs is important. Due to the limited amount of research on PMU networks, further research needs to be conducted to provide overall security. This was the motivation behind the work.

Chapter 2, provides the background behind the PMU network, protocols used, the security gateway, researched attacks and countermeasures. This Chapter provides a basis of knowledge of the general overview of a PMU network and its functionality.

In Chapters 3 and 4 security vulnerabilities for the PMU network are discussed. In Chapter 3 ARP poisoning was used to reroute traffic through a attack computer. This exposed DOS, man-in-the-middle, and packet analysis security vulnerabilities. Chapter 3 also provided security recommendations. Chapter 4 details using side channel analysis to determine measurement data across a VPN. Using HMMs the traffic could be identified. As discussed, this leaves the system susceptible to DOS attacks.

In this paper documented attacks and traffic and side channel analysis are discussed. The hope is by addressing security vulnerabilities to industry and academia, vulnerabilities can be corrected. Although, this thesis has addressed some security concerns, further research is needed expose potential security vulnerabilities. A future security verification agenda is proposed.

5.2 Security Recommendations

In Chapter 3, we discussed vulnerabilities such as DOS due to incorrect passwords, default passwords being used to access the PMU and configuration data and passwords being sent in clear text. Using a security gateway to send traffic through a VPN would encrypt data.

When configuring the PMU, the system shouldn't allow the Telnet protocol. This would prevent passwords from being sent in clear text. The PMU should also require the system administrators to change the default passwords. This would help prevent attackers from gaining access to the passwords.

5.3 Future Work

Although, some vulnerabilities have been exposed, further testing could identify others. We propose a security verification agenda. This section details the future agenda. The security agenda is broken down into 6 parts: penetration testing, protocol inference and analysis, security performance verification, further side channel analysis, game theory analysis, and hardening. When performing these tests, the NERC : (CIP) Critical Infrastructure Protection needs to addressed.

5.3.1 Penetration Testing

For penetration testing, the Common Vulnerabilities and Exposures (CVE), fuzzing, buffer overflow and SSL/TLS vulnerabilities need to be tested. The CVE database discloses known security flaws. This database may hold vulnerabilities related to PMUs. The network needs fuzzing tests. Fuzzing attacks consist of inserting random data into the inputs of a program to expose security vulnerabilities. Since the security gateway uses X.509 certificates, protocol vulnerabilities need to be checked.

5.3.2 Protocol Inference and Analysis

Since the protocol can easily be viewed if messages are in clear text, protocol inference is simple. But, when VPNs are used, side channel analysis can be used. If traffic is in clear text or protocol vulnerabilities can be used to authenticate on the network, than data leakage becomes problematic. Leaked data could be passwords or measurements. If the attacker is able to obtain the password, than the PMU can be taken over.

As shown in this thesis, DOS attacks are an issue. Different protocols can be vulnerable to DOS attacks. DOS attacks need to be addressed so they can be

fixed. DDOS attacks can be carried out against the network. DDOS testing can be performed using tools such as Stacheldraht [15] and Low Orbit Ion Cannon (LOIC) [14]. Each of these tools are free and easily accessible.

5.3.3 Security Performance Verification

While the security of the PMU network is crucial, the power grid also has to provide reliable, efficient, and consistent electricity to millions of people. The performance of the network needs to be evaluated along with the security protocol. To test the performance versus security logical verification, petri-net analysis, and performance sensitivity need to be analyzed.

5.3.4 Side Channel Analysis

This paper detailed side channel analysis in Chapter 4. Further side channel analysis can be used to determine other characteristics about the network. Different parts of the physical implementation of the cryptosystem can be analyzed to find vulnerabilities.

5.3.5 Game Theory

The PMU network can be put into a game theory model. Game theory is the study of strategic decision making. Putting the network into a game theory model would allow for evaluation of security flaws. Depending on the results, decision and control framework could be established.

5.3.6 Hardening

Hardening, when referring to network security, refers to reducing system vulnerability. The security gateway is one device that can be used to harden the network. Along with establishing a VPN, the security gateway is supposed to close unused network ports. To validate this claim, a simple port scanning technique can be tested.

Appendices

Appendix A Curriculum Vitae

Christopher Tate Beasley

Phone: 828-735-0966

Email: beasle6@g.clemson.edu

15 Riggs Hall, Clemson University

Clemson, SC 29634

Expertise: Network and Computer Security, Computer Systems Architecture, Synchrophasor Security

ACADEMIC

M.S. Computer Engineering May 2014
Clemson University, Clemson, SC GPA: 3.57/4.00

B.S. Electrical Engineering May 2012
Western Carolina University, NC GPA: 3.6/4.00

CAREER HISTORY

Clemson University, ECE Department Clemson, SC 08/12 to Present
Research Assistant

- Conducting research under Dr. Richard R. Brooks in computer and network security.
- Projects include Semantic Similarity Detection in Natural Language Documents and Electric Power Synchrophasor Network Cyber Security Vulnerabilities.

Schneider Electric 05/12 to 08/13
Manufacturing Engineering Intern

- Worked on improving process flow and productivity of industrial operations within Schneider's facility.
- Performed and set up data transfer between servers.

Consolidated Metco 05/10 to 08/10
Electrical Engineer Intern

- Improved skills and knowledge of working in the manufacturing industry as an electrical engineer.
- Shadowed various electrical engineers within the facility.

RESEARCH EXPERIENCE

Electric Power Synchrophasor Network Cyber Security Vulnerabilities Clemson, SC 08/13 to Present
Clemson University, Dr. Richard R. Brooks and Dr. G. Kumar Venayagamoorthy

- Performed a literature review of documented attacks.
- Performed vulnerability testing on a PMU network modeled after the IEEE 68 (New England/New York) bus system.
- Provided a security verification plan for future testing.

Semantic Similarity Detection in Natural Language Documents Clemson, SC 08/12 to 12/12
Clemson University, Dr. Richard R. Brooks

- Worked on software that uses hidden Markov models to detect documents that have similar semantic information to documents used as a training set.

PUBLICATIONS AND PRESENTATIONS

- Beasley, Christopher. Venayagamoorthy, G. Kumar. and Brooks, Richard. (In Press). Power Systems Conference on Advanced Metering, Protection, Control, Communication, and Distributed Resources. "Cyber Security Evaluation of Synchrophasors in a Power System."

Bibliography

[1] David Anderson, Chuanlin Zhao, Carl H Hauser, Vaithianathan Venkatasubramanian, David E Bakken, and Anjan Bose. Intelligent design" real-time simulation for smart grid control and communications design. *Power and Energy Magazine, IEEE*, 10(1):49–57, 2012.

[2] Todd Baumeister. Literature review on smart grid cyber security. *University of Hawaii at Manoa, Tech. Rep*, 2010.

[3] Steven M Bellovin and William R Cheswick. Network firewalls. *Communications Magazine, IEEE*, 32(9):50–57, 1994.

[4] Wayne F Boyer and Scott A McBride. Study of security attributes of smart grid systems–current cyber security issues. *Idaho National Laboratory, USDOE, Under Contract DE-AC07-05ID14517*, 2009.

[5] Richard Brooks. *Introduction to Computer and Network Security Navigating Shades of Gray*, volume 1. Taylor and Francis Group, LLC, 6000 Broken Sound Parkway, NW Suite 300,Boca Raton, FL, 33487.

[6] Franco Callegati, Walter Cerroni, and Marco Ramilli. Man-in-the-middle attack to the https protocol. *IEEE Security and Privacy*, 7(1):78–81, 2009.

[7] Salvatore D'Antonio, Luigi Coppolino, Ivano Alessandro Elia, and Valerio Formicola. Security issues of a phasor data concentrator for smart grid infrastructure. In *Proceedings of the 13th European Workshop on Dependable Computing*, pages 3–8. ACM, 2011.

[8] WG Halfond, Jeremy Viegas, and Alessandro Orso. A classification of sql-injection attacks and countermeasures. In *Proceedings of the IEEE International Symposium on Secure Software Engineering, Arlington, VA, USA*, pages 13–15, 2006.

[9] William GJ Halfond and Alessandro Orso. Amnesia: analysis and monitoring for neutralizing sql-injection attacks. In *Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering*, pages 174–183. ACM, 2005.

[10] Wei Hu, Jason Hiser, Dan Williams, Adrian Filipi, Jack W Davidson, David Evans, John C Knight, Anh Nguyen-Tuong, and Jonathan Rowanhill. Secure and practical defense against code-injection attacks using software dynamic translation. In *Proceedings of the 2nd international conference on Virtual execution environments*, pages 2–12. ACM, 2006.

[11] internet. `http://www.wireshark.org/`. Accessed: 2013-12-15.

[12] internet. `http://www.kali.org/`. Accessed: 2013-12-15.

[13] internet. `http://www.wired.com/threatlevel/2013/12/bgp-hijacking-belarus-iceland/`. Accessed: 2013-12-15.

[14] internet. Low orbit ion cannon (loic). `http://sourceforge.net/projects/loic/`. Accessed: 2013-12-15.

[15] internet. Stacheldrahtv4. `http://packetstormsecurity.org/distributed/stachel.tgz`. Accessed: 2013-12-15.

[16] R Kuffel, J Giesbrecht, T Maguire, RP Wierckx, and P McLaren. Rtds a fully digital power system simulator operating in real time. In *WESCANEX 95. Communications, Power, and Computing. Conference Proceedings., IEEE*, volume 2, pages 300–305. IEEE, 1995.

[17] Felix Lau, Stuart H Rubin, Michael H Smith, and Ljiljana Trajkovic. Distributed denial of service attacks. In *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, volume 3, pages 2275–2280. IEEE, 2000.

[18] Hua Lin, Santhosh Sambamoorthy, Sandeep Shukla, James Thorp, and Lamine Mili. A study of communication and power system infrastructure interdependence on pmu-based wide area monitoring and protection. In *Power and Energy Society General Meeting, 2012 IEEE*, pages 1–7. IEEE, 2012.

[19] Chen Lu and Richard Brooks. Botnet traffic detection using hidden markov models. In *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, page 31. ACM, 2011.

[20] KE Martin, D Hamai, MG Adamiak, S Anderson, M Begovic, G Benmouyal, G Brunello, J Burger, JY Cai, B Dickerson, et al. Exploring the ieee standard c37. 118–2005 synchrophasors for power systems. *Power Delivery, IEEE Transactions on*, 23(4):1805–1811, 2008.

[21] T Morris, S Pan, J Lewis, J Moorhead, B Reaves, N Younan, R King, M Freund, and V Madani. Cybersecurity testing of substation phasor measurement units and phasor data concentrators. In *The 7th Annual ACM Cyber Security and Information Intelligence Research Workshop (CSIIRW)*, 2011.

[22] Siddhartha Muthyala. Communication security for smart grid distribution networks. 2013.

[23] Krish Narendra and Tony Weekes. Phasor measurement unit (pmu) communication experience in a utility environment. In *2008 Cigre Canada Conference-Technology and Innovation for the Canadian Power Grids of the Future (Winnipeg, Manitoba, Canada) XI. BIOGRAPHIES*, 2008.

[24] Rolf Oppliger, Ralf Hauser, and P David BASIN. Ssl/tls session-aware user authentication. *Computer*, 41(3):59–65, 2008.

[25] J Arturo Pérez, Victor Zarate, Angel Montes, and Carlos Garcia. Quality of service analysis of ipsec vpns for voice and video traffic. In *Telecommunications, 2006. AICT-ICIW'06. International Conference on Internet and Web Applications and Services/Advanced International Conference on*, pages 43–43. IEEE, 2006.

[26] Lawrence Rabiner. A tutorial on hidden markov models and selected applications in speech recognition. *Proceedings of the IEEE*, 77(2):257–286, 1989.

[27] Jason M Schwier, Richard R Brooks, Christopher Griffin, and S Bukkapatnam. Zero knowledge hidden markov model inference. *Pattern Recognition Letters*, 30(14):1273–1280, 2009.

[28] Cosma Rohilla Shalizi and James P Crutchfield. Computational mechanics: Pattern and prediction, structure and simplicity. *Journal of statistical physics*, 104(3-4):817–879, 2001.

[29] Daniel P Shepard, Todd E Humphreys, and Aaron A Fansler. Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3):146–153, 2012.

[30] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, 2012.

[31] William Stallings. *Network and internetwork security: principles and practice*. Prentice-Hall, Inc., 1995.

[32] John Stewart, Thomas Maufer, Rhett Smith, Chris Anderson, and Eren Ersonmez. Synchrophasor security practices. *Schweitzer Engineering Laboratories, Pullman, Washington (¡ www. selinc. com/WorkArea/DownloadAsset. aspx*, 2010.

[33] Mihaljev Tamara, Lucilla de Arcangelis, and Hans J. Herrmann. Inner-arrival times of message propagation on directed networks. 2012.

[34] Ganesh Kumar Venayagamoorthy. Dynamic, stochastic, computational, and scalable technologies for smart grids. *Computational Intelligence Magazine, IEEE*, 6(3):22–35, 2011.

[35] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on cyber security for smart grid communications. *Communications Surveys & Tutorials, IEEE*, 14(4):998–1010, 2012.

[36] Liwei Yuan, Weichao Xing, Haibo Chen, and Binyu Zang. Security breaches as pmu deviation: detecting and identifying security attacks using performance counters. In *Proceedings of the Second Asia-Pacific Workshop on Systems*, page 6. ACM, 2011.

[37] S Zargar, James Joshi, and David Tipper. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. 2013.