2008

Web-based relay management with biometric authentication

Brian Graeber
West Virginia University

Web-Based Relay Management with Biometric Authentication

By

Brian Graeber

Thesis submitted to the
College of Engineering and Mineral Resources

at West Virginia University
in partial fulfillment of the requirements
for the degree of

Master of Science
In
Electrical Engineering

Arun Ross, Ph. D
Roy Nutter, Ph. D.
Muhammad Choudhry, Ph. D. Chair

Lane Department of Computer Science and Electrical Engineering

Morgantown, West Virginia
2008

Keywords: Cyber Security, Biometrics, Protective Relay, Power System, Cyber Security

Abstract

Web-Based Relay Management with Biometric Authentication

Brian E. Graeber

This thesis proposes a web-based system for managing digital relay settings. These relays are deployed in the power system to protect sensitive and expensive equipment from physical damage during system faults and overload conditions. Providing this capability exposes these devices to the same cyber security threats that corporations have faced for many years.

This thesis investigates the risks and requirements for deploying the proposed system. A breakdown in the protection that these relays provide would cause power outages. The cost of outages can be significant. Therefore cyber security is critical in the system design. Cyber security requirements for the power industry identify access control as an important aspect for the protection of its infrastructure. If properly implemented, biometrics can be used to strengthen access control to computer systems.

The web-based relay management system uses fingerprint authentication along with a username and password to provide access control. Website users are given access to functionality based on user roles. Only high level users may attempt relay setting modification. The relay management system interacts with a database that stores the current relay settings, relay setting restrictions, and a queue of relay updates. A process is implemented to verify attempted setting changes against these setting restrictions. This provides an extra security layer if users attempt harmful changes to protection schemes. Valid setting changes are added to the queue and a separate relay update program communicates these changes to the relay. The database and relay update program protect the relays from direct modification. These features combined with biometric authentication provide a strong layered scheme for protecting relays, while supplying an easy to use interface for remotely using their capabilities.

Acknowledgements

I would like to thank Dr. Muhammad Choudhry for his patience and support throughout my long journey through graduate school. I would also like to thank Dr. Ross and Dr. Nutter the information they gave me to help my research. Another thanks goes Mike Spencer for his hard work in preparing the power simulator for demonstrating the results of this thesis. Last but not least, I would like to thank all of my family and close friends that have stuck by me during the past few years. Without their help, I would not have had the strength to complete this work.

Table of Contents

List of Figures

List of Tables

Chapter 1
Introduction

Cyber security is a growing concern for companies and individuals alike. Consumers alone spent an estimated $4.4 billion in 2007 purchasing just antivirus software [1]. Corporations have an even higher cost of protection. Still each year businesses, individuals, and government rely more on the Internet to interact. Today people trade stocks, manage bank accounts, pay bills, purchase goods, and even submit their taxes online. These systems must be designed to protect these transactions and their users from cyber attack.

The power industry is not immune to cyber attack. The structure of the power system is evolving to a more connected network. A network of Supervisory Control and Data Acquisition (SCADA) devices operates to keep the nations grid running reliably. Yet, with a combination of problems this network can lose control and result in expensive blackouts like the Northeast Blackout of 2003. With global terrorism on the rise, the agencies governing the North American grid have recognized the cyber threats posed to a vulnerable electric grid. These agencies created requirement designed to help utilities identify and protect critical systems.

The outlook of the grid is also changing. Technology advances in distributed generation promise new localized grid systems where more data and functionality is accessed remotely. A key security issue with protecting data is access control. This thesis introduces an advanced access control application to remotely modify relay settings. These setting protect a variety of devices that are critical to the operation of the power system.

Chapter 2
Literature Review

2.1 Introduction

This section introduces the costs that cyber attacks have created for businesses that use the Internet. The power system is not immune to these risks. It is possible that breakdowns in utility cyber security could cause blackouts. The changes in utility business practices and technological advancement in the power system are described and linked to increased cyber vulnerabilities for the power industry. The agencies responsible for the development and regulation of the power system are identified along with the roles they have in protecting it against cyber threats. This thesis proposes a system for remotely controlling devices responsible for protecting power system components. Biometric authentication is discussed as a solution to access control for the system.

2.2 Cyber Security Threats

With the global acceptance of the Internet, cyber attacks have become a serious threat to any system that is connected to it. US corporations spend an estimated $37 billion a year on IT security [2]. This money is used for security software, intrusion detection systems, virus scanners, firewalls, and employee training and awareness programs. From 2006 to 2007, the average loss per company resulting from cyber attacks fell from $345 thousand to $289 thousand [3]. But, total estimates for losses due to cyber attacks in the US are still at least $100 billion per year (2004 estimate) [2].

Since the Internet has been commercialized, there have been many costly assaults to systems that utilize it. Viruses are the most commonly publicized attacks. Famous viruses such as Melissa, Code Red, and Slammer have collectively caused billions of dollars in losses across the world [4]. The most significant viruses have corporate loss estimates exceeding a billion dollars [2]. These viruses feed on users with inadequate cyber security protection. At their worst, viruses can render systems inoperable or their data and functionality compromised. Table 2.1 is a listing of estimate losses for ten of the more prolific viruses in history.

Table 2.1 Estimated Costs of Virus Attacks [2].

(billions of dollars)

Attack	Year	Mi2g	CEI
SoBig	2003	30.91	1.10
Slammer	2003	1.05	1.25
Klez	2002	14.89	0.75
BadTrans	2002	0.68	0.40
Nimda	2001	2.62	2.75
Code Red	2001	2.62	2.75
Sir Cam	2001	2.27	1.25
Love Bug	2000	8.75	8.75
Melissa	1999	1.11	1.10

Mi2G and CEI (Computer Economics Incorporated) are two different organizations that perform analysis of virus cost. The numbers given are estimates and can be considered as a range of cost.

Viruses are not the only attacks that pose a cyber security threat. Variations of denial of service (DOS), distributed denial of service (DDOS) attacks, hacking, and software exploits all pose serious risks to Internet-connected systems [5]. DOS and DDOS attacks attempt to render a system useless by flooding it with invalid requests or messages. These messages can consume network, processor, or other system resources to the point where they cannot respond to valid traffic [6]. Standard DOS attacks use one host to launch an attack, but the more complicated DDOS attacks spread to multiple hosts and launch a more powerful strike. A DDOS attack named MafiaBoy was used against several large websites in 2000 and caused an estimated $1.7 billion in lost revenue [5].

Hacking is defined as gaining authorized access to computer systems. This often involves stealing information for profit. From 2003 to 2008 more than 41 million credit and debit card number were stolen from US banks. These stolen numbers resulted in losses or hundreds of millions dollars for banks and individuals. [7] There are also many cases where US government agencies were hacked including NASA, ARMY, NAVY, and Air Force. [8] Also, there are two instances where nuclear facilities were hacked. One instance was performed in Chicago in 2002 by an 18-year old [9]. The other instance was part of a planned test which ended up with control of a key system [10]. Hacking is a large problem that must be addressed when designing and administrating any computer system. A well designed access control system can significantly reduce the success rates for these attacks.

2.3 Power System Cyber Security

The power system underpins the social and economic infrastructure of the United States. A reliable source of electricity provides the basis for the way Americans work and live. The power system relies on its vast transmission network to provide redundancy, transfer power, and increase reliability. The entire nation is connected to this network or “grid” [5]. Like the Internet, this connectivity allows everyone to share resources, but also allows problems to propagate quickly to other areas. For example, the Northeast blackout of 2003 caused an outage that spread to affect 50 million people two days. The events that caused this blackout were a result of improper right of way maintenance, alarm system failure, poor human communication, and high system load [11].

Computers are used throughout the power industry for relay protection, SCADA/EMS (Energy Management System), power plant control, business operations, and everyday administrative purposes. As technology has advanced, these systems have changed from separate entities to a more integrated system. This integration opens up communications pathways between business related networks and power system control networks [12]. Business networks are likely connected to the Internet, thereby creating a potential link from the cyber security threats that exist there to critical power system networks. Figure 2.1 below depicts a simplified view of the power system depicting the connection of business system to control centers.

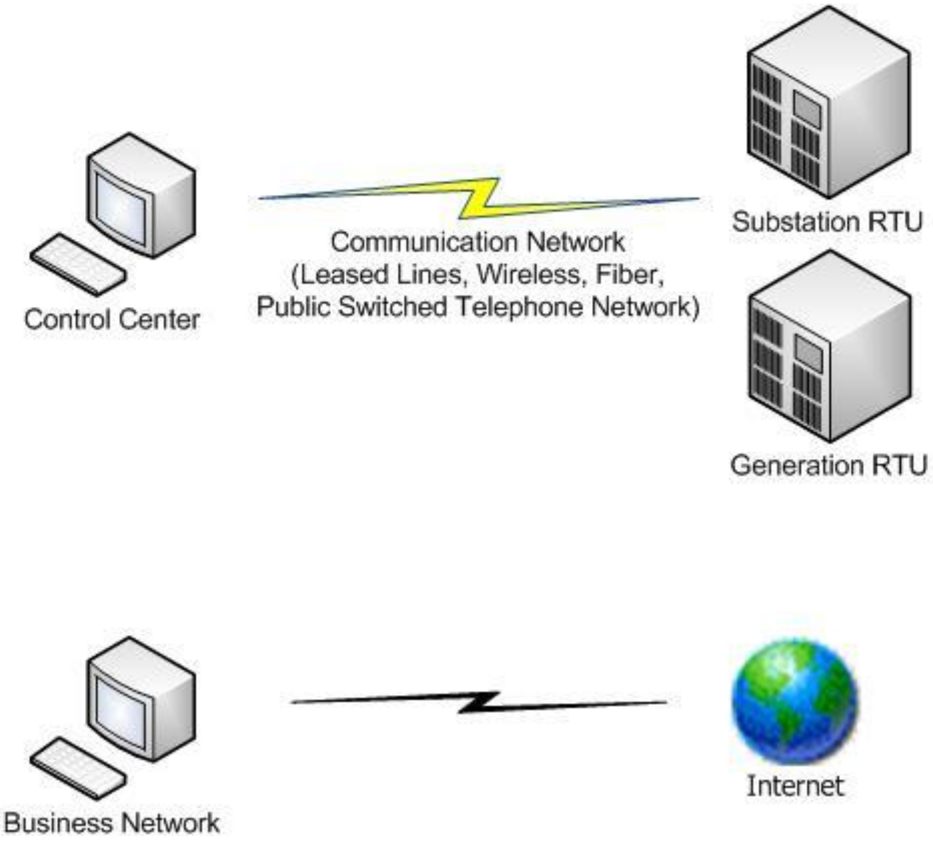


Figure 2.1: Power System and Utility Business Networks [13].

Control centers are the main communication hub for power systems and are also responsible for its safe operation. The Remote Terminal Units (RTU's) are the data collection and communication centers for generation, distribution, and transmission systems. These devices communicate operational information back to the control center via the indicated the communication network. New connectivity now exists between control centers and business networks, creating vulnerability to cyber attacks.

This security risk has created potential problems for the devices that are responsible for controlling the power system, Supervisory Control and Data Acquisition (SCADA) devices. These devices were not originally designed with security in mind, so opening up older devices to security threats is a major concern. In 2003, an infected computer system in an Ohio power plant caused the monitoring system to stop working for five hours [10]. These types of systems are implemented with SCADA devices and are critical to safely operating power plants, transmissions lines, control systems, and distribution substations.

Protection relays have moved from analog and electromechanical devices to microprocessor control. The differences between these devices are discussed in detail in the Section 3.2.1 Relays. The advantages of the microprocessor based relays come at the cost of potential security risks. If the protective relay network is not secure, relay settings could be changed to unsafe values. These relays protect transmission lines, transformers, generators, and other equipment essential power system operations [48]. If protection settings are changed and a power system fault occurs, it is likely that this equipment could be damaged. This damage could result in extended power outages due to the lack of availability of replacement devices and the complexity of repairs. For example, lead times for transmission level transformers can be several months [14].

The communication network linking control centers to remote systems are separate from public networks. This provides better security, but the demands of newer technologies (Section 3.2.2) and market deregulation push the limits of this network's capabilities. Time sensitive data must be passed between locations accurately. Utilities are utilizing public network such as the internet to meet the demands, but this opens up the critical infrastructure of the power system to cyber security threats.

2.4 A Weaker Grid by Deregulation

There are other reasons for increased vulnerability on the power system. The Energy Policy Act of 1992 was passed by Congress to promote open market energy trading, also known as deregulation. The primary purpose of this act is to provide a competitive market for energy purchasing, and in turn save consumers money. From 1989 to 2002 the purchasing of power increased from 17.8% to 37.3 % for investor owned utilities. This purchasing has put a heavier load on the nation's transmission systems [15]. Due to the high cost and low return on investment, little has been done to increase the capacity of the transmission system [5]. Government regulations require power companies to provide a transmission system that has the capacity to reliably provide power to customers even during transmission contingencies. The industry has adequately conformed, but the increased utilization of the transmission system is still a weak link in the security of the power system [15].

2.5 Costs of Power Outages

Cyber security threats could potentially cause power outages, resulting in significant economic losses. Power outages occur every day throughout the country. Weather causes most problems in the form of a short term loss of power. Large storms can cause longer losses that spread over large areas. These outages disrupt businesses and cause a loss in revenue. The costs are hard to quantify but yearly estimates range from $26 billion to $150 billion in the US [16]. Table 2.2 shows a list of loss totals for some modern power outages.

Table 2.2 Outage Costs [16], [17].

Date	Location or Company	Outage Length	Losses
May 1997	Formosa Plastics	2 Minutes	$11 Million
1998	Auckland, New Zealand	2 Months	$56 Million (est)
1999	New York City	Not given	$100 Million
2003	Silicon Valley, California	Rolling Blackouts	$75 million

The losses shown in the table above could easily be caused by disabling a handful of transmission or distribution locations. It only takes a few seconds of outage to disrupt large industrial processes, shutdown computer systems, and interrupt various business transactions.

The largest power outage to date happened in the northeastern US in 2003. As noted above, this outage affected about 50 million people. The Federal Energy Reliability Council (FERC) found that the overall cost to power companies and businesses was estimated at $4 to $10 billion. This outage started as a fault on a medium sized transmission line and propagated over a larger area due to human and computer error [15]. Though no link was found to cyber attacks, future outages could be created in a similar fashion. An attacker could gain access to a few key systems, disabling warning systems and protection schemes. Meanwhile a fault could be physically caused in an attempt to create a similar chain reaction.

2.6 Government Policy

There are several US government organizations that implement regulations, enforce policy, and provide research support for electric utilities. These agencies include FERC, North American Electrical Reliability Council (NERC), Department of Energy (DOE), and the National Institute of Standards and Technology (NIST). FERC and NERC are the primary policy makers for the power industry.

FERC oversees the entire energy sector including oil and gas industries. FERC's responsibility in the power industry is to manage the interstate transmission system and oversee the sale of electricity in interstate commerce [18]. FERC's activity in cyber security is closely tied to the research and recommendations provided by the not for profit agency, NERC.

NERC's goal is centered on maintaining a reliable power infrastructure. Since the northeast blackout of 2003, NERC has been very active in policy areas concerning Information Technology and cyber security [19].

The DOE and NIST, generally provide support for the power industry. Research by these organizations is performed to improve efficiency of power generation and delivery, increase reliability of power, create new methods of power generation, and improve the security of the power system.

2.6.1 NERC

After the 2003 blackout, NERC was responsible for researching the causes and providing a report with recommendations on preventing similar events in the future. The following are the key findings from the Physical and Cyber Security Aspects section of NERC's report on the 2003 Blackout [15]:

1. Interviews with Emergency Management Systems (EMS) developers indicate that there is a potential for cyber security issues through these systems. These vulnerabilities include loosely controlled system access, inadequate software patching, and unnecessary software installations.

2. Links from SCADA networks to other systems create increased vulnerability.

3. A cyber security attack was not involved in the blackout, but computer failure did play a large role in failure of the grid. An Alarm and Event Processing Routing (AEPR) failed on its primary server and tried to run on the backup. The backup server also failed and the system operators were unaware of this. This software is responsible for reporting grid problems such as transmission line outages. During the time the AEPR was down,

> several transmission lines went out of service and operators received no indication of the events. Therefore they did not know to take corrective actions.

NERC maintains a set of standards named Critical Infrastructure Protection (CIP) with the purpose of protecting the security of the power system. The most recent version of these standards was developed in 2006. Since then these standards have been updated and submitted for review to FERC and await approval [20]. CIP is separated into the nine sections:

Table 2.3 NERC CIP Standards [17].

1. Sabotage Reporting
2. Critical Cyber Asset Identification
3. Security Management Controls
4. Personnel & Training
5. Electronic Security Perimeters
6. Physical Security of Critical Cyber Assets
7. Systems Security Management
8. Incident Reporting and Response Planning
9. Recovery Plans for Critical Cyber Assets

CIP-2 requires that all cyber assets critical to the reliable operations of the Bulk Electrical System be identified and documented. These assets include control centers, transmission substations, generation resources, and protection systems. Parts of these systems qualify as critical assets because they utilize routable protocols that communicate on open networks [21]. A web-based relay management system (WRMS) that utilizes the Internet would certainly meet the criteria to be critical cyber asset. The computer controlled relays used in the WRMS protect generation, transmission, and distribution devices. A breakdown in security for these devices could result in serious reliability problems for the bulk electrical system.

CIP section 5 and 7 are mentioned in Chapters 2, 4 and 5. References to the CIP regulations are made when the system design considered these regulations. Also note that NERC is in communication with the DOE and NIST for the creating and updating of these standards.

2.6.2 DOE

The DOE performs research and development for the modernization of the grid. Research areas include control center security, distributed generation, smart grid, and transmission reliability. Below is a summary of the research and information that is important to this paper [22].

The DOE's document entitled "Roadmap to Secure Control Systems in the Energy Sector" has some key points that can be applied to the Web-bases Relay Management System (WRMS). This project makes use of commercial and free software instead of the custom-designed software currently used in most locations. Since commercial and free software is available to the general public, the exploits for this software are also more available. The software selected for use in power systems must have adequate support and patching capability to keep up with the changing cyber security threats. Also this roadmap emphasizes that increased use of public networks have made control systems more vulnerable to cyber attack [23]. The information sent over these networks must be protected along with the systems that interface with it.

Some of the research performed by the DOE could create an increased need for secure remote management of systems such as the one proposed in this paper. Distributed generation and the smart grid concepts are discussed in their respective sections (3.2 and 3.3).

2.6.3 NIST

NIST is another government agency with the purpose of creating and revising standards in many areas including IT and Control Systems security. There are two papers of interest to this thesis: the Guide to Industrial Control Systems (ICS) and the Guidelines on Securing Public Web Servers.

The Guide to Industrial Control Systems contains information about the vulnerabilities ICS. The vulnerabilities due to passwords in of the most interest to the WRMS. Below is a listing of the applicable password vulnerabilities:

Table 2.4 Password Vulnerabilities [24].

1. Lack of adequate password policy.
2. No password used.
3. Password disclosure by both human and un-encrypted transmission.
4. Poor password complexity.
5. Poor access controls.

The WRMS is not an ICS, but both have the same topology, an access point, a network link, and control devices [24]. So, password problems for one can apply to the other. The WRMS utilizes biometric authentication and data encryption to address these common vulnerabilities.

The Guidelines to Securing Public Web Services is a much more relevant document to the WRMS since the application resides on a web server. This document provides information on firewalls, user authentication, encryption, and vulnerabilities in the content of the websites [25]. The WRMS is designed with these vulnerabilities in mind.

2.6.4 Government Overview

The US government has taken many steps to identify and address vulnerabilities in the power system and mandate compliance to cyber security standards. NERC has the legal power to enforce standards it creates with cyber security, thus forcing utilizes to comply. The DOE's research on modernizing the grid and the changes the industry is making towards this effort is increasing the usage of public networks which increases cyber vulnerabilities of the grid. The DOE, NIST, and NERC are working together to provide utilities with tools they need to safely create and deploy systems like the WRMS to the power system infrastructure.

2.7 Biometric Authentication

Biometric authentication is emerging as a useful technology for securing IT resources. Biometrics uses physical characteristics or behavioral traits to potentially replace the passwords and PIN's that are currently popular with computers, ATM's, and websites [26]. It is important to understand the strengths and weakness of biometric authentication in order to implement a system that safely uses biometrics for access control.

Biometric authentication involves choosing a modality (such as fingerprint) to identify a person. If a fingerprint is chosen, then the user must enroll in the system and a digital representation of that fingerprint must be stored. This could be a database or smart card. If the digital fingerprint is not protected, it could be stolen and used by hackers to gain access to a secure system. Users often present their biometric to a system from a remote location. The biometric data travel across a network and must be protected while in transit to prevent it from being stolen [27].

If biometric authentication is not used carefully, then it is possible that it is a less secure solution than passwords. This section compares a strong password verification scheme with a fingerprint biometric scheme combined with a weak password.

Passwords are considered knowledge based authenticators. This is information that a user must know to use. The drawbacks to passwords are that they can be easily shared, forgotten, or written down and stolen. Password complexity can also vary significantly. Short passwords consisting of dictionary words can make password security easy to break or weak. Longer passwords consisting of a larger set of characters makes the number of possible passwords to guess much higher, constituting a strong password. The drawback of strong passwords is that users are more likely to forget them or store them in an unsecure manner.

Biometric identification is much more complex. When biometric data is captured, it is turned into a digital representation. The digital representation has a longer length than passwords and also the character set is much broader. This gives a much larger amount of possible of character combinations than passwords. However, biometrics systems do not require a 100% match between the stored representation and the supplied one. Matching algorithms compare the two representations and give a matching score. If the score is acceptable, the user is said to match and may be granted access. This algorithm is not perfect and introduces an error called False Match Rate (FMR). This number is a percentage chance that an imposter will be validated as a valid user in the system in a one to one matching situation. This error effectively reduces the strength of the representation [28]. Figure 3 is a chart containing experimentally found FMR percentages for common modalities.

Table 2.5 FMR by Modality [28].

Modality	FMR
Fingerprint	0.01% - 0.15 %
Hand	0.01% - 0.15 %
Voice	0.01% - 0.15 %
Face	5% - 10 %
Iris	0.0001 %

Passwords do not have an FMR so these values must be converted to keyspace to compare biometrics to passwords. A keyspace is the number of possible values to a key. For passwords this is defined by the following equation:

$$k_p = c^n$$

Where n is the number of characters in the password and c is the number of different values of the characters.

Keyspace for biometrics considers the FMR and is defined in the following equation.

$$k_b = \frac{1}{FMR(1)}$$

Note that the supplied FMR is from one user attempt at verification.

Using the experimentally found FMR's and given password keyspaces the following chart is derived to compare keyspace sizes (see Table 2.5).

Table 2.6 Verification Method Keyspace Strength [28].

Verification Method	Keyspace
PIN (4 Digit)	10^4
Password (Strong)	2.2 x 10^14
Password (Weak)	10^6
Iris	10^6
Fingerprint	10^4
Face	6.25

An important note here is that a fingerprints and PINs have the same keyspace and even weak passwords provide more. Keyspace is an indication of how well a verification method is protected against client or brute force attacks. This is just a matter of guessing a password or supplying a biometric to attempt access. If only keyspace is considered fingerprints are not the best solution, but there are ways to improve performance. If a verification system limits the number of failed verifications, the effectiveness of the keyspace is greatly increased.

In fact, a combination of a biometric data and a password provides a better solution to either method alone. The strength of a biometric is that it is not easily shared with others, which is a weakness of passwords. The strength of a password is its larger keyspace and changeability (fingerprint biometrics typically have neither attribute). In short, the password provides a changeable, easy to administer option to identify a user while the biometric backs up the password by nearly eliminating the user errors associated with passwords [28].

This combination of biometrics and passwords is used by the WRMS to meet access control requirements cited in CIP-5 Section R2.4.

> “Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at

> the access points to ensure authenticity of the accessing party, where technically feasible.” [21]

2.8 Conclusion

Cyber security currently poses a threat to the operation of the power system and its future advancement will only increase this threat. Government regulations are causing utilities to address these issues. Biometrics can be used access control to help utilities meet government standards and protect the nation’s electrical grid.

Chapter 3
Power System Overview

This chapter describes the operation of each sector of the power system. The key focus is to show locations of the devices where the WRMS could be used. Since the project works with a distribution relay, a more detailed description of a distribution substation is presented. Also technologies such as computer controlled relays, smart grids, and distributed generation are introduced at the end of this chapter.

3.1 Power Industry Sectors

3.1.1 Generation

Although there are many sources of energy for electricity production, most power plants share the connection and control layout in figure 3.1 below.

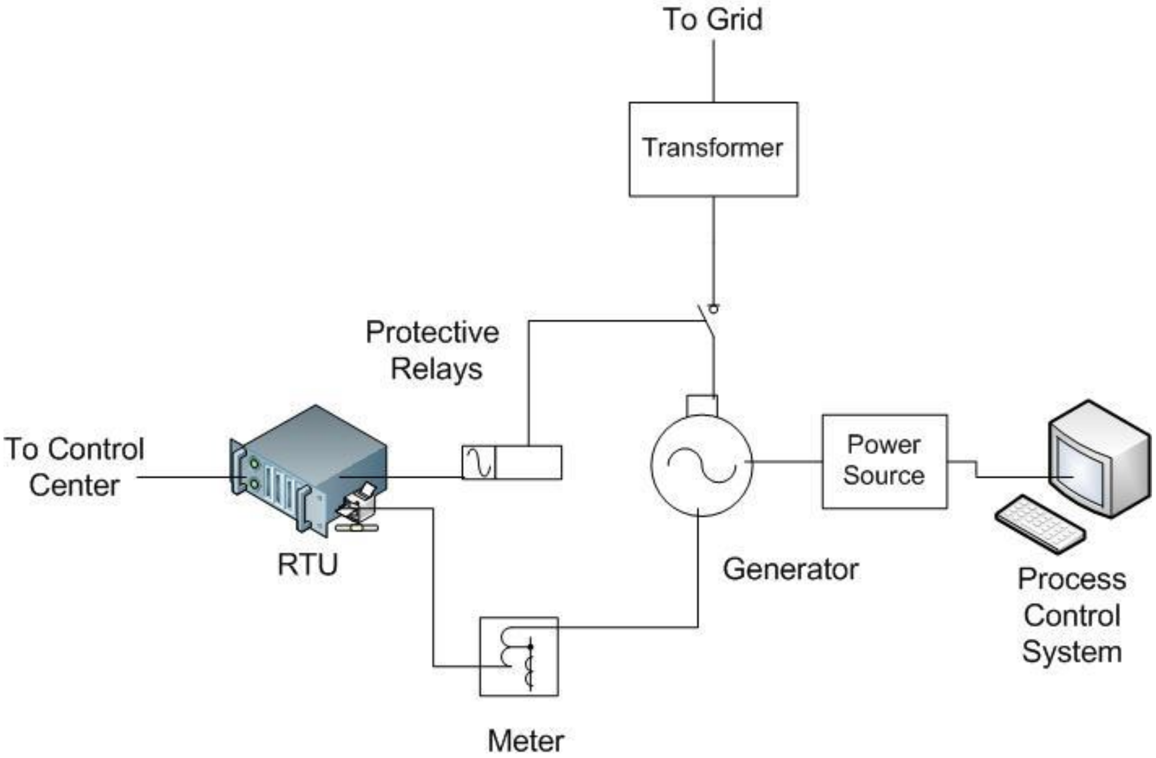


Figure 3.1 Power Plant Block Diagram [29].

The generator and power source are connected to a process control system which is responsible for varying output power and voltage of the generator. On the electrical side, there is a network of relays configured to protect the generator from damage. These relays could be a system of electromechanical relays or even a single computer controlled relay. The RTU (SCADA device) interfaces with the relay and metering systems and communicates this data back to a centralized control center (see section 3.1.4). The RTU (Remote Terminal Unit) also receives control signals from the control center that indicate the amount of power needed from the generator [29].

3.1.2 Transmission Substation

Transmission substation convert the high voltage of incoming transmission lines down to lower distribution levels. Transmission substations can vary greatly in size and layout, but most follow the form in Figure 2.

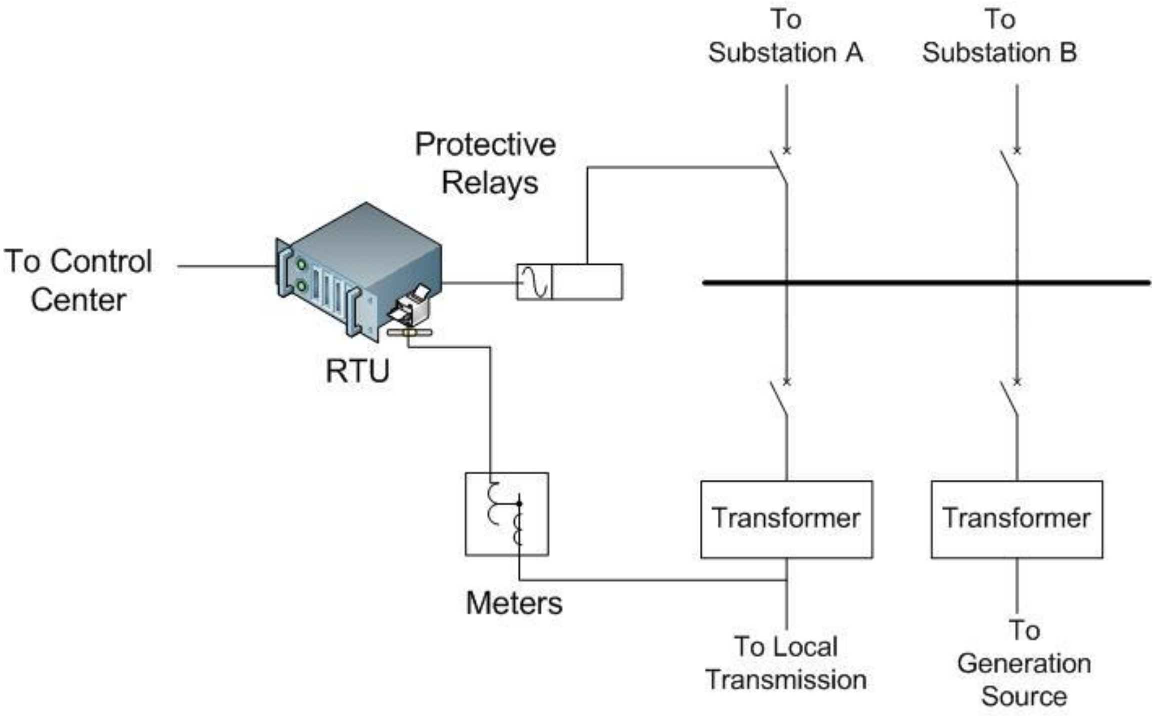


Figure 3.2 Typical Transmission Substation [29].

Power enters the substation as a high voltage from the local transmission system and is stepped down with a transformer for the substations A and B. A generation source is also indicated connected to the substation. Protective relays are in placed in line with every external connection and around transformers within the substation. If computer controlled relays are used, they are networked with the RTU and provide relay status, voltage, current, and power information. The meters monitor energy flowing in and out of the substations which is also communicated to the RTU. This data is communicated back to a control center. Note that the RTU is a SCADA device like the one in the Generator section [29].

3.1.3 Distribution Substation

As seen in Figure 3.1 distribution substations are very similar to transmission substations. Their main purpose is to convert distribution level voltage down to medium levels for utilization. Figure 3.3 is a typical distribution substation.

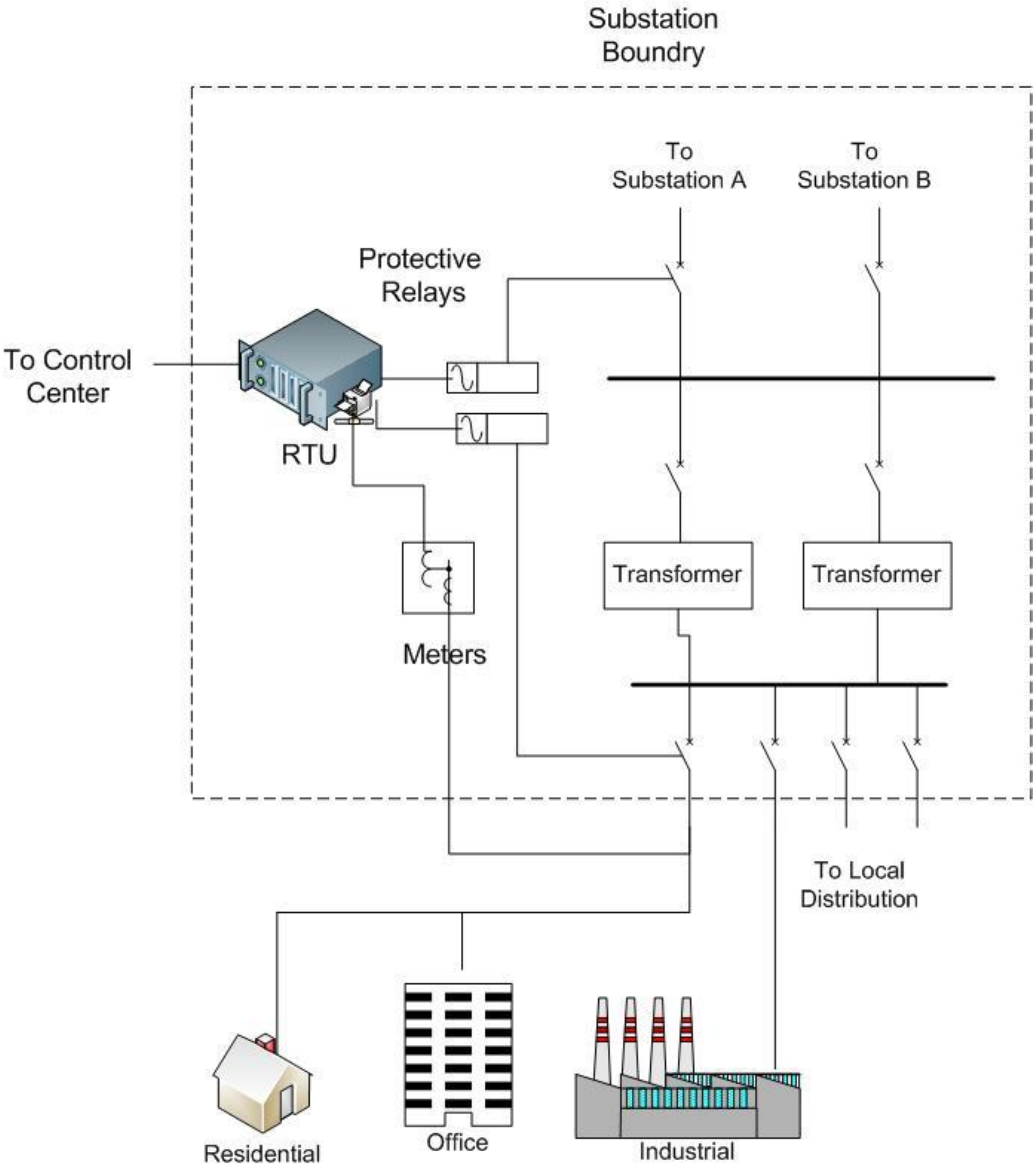


Figure 3.3 Typical Distribution Substation [29].

The relays at this level are likely electromechanical type with no communication capability. However, computerized relays are becoming more common in distribution such as the SEL-751 distribution feeder relay used for the WRMS. Other technologies such as automated meter reading operate from distribution substations. These devices typically work wirelessly and provide a pathway for attackers to exploit [29].

3.1.4 Control Centers

Control centers contain the systems that are important for the operation and maintenance of the generation, distribution, and transmission resources that have been described in this chapter. The control center communicates through leased lines, wireless (microwave), fiber, and public telephone networks to these resources. The SCADA system within the control center communicates control signal to the RTU's while the RTU's returns data that is important for monitoring the electrical system. This data includes power flows, relay status, and voltage levels. Energy Management Systems (EMS) also operate with data collected at control centers. These systems are responsible for optimizing power generation and transmission [29]. Control centers are likely location for using the WRMS.

3.2 Distribution Substation Technology

3.2.1 Relays

As mentioned before, relays are responsible for protecting the equipment used in the power system. These devices can detect voltage, current, frequency, temperature, and many other conditions and trigger action if these values are outside of a safe operating range. There are three types of relays: electromechanical, solid state and microprocessor based. Each type of relay receives a number of inputs and controls a number of circuit breakers.

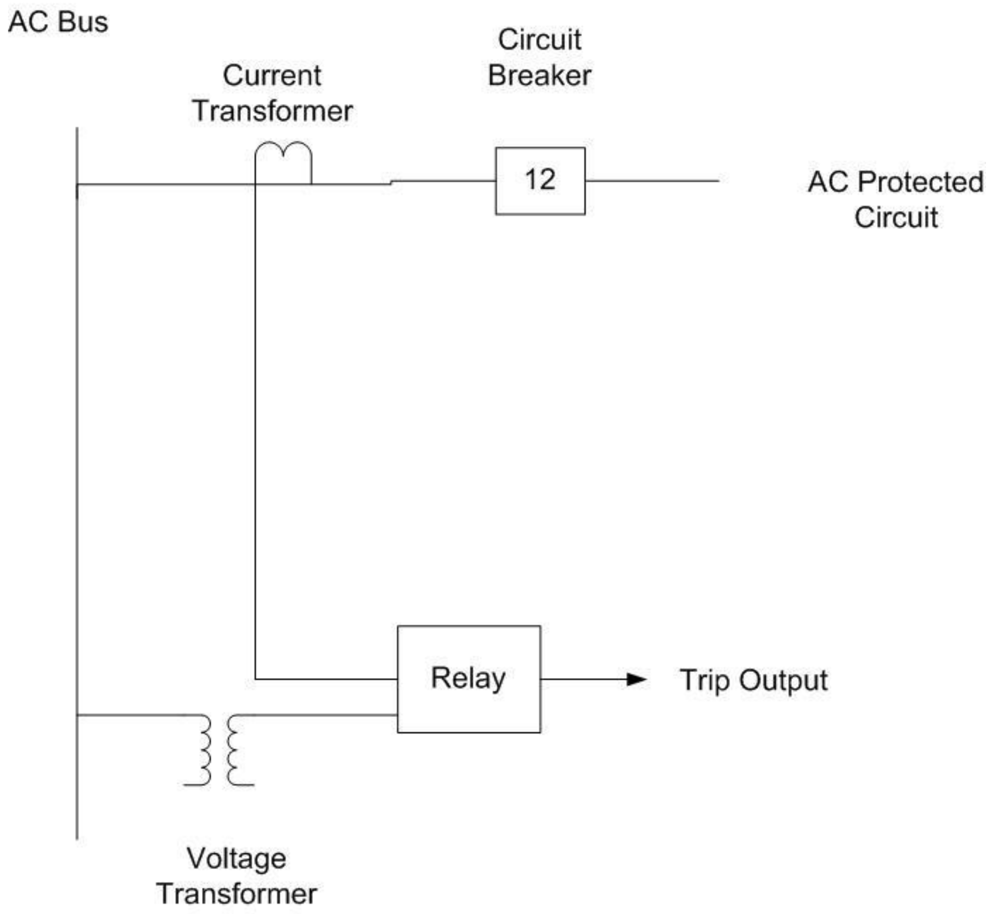


Figure 3.4 General Relay Connections [48].

The relay depicted above could be any of the three mentioned types. This relay senses voltage and current from a single phase of an AC bus and sends a trip signal to the circuit breaker labeled 12 on the AC protected circuit. The inputs of the relay do no operate at distribution levels and must be stepped down with the indicated current and voltage transformers [48].

Electromechanical and solid state relays are usually limited to single functions such as current, voltage, power, or temperature. If protection is needed from multiple types of faults, then multiple relays must be used. Microprocessor controlled relays are becoming more popular and can substitute for multiple legacy relays. The following are some benefits of computer controlled relays listed in Protective Relaying Principles and Applications.

Table 3.1 Microprocessor Relay Advantages [48].

1. More protection, less cost.
2. Wiring Simplification.
3. Greater Flexibility.
4. Less maintenance requirements.
5. Event recording capability.
6. Data acquisition for metering.
7. Built in logic for control and automation.
8. Communication capability – ability to design enhanced protection schemes.
9. Capabilities for remote interrogation and setting applications.

The WRMS uses the communication capability of these relays to remotely change protection settings.

These capabilities do have some disadvantages. Since microprocessor controlled relays can replace multiple elecromechanical ones, they become a single point of failure for a protection scheme. Also, the extra features result in larger and more complicated user manuals. A full implementation of these features can result in longer setup times [48]. The use of a remote setting application is a security risk if it is not protected from unauthorized use. The WRMS addresses security of remote access in its design.

3.2.2 Distributed Generation and the Modern Grid

Distributed generation is a small-scale production of electricity at or near its destination. This concept is becoming popular as technology is increasing the efficiency and decreasing the cost of deployment. Distributed Generators (DG's) are also used as backup power devices for locations that require highly available power sources such as hospitals. Some large industrial plants utilize DG's to generate steam and electricity for their processes (cogeneration). Traditional centralized power plants generate over 100 megawatts, while distributed generation systems range from 100 kW up to the 100 MW range. Growth of distributed generation has the potential to significantly supplement the power system as load grows [30].

New concepts for the ways that distribution networks operate have been proposed to increase reliability. Advanced control techniques, distributed generation, and better metering and protection devices are used to accomplish lower cost, better efficiency, and higher reliability [49]. The Smart Grid, Modern Grid, and Microgrids are the names a few concepts. Below is an example of a Microgrid.

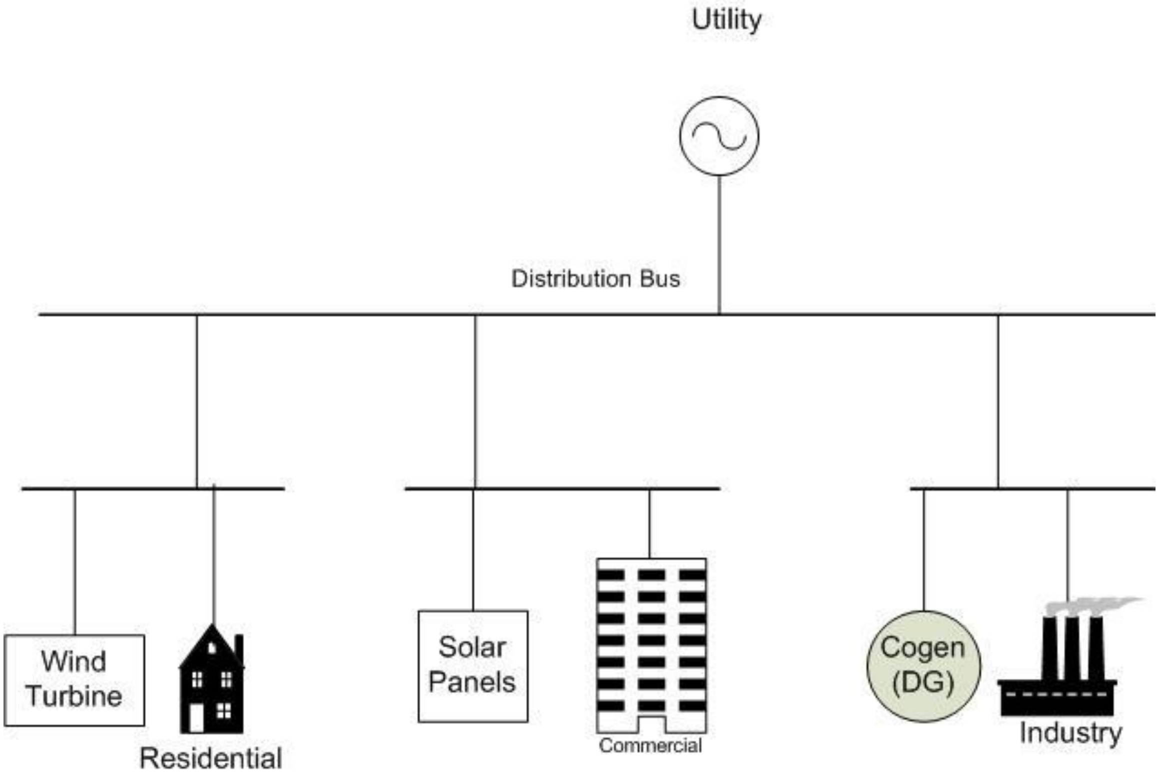


Figure 3.5 Microgrid Example [31].

Microgrids use multiple power sources (DG) and a connection to the utility to provide increased reliability. In the event that the DG in the above system cannot meet the demand, the needed power is delivered from the external utility. If a power outage removes this external source, then a control system removes less critical loads from the system until there is excess power. Any extra power generated by the DG's can leave the Microgrid for sale to the utility.

The Modern Grid and Smart Grid concepts build on this model and address communication strategies, measurement technologies, and advanced control. Distributed Generation is a key similarity between each of these concepts and is their deployment provides a use for the WRMS in the power system.

When a DG generates more electricity than the local demand, the excess power will flow back into the substation along the feeder. Power directional relays are necessary to monitor this export energy [29]. As additional DG's are introduced to a distribution system, changes may be necessary in the protection schemes to accommodate the new electricity source. Managing these changes could be a use for the WRMS.

Chapter 4
Web-Based Relay Monitoring System with Biometric Authentication (WRMS)

4.1 Introduction

The WRMS is a web based tool for modifying relay settings of a SEL-751A Feeder Protections Relay. This system uses a combination of fingerprints and passwords for authentication of the user through the web browser. The purpose of this system is to provide a safe way to modify protection schemes without engineers needing to travel to remotely located substations. Figure 4.1 shows an overview of the RMSS.

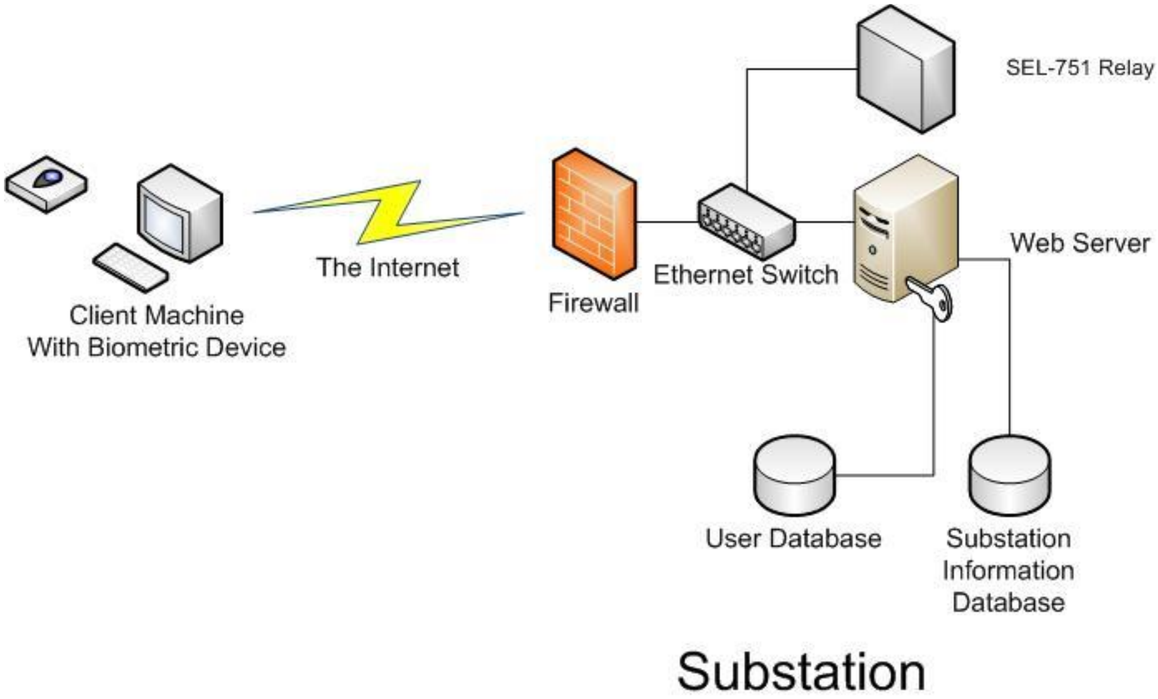


Figure 4.1 WRMS Overview.

A user uses the Internet Explorer web browser to request the website hosted on the web server shown above. He or she must provide a correct username, password, and fingerprint to access any functionality within the website. Once access is granted the user has the ability to view settings, modify settings, check relay status, and monitor the status of requested relay modifications. The user’s access level determines the website functionality available. The databases and software required to perform these tasks is all located on the web server shown above. The website only has the functionality to access and update the substation information database. A web user has the capability to request a change to relay settings. Another application was developed to run in the background as a separate entity. This program periodically reads the modification requests, determines their validity, and updates the relays accordingly. This provides another layer of protection from the outside world. This chapter is a walkthrough of each part of this system.

4.2 Login Process

The framework for the login process was motivated by [35]. Below is a flow chart representing the login process of the WRMS.

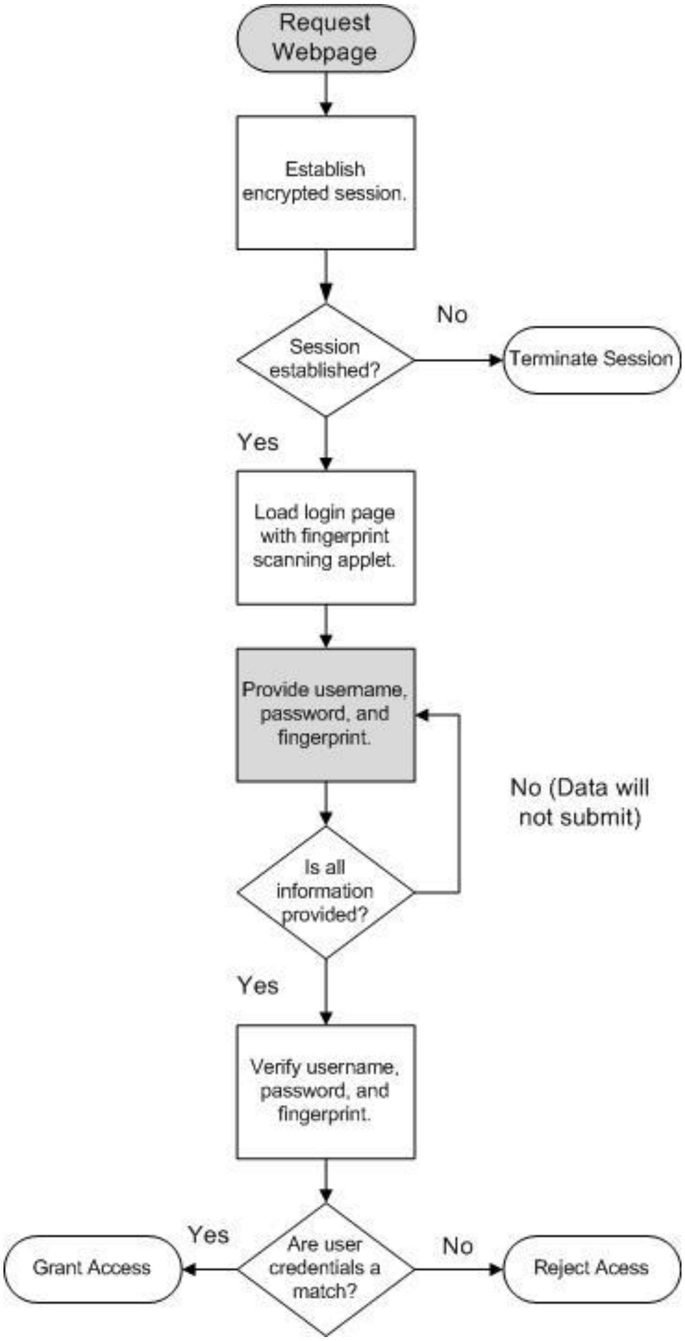

Request Webpage
Establish encrypted session.
Session established?
No
Terminate Session
Yes
Load login page with fingerprint scanning applet.
Provide username, password, and fingerprint.
No (Data will not submit)
Is all information provided?
Yes
Verify username, password, and fingerprint.
Yes
Grant Access
Are user credentials a match?
No
Reject Acess

Figure 4.2 Login Process.

The first step in the login process is the creation of the secure session. This is done so that the user's biometric data, login, and password are sent across the internet as encrypted data. The secure session consists of the exchange of an encryption key and session id between the web browser and server. The encryption key is used to create an SSL (Appendix B) connection to encrypt all data exchanged while the website is used. The session id is a pseudo-random number generated by the website application and sent to the browser. The number is used by the web application to establish one to one relationship to the user's web session (Appendix B). If an SSL connection and session id are established, the web server transmits the login web page. If either condition is not met, the web server will not serve the login page.

The login page consists of an ActiveX object (Appendix B) that contains the fingerprint scanning functionality, a username text box, a password text box, and a submit button. The ActiveX object initializes if the browser is Internet Explorer (IE) and the Griaule biometric scanning software is installed on the client machine. Both IE and Griaule are discussed in more detail in Appendix A. The following flowchart describes the process the object follows to obtain a fingerprint template.

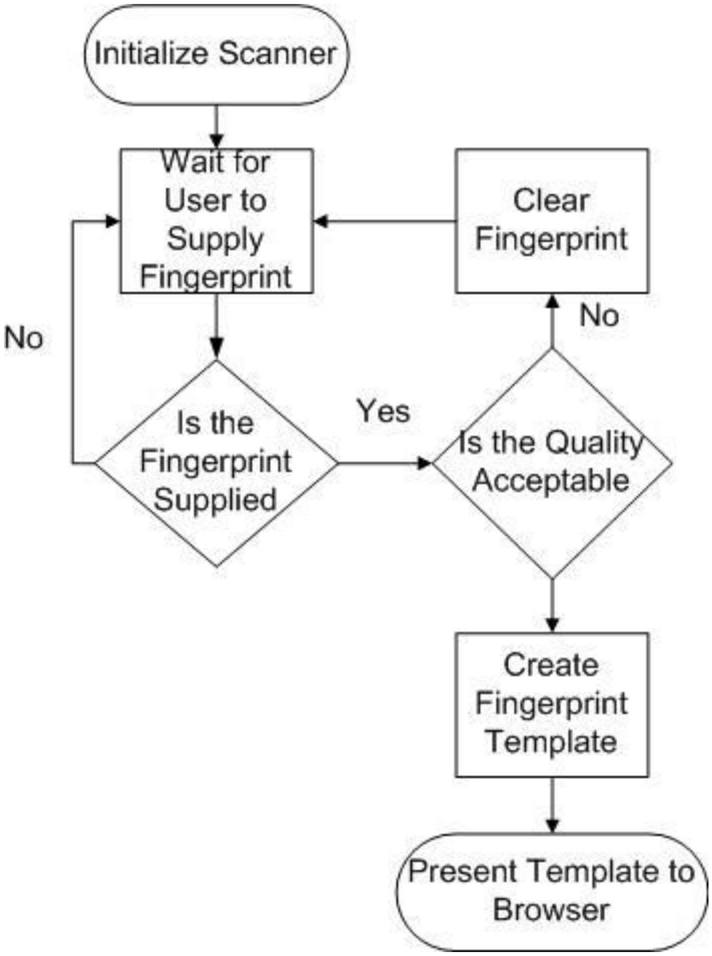
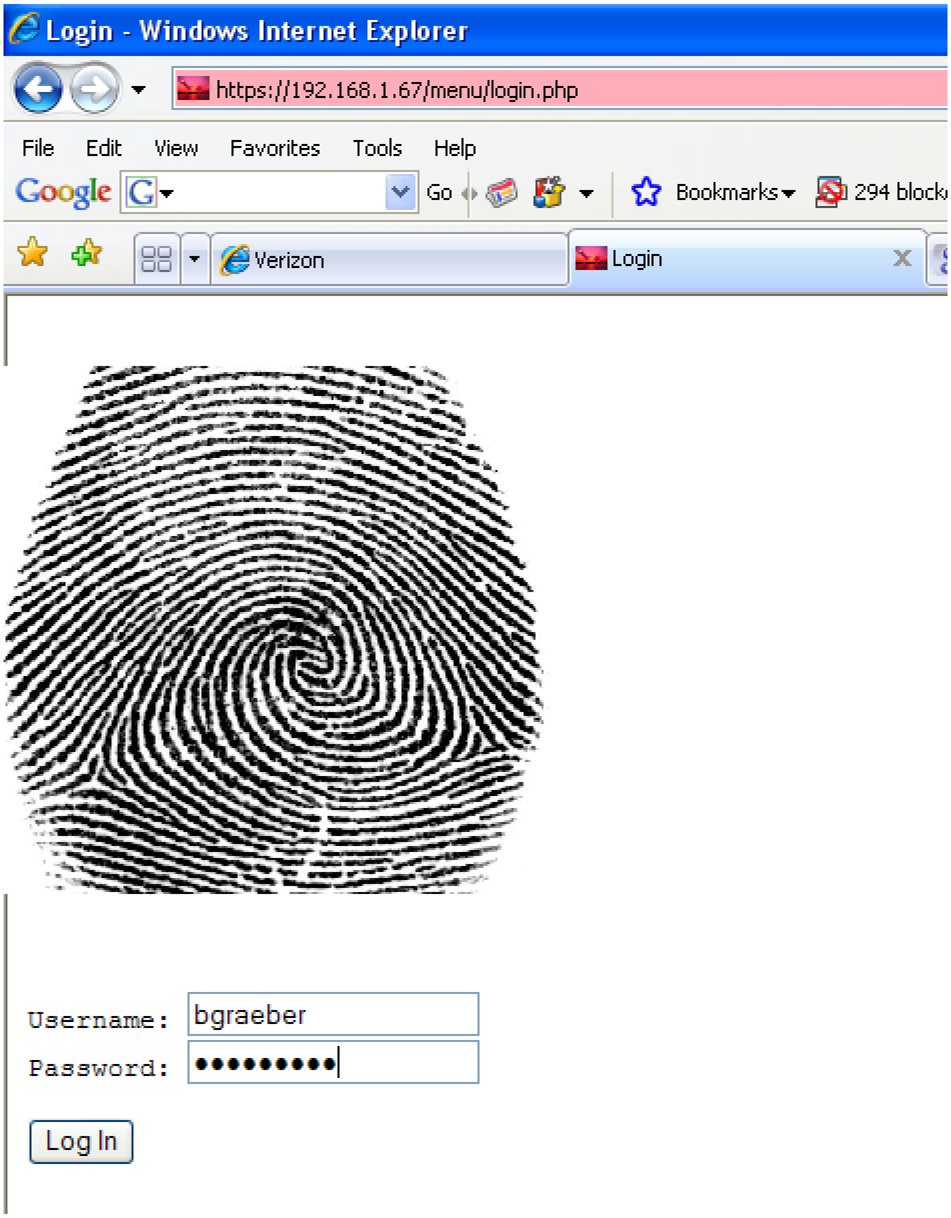

Initialize Scanner
Wait for User to Supply Fingerprint
Clear Fingerprint
No
No
Is the Fingerprint Supplied
Yes
Is the Quality Acceptable
Create Fingerprint Template
Present Template to Browser

Figure 4.3 Finscan.dll (ActiveX object) Fingerprint Template Capture Flowchart.

The object first initializes the fingerprint scanner and instructs the hardware to capture an image once the user has placed his or her finger on the scanner. After the image is captured, a quality score is determined by the number of minutiae found on the fingerprint. If this value is too low, an error message is posted on the object and the user has the opportunity to rescan the fingerprint. If the quality is acceptable, a template is created and the data is presented to the web browser. Figure 4.3 shows a picture of a successful fingerprint scan.

The user must also supply a username and password to the web browser before any data can be submitted to the web server. Figure 4.4 also shows the login page with all data entered correctly just prior to clicking the submit button.



Username: bgraeber

Password: ●●●●●●●●●●

Figure 4.4 Website Login [32].

Once the submit button is clicked the username, password, and fingerprint are sent to the web server for validation. If the username, password, and fingerprint do not match, a blank page is returned and the session id is removed. Otherwise, the menu page is loaded.

4.3 Website Main Menu

The menu page consists of a list of links the user is allowed to follow. The links listed change depending on the access level the user has on the website. High level users have the capability to edit relays setting and even administer accounts. Lower level users may only be able to view relay status and setting. This access level is stored in the User Database and ranges from one to nine. Below is a list of website functions and their corresponding access level.

Table 4.1 Website Function Access Level.

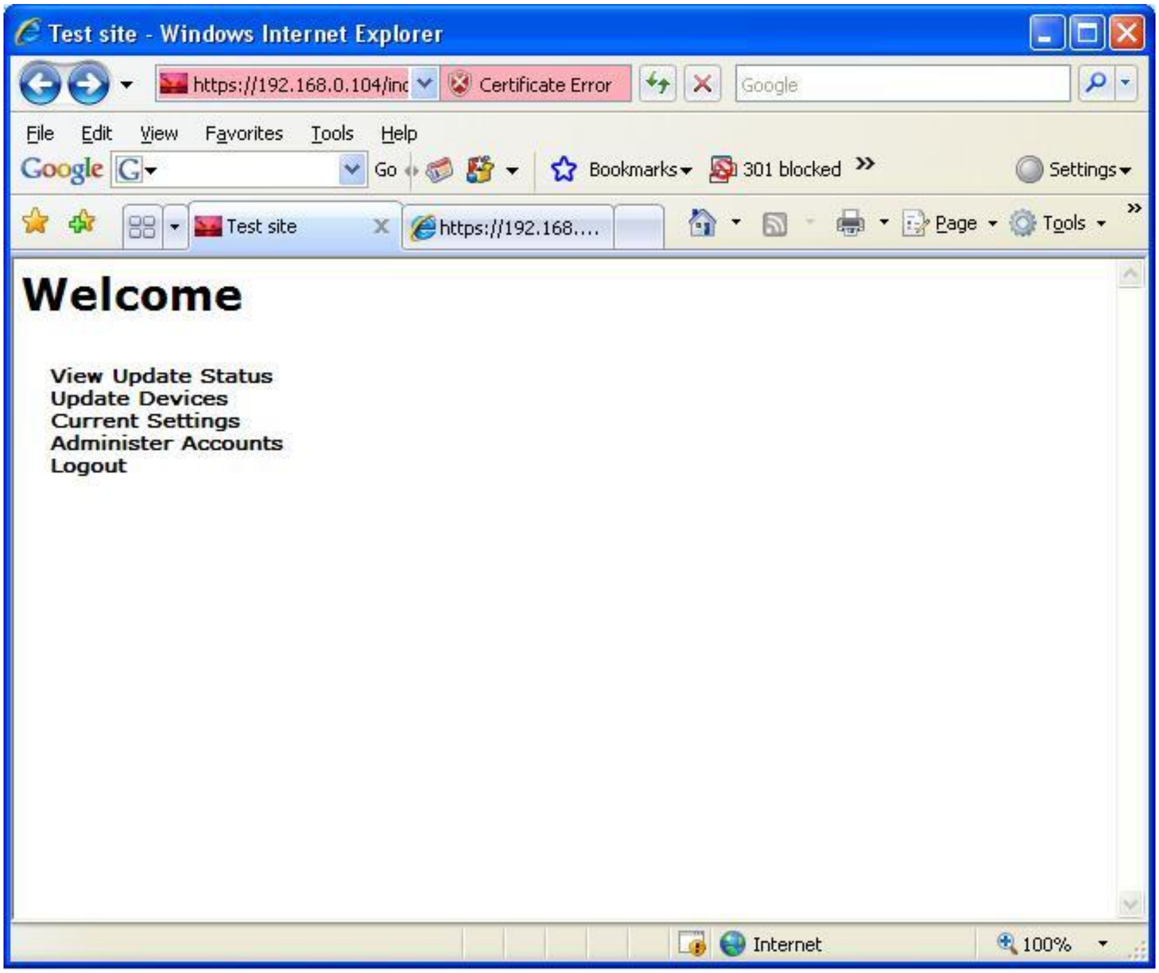
Access Level	Function
1	Logout
3	Current Settings
4	View Update Queue
7	Update Devices
9	Administer Accounts

Users obtain access to functions that are less than or equal to their assigned access level. The empty access level numbers are reserved for any future updates in functionality. This restriction of functionality is required by CIP-7 Section 5.1. This section states

> "The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed." [21]

Users of the WRMS can be restricted to only the capabilities that are necessary to their job description.

This main menu remains available the entire time a user is logged into the website. Figure 4.5 is an example of the main menu page with all available options.



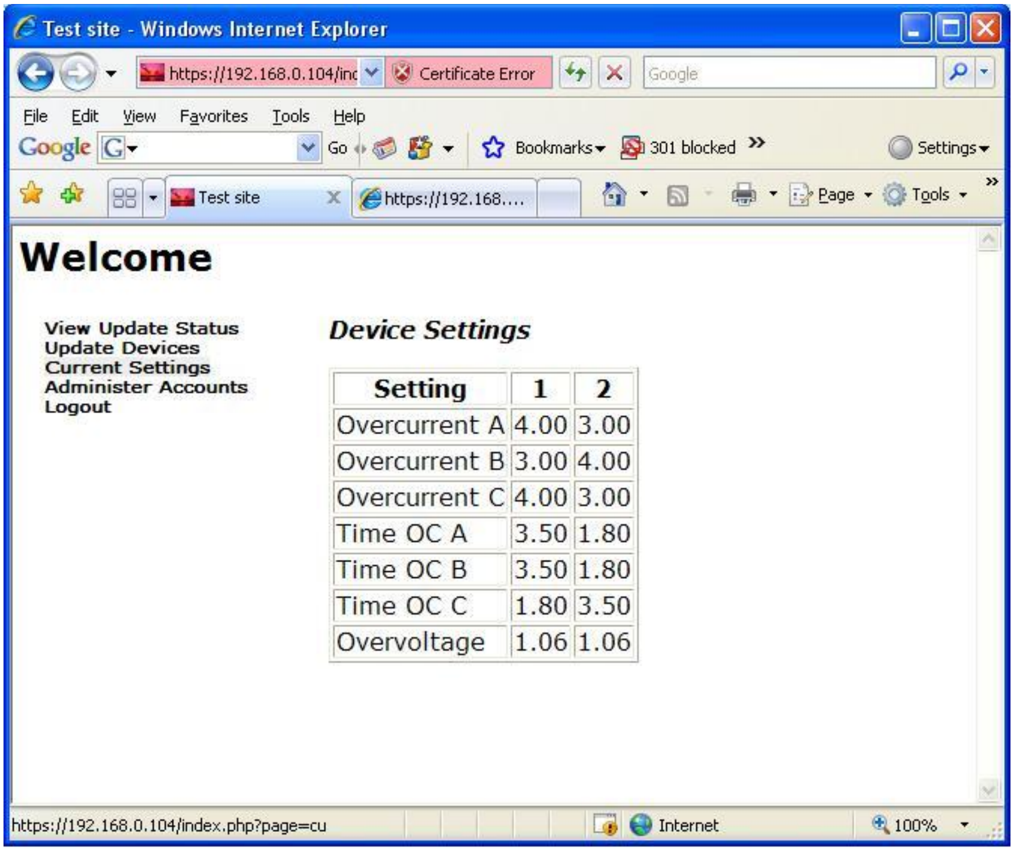
Welcome

View Update Status
Update Devices
Current Settings
Administer Accounts
Logout

Figure 4.5 Menu Page with Full Options.

4.3 Current Settings

This page is a listing of relays and their settings in the substation database. The WRMS only includes three phases of instantaneous overcurrent and time overcurrent along with a single phase of overvoltage relay settings. The system could be expanded to include all of the modifiable fields for future implementations. The columns indicate the device number and the rows indicate the relay settings. There is no modifiable data in this web page which is the reason it has such a low access level in the menu. Figure 4.6 is an example of the Current Settings web page.



Test site - Windows Internet Explorer
https://192.168.0.104/inc
Certificate Error
Google
File Edit View Favorites Tools Help
Go
Bookmarks
301 blocked
Settings
Test site
https://192.168....
Page
Tools
https://192.168.0.104/index.php?page=cu
Internet
100%

Welcome

View Update Status
Update Devices
Current Settings
Administer Accounts
Logout

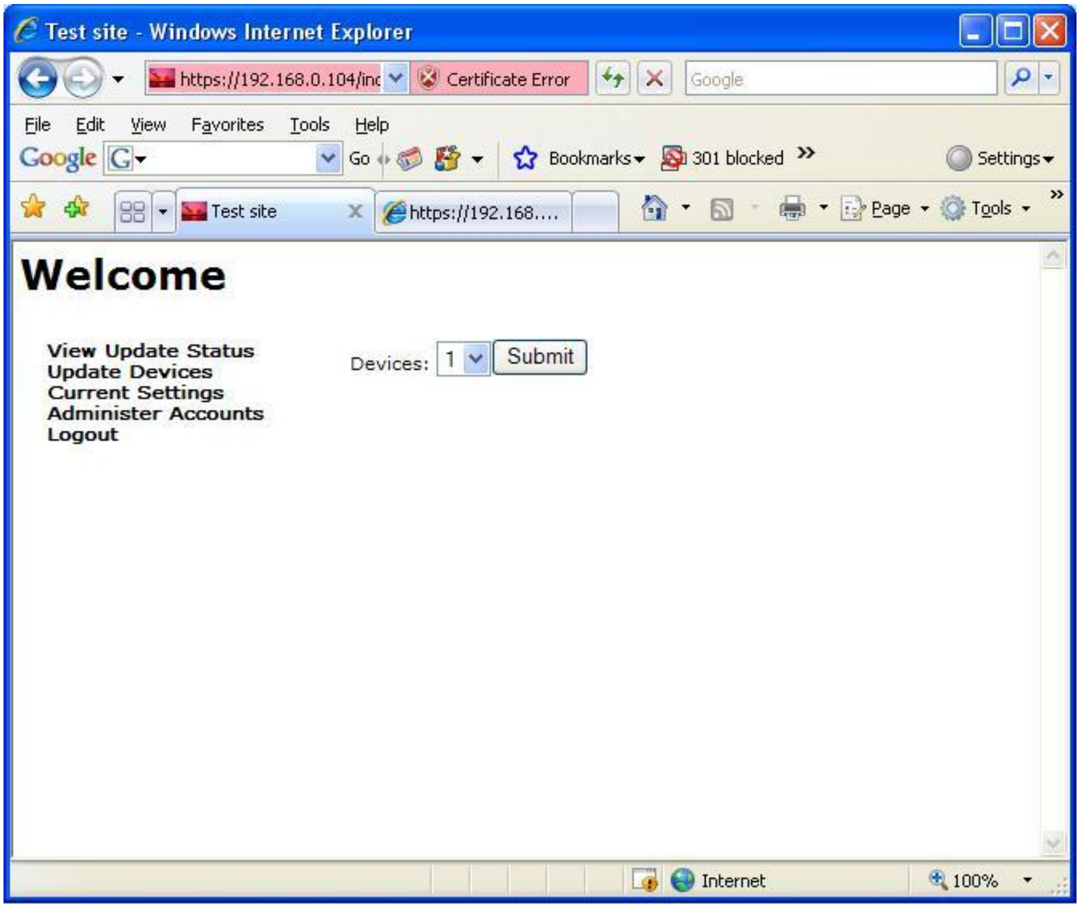
Device Settings

Setting	1	2
Overcurrent A	4.00	3.00
Overcurrent B	3.00	4.00
Overcurrent C	4.00	3.00
Time OC A	3.50	1.80
Time OC B	3.50	1.80
Time OC C	1.80	3.50
Overvoltage	1.06	1.06

Figure 4.6 The Current Settings Web Page.

4.4 Update Devices

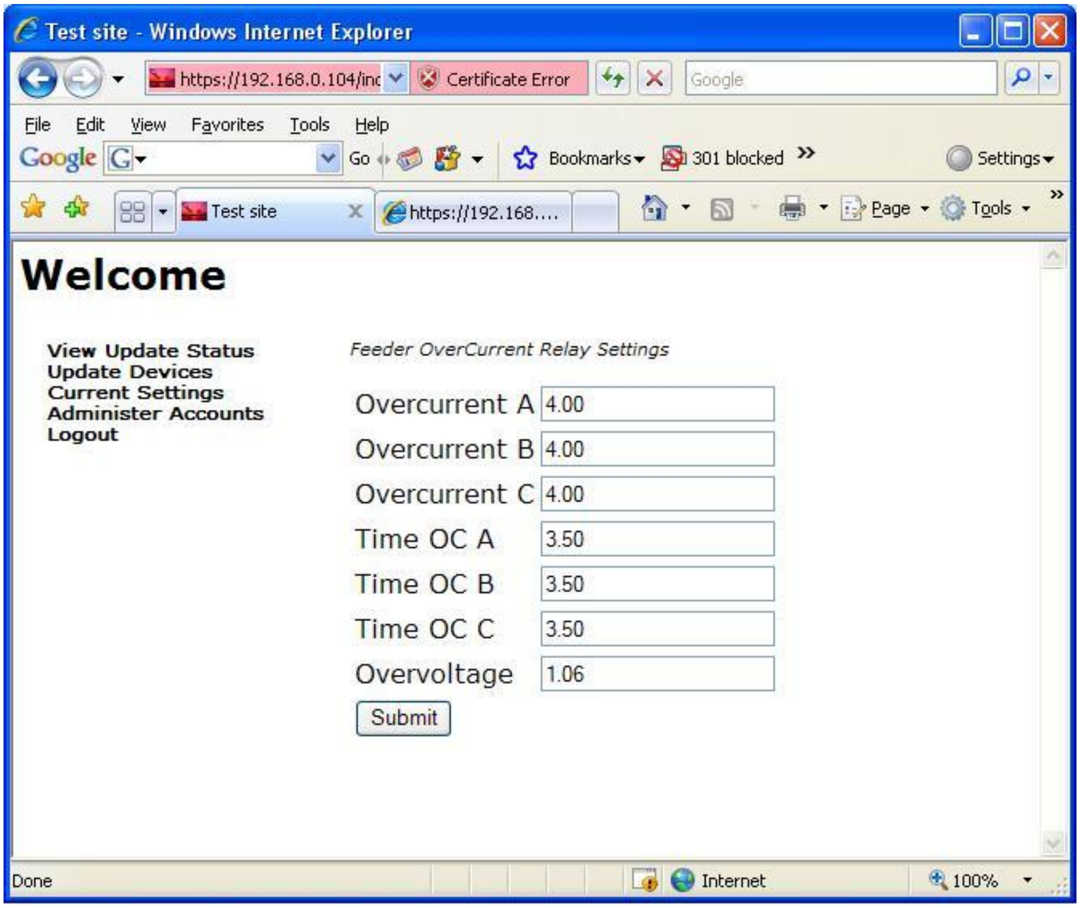
This menu option is where the user can make updates to SEL-751A device settings. Through this page the user has the capability to make changes to relay settings. This is the reason it is assigned a very high access level (indicating a high security level). Figure 4.6 shows the first page where the user is given a drop down box to select the relay to modify.



Devices: 1

Figure 4.7 Relay Selection Web Page.

The user selects the number corresponding to the correct relay and clicks the submit button. A new page loads with input boxes for overcurrent, time overcurrent and overvolatage settings. Figure 4.8 shows this page.



Welcome

View Update Status
Update Devices
Current Settings
Administer Accounts
Logout

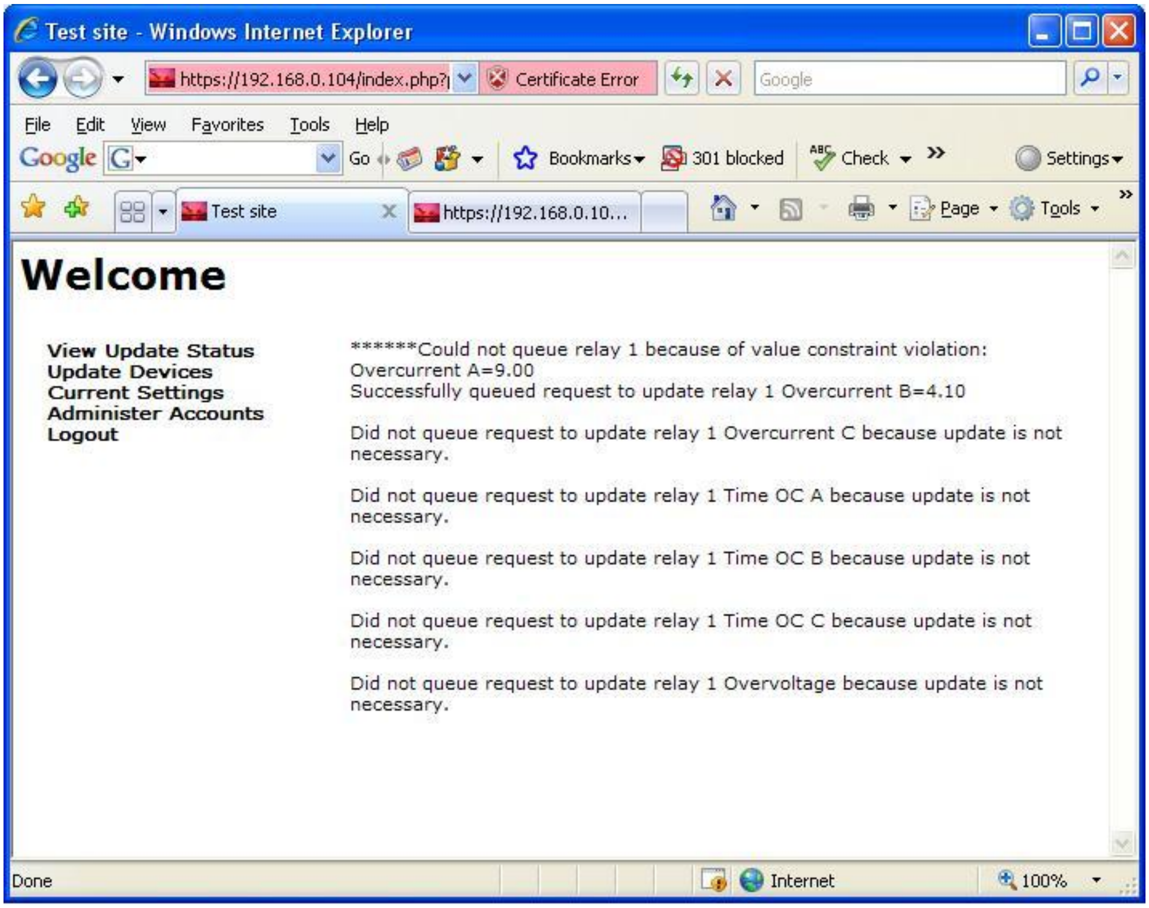
Feeder OverCurrent Relay Settings

Overcurrent A	4.00
Overcurrent B	4.00
Overcurrent C	4.00
Time OC A	3.50
Time OC B	3.50
Time OC C	3.50
Overvoltage	1.06

Submit

Figure 4.8 Update Device Setting Page.

Each of the text boxes is populated with the current settings of the relay. The user can change any number of the settings. When the changes are complete, the user must click the submit button. Once the data is submitted it goes through a verification process before it is written to the substation database. This process is explained in Section 4.8 Change Verification. Assuming all changes are valid, a new page is displayed with a list of the relay modifications made. Any invalid changes are also displayed. Figure 4.9 show an example of this page.



Welcome

View Update Status
Update Devices
Current Settings
Administer Accounts
Logout

******Could not queue relay 1 because of value constraint violation: Overcurrent A=9.00
Successfully queued request to update relay 1 Overcurrent B=4.10

Did not queue request to update relay 1 Overcurrent C because update is not necessary.

Did not queue request to update relay 1 Time OC A because update is not necessary.

Did not queue request to update relay 1 Time OC B because update is not necessary.

Did not queue request to update relay 1 Time OC C because update is not necessary.

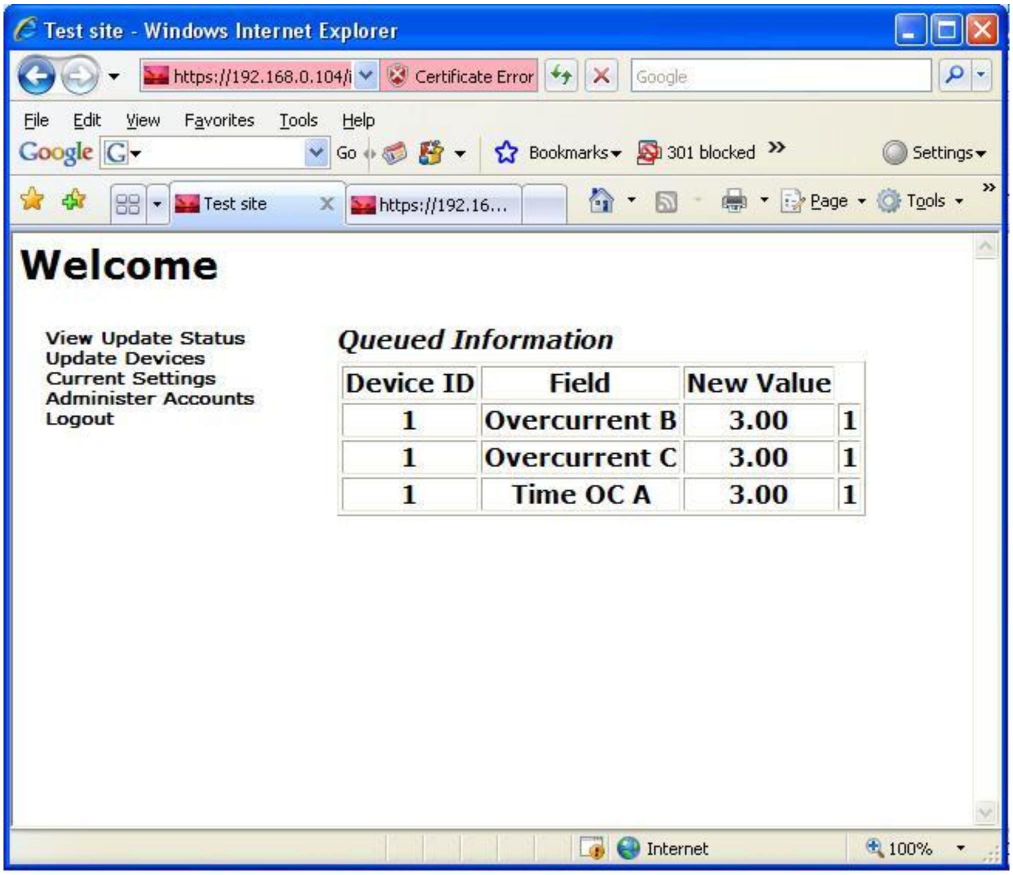
Did not queue request to update relay 1 Overvoltage because update is not necessary.

Figure 4.9 Change Results Web Page.

An example of an invalid change, a valid change, and no setting change are all displayed in the figure above.

4.5 View Update Status

This web page displays a table of all the relay changes that are waiting to be applied. The information displayed here is read only which is reason this page has a low access level. This access level is higher than the current settings page because it indicates more functionality. Figure 4.10 is an example of this page.



Welcome

View Update Status
Update Devices
Current Settings
Administer Accounts
Logout

Queued Information

Device ID	Field	New Value	
1	Overcurrent B	3.00	1
1	Overcurrent C	3.00	1
1	Time OC A	3.00	1

Figure 4.10 View Update Status Web Page.

The table shows the device number, setting name, setting value, and a status number. The status number indicates what point the update is in the update process. Below is a table with list of status numbers and their meaning.

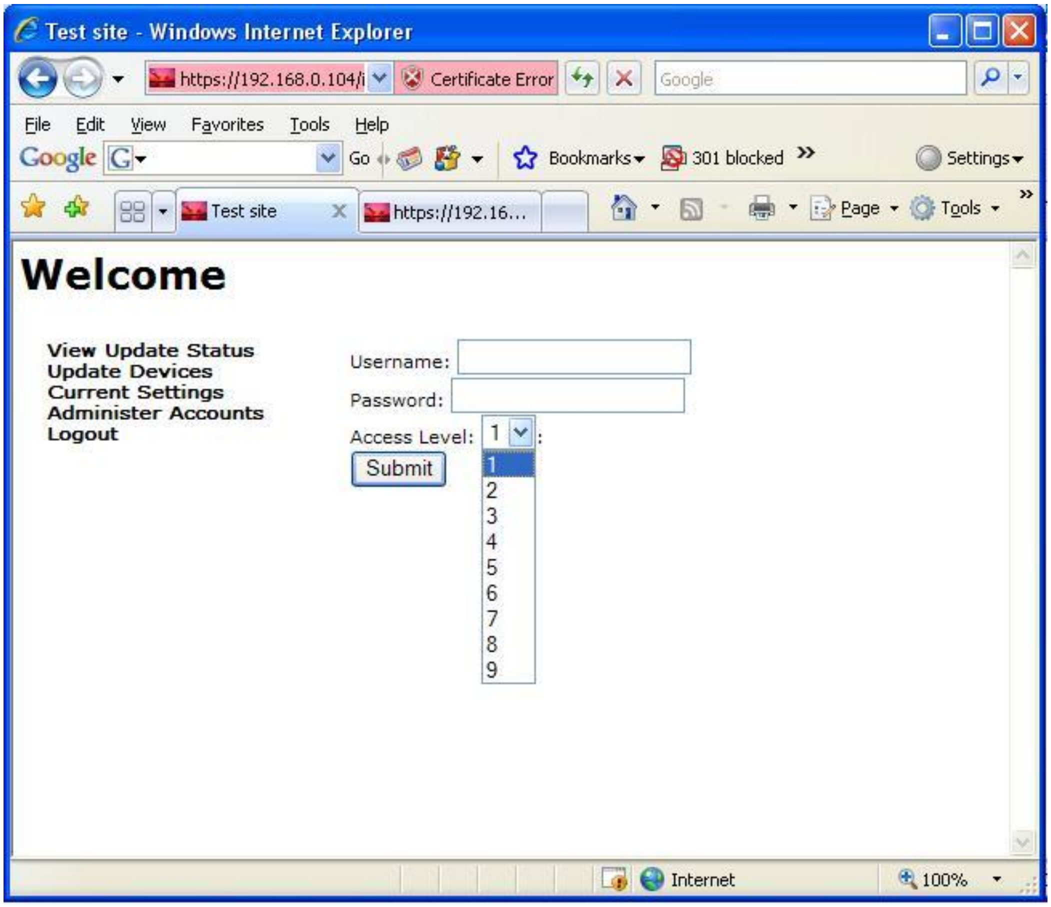
Table 4.2 Status Number Definitions.

Status Number	Definition
1	Waiting for update process.
2	Selected for update.
3	Waiting for verification.
9	Failure to update device.

A more detailed description of each step is described in Section 5.4 Server Application. The user must click the View Update Status link in the menu to view this table.

4.6 Administer Accounts Web Page

This page allows the user to create a new account for the website. It is only available for test reasons to quickly create user accounts. The user has the ability to insert a new user into the system with any username, password, and access level that he or she wants. The highest access level is assigned to this page, but in a deployed system this page should not be included at all. Write permission has to be granted to the Users database for the website so that this page can function. If an access level nine account is compromised, the user has the capability to create bogus accounts from anywhere in the world. Figure 4.11 shows the account administration web page.



Welcome

Username:

Password:

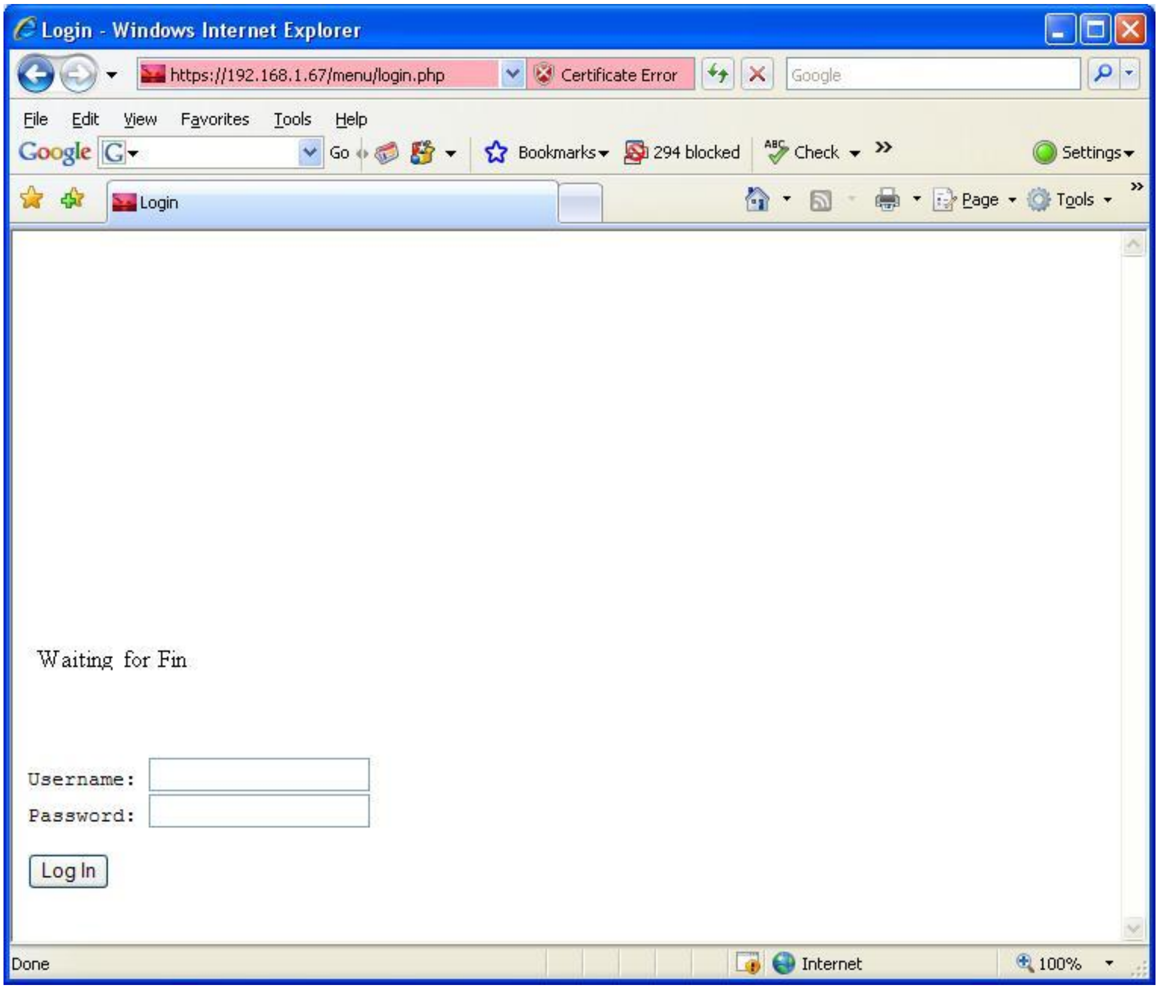
Access Level: 1 :

Figure 4.11 Account Administration Web Page.

The user must enter data in the username and password field and select an access level from the drop down box, then click the submit button. The page will then reload back at the menu page.

4.7 Logout

This page is used when a user is done working with the website. When this link is clicked the user's session information is properly cleaned up on the web server. This keeps future users of the web browser from wrongfully gaining access to the website. Once this link is clicked, the web browser will reload and display the page shown in Figure 4.12.



Waiting for Fin

Username:

Password:

Log In

Figure 4.12 Website After Logout.

4.8 Change Verification

Change verification functions as a separate security layer to verify the validity of user input. Each changed relay setting is run through a check to make sure that this number is within a range of values or a percentage of default value. These restrictions are stored in the substation database with one for every setting and relay combination. Table 4.3 is an example row from this database table.

Table 4.3 Relay Setting Restrictions.

Relay Number	Setting Name	Default Value	Percentage High	Percent Low	Value High	Value Low
1	50P1P	10	10	10	0	0

This row is read when a user attempts to change the phase A overcurrent setting (50P1P) for relay number one. The percentage high, percentage low, and default columns are used when setting restrictions are based on a percentage. In the case of this row, overcurrent values can range from nine to eleven. The value high and value low columns are used to indicate numerical limits. If a user attempts a relay setting change outside of this range, it is rejected by the system. This may reduce the damage that can be done if an account is compromised or if a user makes a typing mistake. Figure 4.11 is a flow chart showing this process.

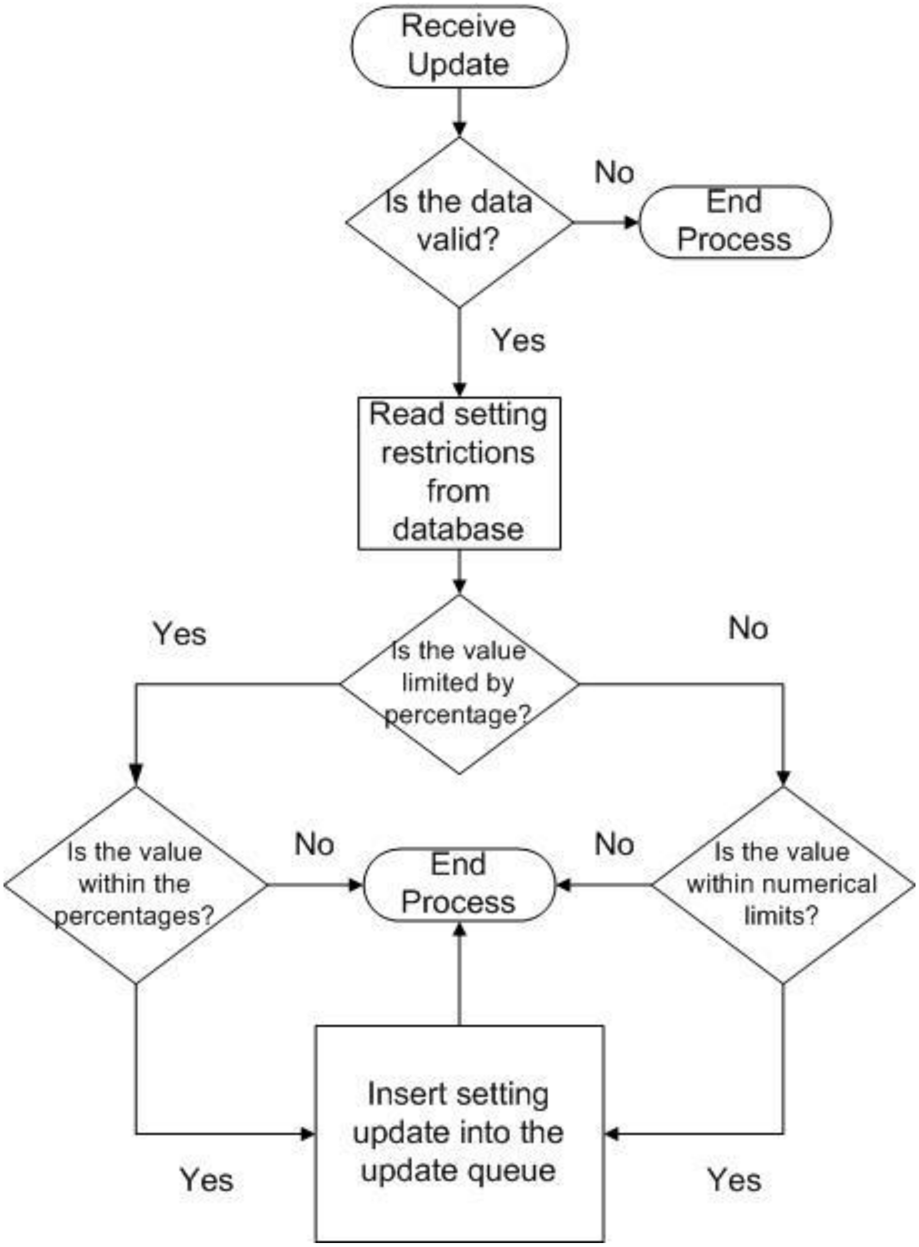

Receive Update
Is the data valid?
No
End Process
Yes
Read setting restrictions from database
Yes
Is the value limited by percentage?
No
Is the value within the percentages?
No
End Process
No
Is the value within numerical limits?
Insert setting update into the update queue
Yes
Yes

Figure 4.13 Change Verification Flowchart.

Once a change has been verified as valid, a row is written in the update list table in the substation database. The setting will not be changed until the update process is executed.

4.9 Update Process

The update process is responsible for reading relay changes from the substation database and correctly applying them to the relays. There is no user interaction for this process and it is completely separate from the website. This process is started as a scheduled task every two minutes by the operating system the website is running on. Updating the relays takes several seconds, so a separate process was made to change settings in the background. The two minute delay gives time for all of the requested changes to be made and verified. Also it gives the user an opportunity to notice a mistake and quickly change a setting back. Section 5.4 Server Application describes this process in more detail.

Chapter 5
Web-Based Relay Management System Design

5.1 Introduction

The WRMS uses a range of hardware and software products to operate. This chapter describes the components and how they work together. Appendices A and B are supplements to this chapter and contain detailed descriptions of the products and concepts used.

5.2 Web Server

The web server contains all of the code and software to provide web pages, authenticate users, change relays settings, and log website events. This machine is networked with the firewall, switch, and SEL relay as shown is Figure 5.1

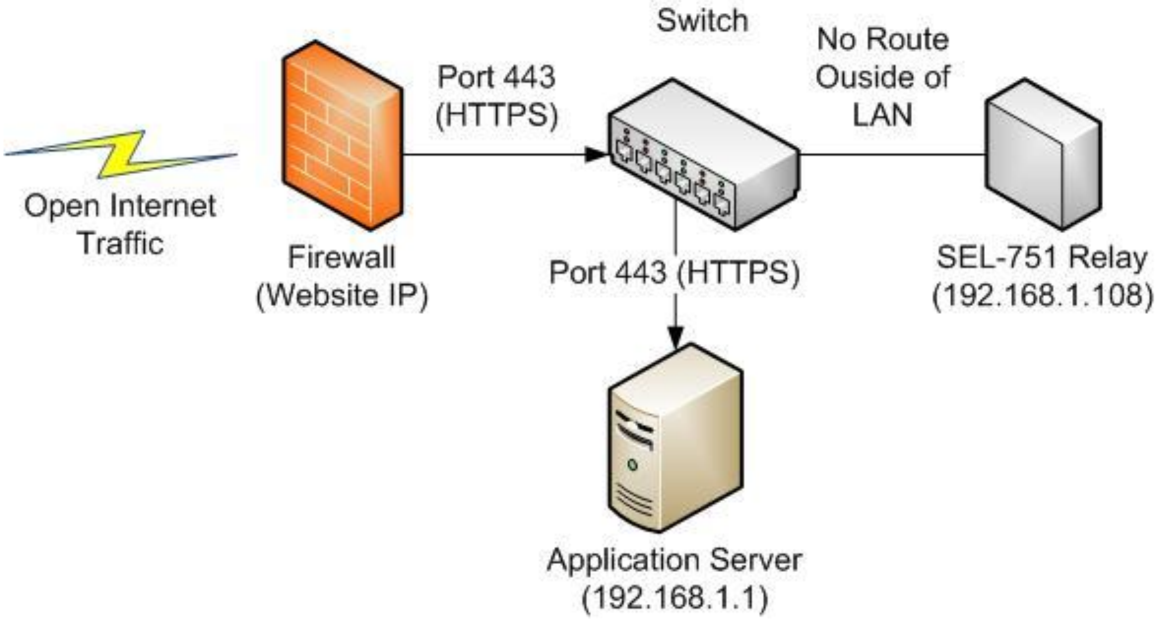


Figure 5.1 WRMS Network Diagram.

Internet traffic travels between source and destination locations across the Internet using the Internet Protocol (IP). Applications use different protocols to communicate across the Internet. In order for more than one application to communicate from a client machine, each application uses a different port number. The Internet Traffic block indicates requests from any client to any valid port. The protocol the WRMS web server uses to receive web page request is HTTPS which uses port 443. The firewall can receive requests on any port, but it only lets requests to port 443 pass through. All other requests are ignored.

CIP-5 requires the protection of an electronic security perimeter as well as access points outside of this area [21]. The firewall is used to define this perimeter. Information and systems inside of the firewall are considered cyber security assets. The firewall also helps the WRMS meet Section R2.3 of CIP-7 which requires that only necessary ports are enabled for normal and emergency operation.

The switch serves as central connection point for the firewall, Application Server, and SEL-751 Relay. Only one relay is used from the WRMS, but any number of relays can be connected as long as there are available ports. The switch is responsible for getting the correct data to the devices connected to it by using IP's to route data. IP addresses are assigned to the application server and relays. The firewall forwards all requests for web pages on port 443 to IP address 192.168.1.1 which is the web server. This request is then sent only to the Application Server (see Appendix A for hardware specifications). Once the web page request reaches the web server it is handled by the operating system (Windows XP Appendix A) and directed to Apache HTTP Server (Appendix A) which is waiting for connections on port 443. The next action is the responsibility of the web server software. Figure 5.2 shows the block diagram for the web server and its components.

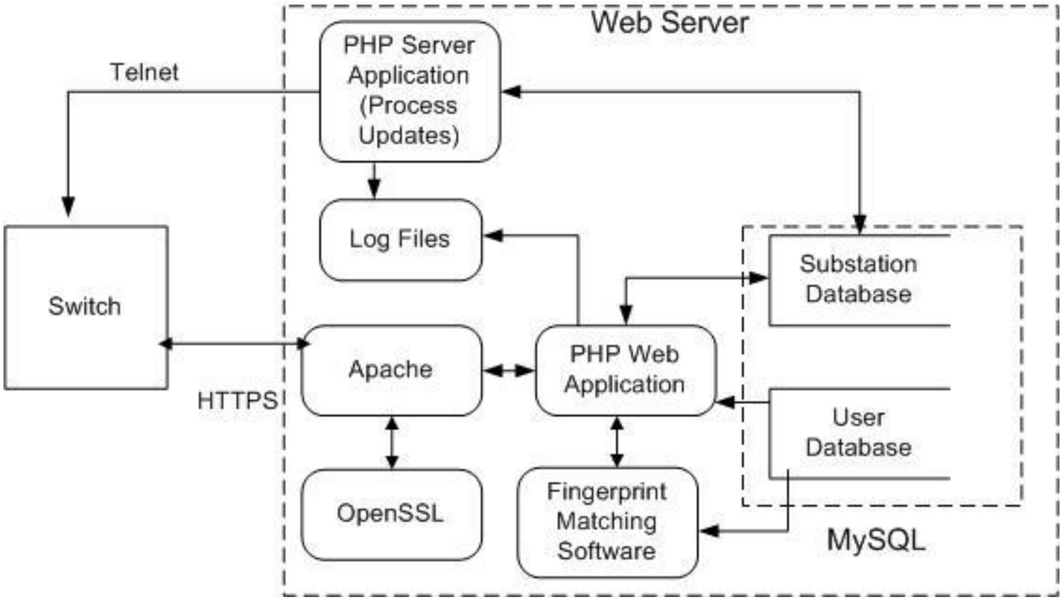


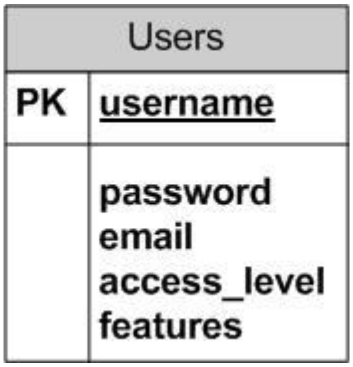
Figure 5.2 Web Server Components.

Apache is configured to only accept HTTP requests on port 443 and handles these requests as encrypted data. Using the OpenSSL plug-in (Appendix A) a secure connection is established. From this point on, all data that is transmitted between the client and server is encrypted using SHA-1 encryption. (Appendix B) and must be decrypted by OpenSSL and then passed back to Apache to be processed. Apache just receives the request and opens or executes the filename provided in the request. The PHP Web Application is a set of files that generate the web pages requested by system users, update relay settings in the database, and interface with the fingerprint matching software.

PHP is a scripting language that is commonly used to generate web pages (Appendix A). The web application uses PHP’s capabilities to interact with substation database and dynamically create the information presented to the user in the Current Settings, View Update Queue, and Update Devices web pages. The Current Settings and Account Administration pages have the capability to alter data in the substation database. The Login page access interfaces with the Users database and the fingerprint matching software.

5.2 Fingerprint Matching Software and the Users Database

The fingerprint matching software is Windows COM (Appendix B) application that is used to match users with the Griaule SDK (Software Development Kit). The version of PHP used cannot directly interface with the Griaule SDK so a wrapper application was created that could be used by PHP. Figure 5.4 shows interaction of the Login PHP script with the Users database and fingerprint matching software. Figure 5.3 is the only table in the user database.



Users	
PK	username
	password email access_level features

Figure 5.3 User Database.

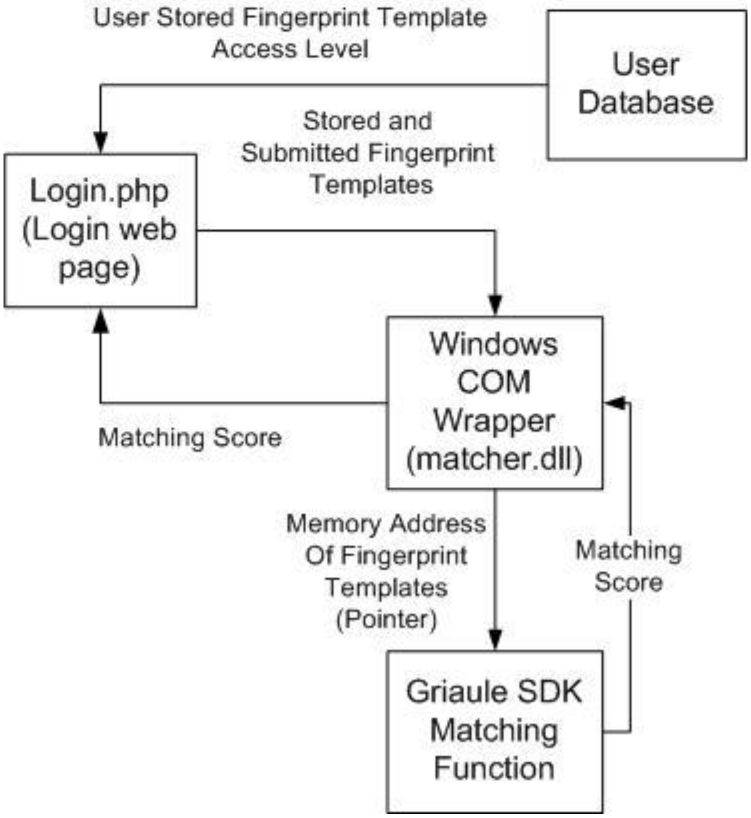

User Stored Fingerprint Template
Access Level
User Database
Stored and Submitted Fingerprint Templates
Login.php (Login web page)
Windows COM Wrapper (matcher.dll)
Matching Score
Memory Address Of Fingerprint Templates (Pointer)
Matching Score
Griaule SDK Matching Function

Figure 5.4 Login Data Flow Diagram.

Once a user submits their data to the server, login.php is executed by Apache. The user database is queried for a stored fingerprint template and access level by the submitted username and password. The database returns a template only if the username and password match values stored in the database. Next, the stored template and submitted template are passed to the Windows COM program named matcher.dll. This program then interfaces with the Griaule SDK which compares the templates and assigns a matching score. This score is passed back to matcher.dll and then back to login.php. If this score is high enough, the user is authenticated and the menu page is returned to the user.

5.3 MySQL and the Substation Database

MySQL (Appendix A) is the database program used for housing both the Substation and User databases. This section describes the data in the Substation database and the manner it is used with the Web Application and Server Application. The tables in this database are shown in the figures below.

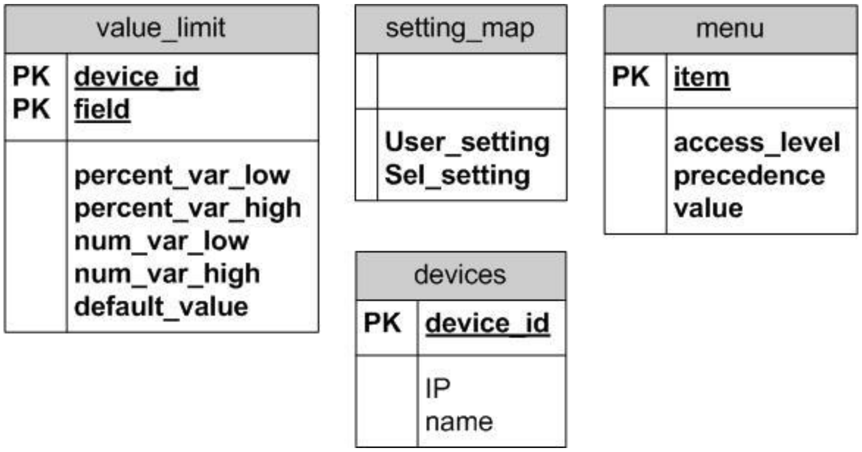


Figure 5.5 Read Only Database Tables.

The data in these tables cannot be changed by either the web or server application. The devices table contains a list of all relays along with an IP and name for each one. The IP is used to identify each relay on the network. The value limit table contains the restrictions placed on each relay (device_id) and setting (field) combination. The setting map contains a list relay settings (ex. Overcurrent A) and their corresponding name in the SEL-751 relay (ex. 50P1P). This data is used by the Server Application to build the commands that update relay settings. The menu table is used by the web application to create the menu web page. The item field contains all of the options available in the menu web page. The access level is used to control which users can access each menu item. The precedence and value field are used to format the web page. The table below shows the restrictions place by value in each table.

Table 5.1 Website Restrictions from Substation Database Tables.

Table Name	Restriction
value_limit	Limits the range of acceptable values a user can input for relay settings.
setting_map	Limits the relay settings that can be modified by the web application.
menu	Limits the website functionality available to users by their access level.

Figure 5.5 shows the remaining tables in the Substation database.

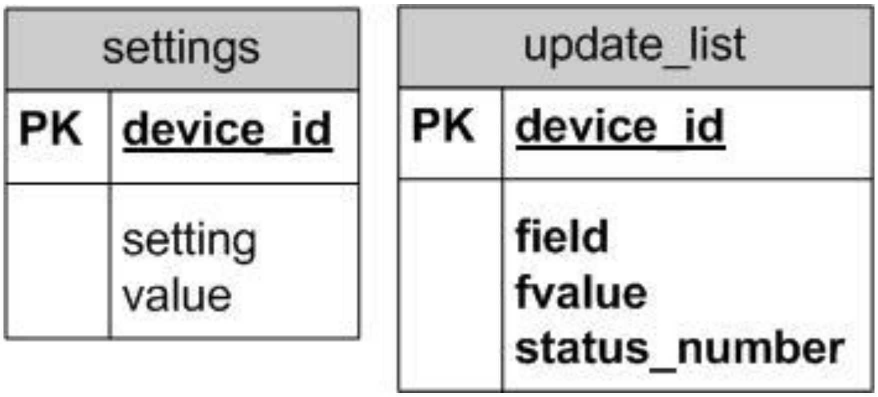


Figure 5.6 Modifiable Substation Database Tables.

The settings table stores the values for every device and setting combination in the WRMS. The update list is used as the queue for changing relay settings. Device id is the relay number, field is the relay setting name, fvalue is the new setting, and status_number is described in Table 4.2. The web application can read this data and insert new rows, while the server application can read, update, modify, and delete the data in this table. Below is a data flow diagram showing the interaction between these two tables and the web and server applications.

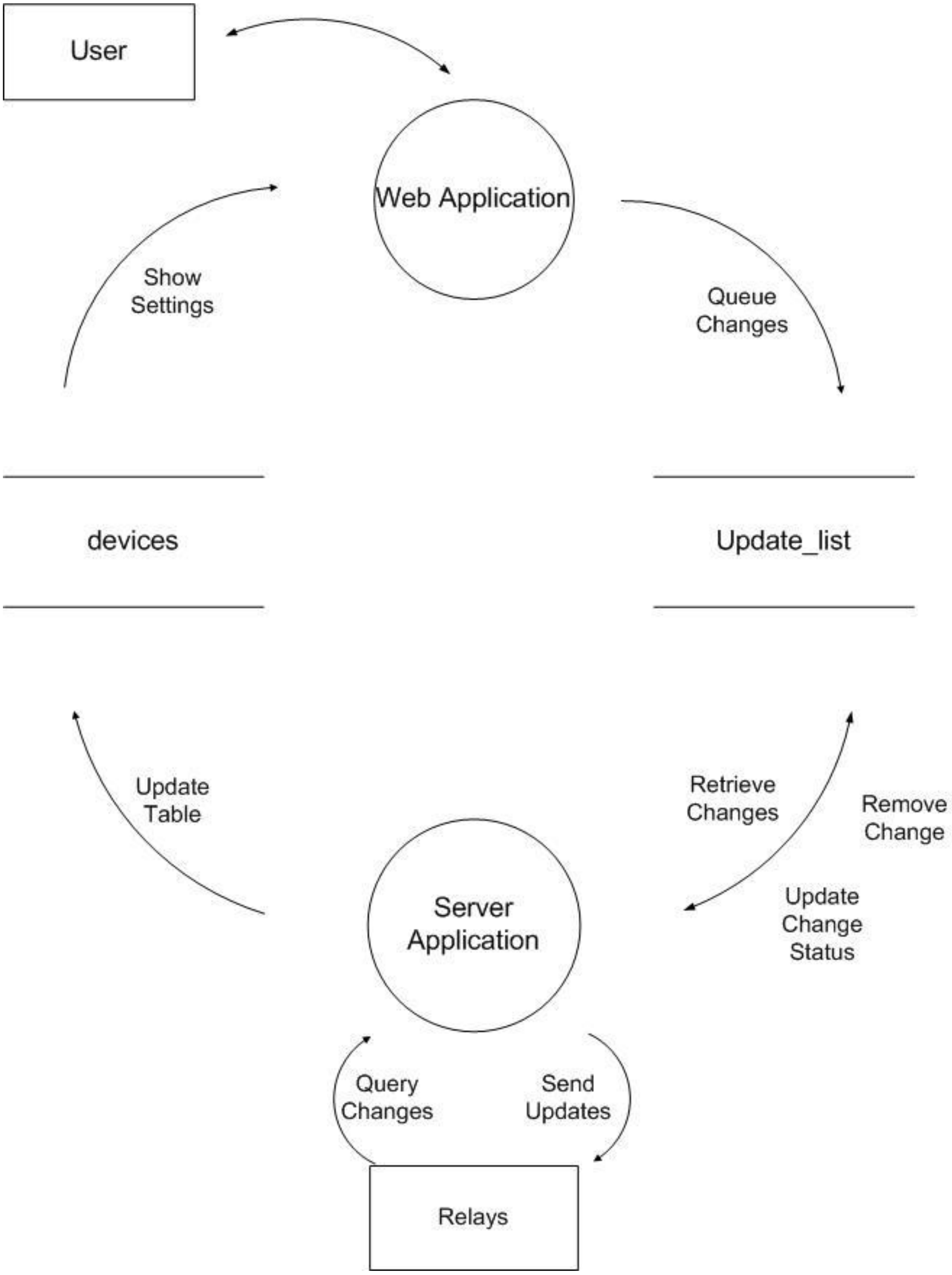


Figure 5.7 Web and Server Application Data Flow Diagram.

The process that updates the relay setting is decoupled from the web application by the devices and update_list tables. This allows the slow relay updating process to occur separate from the website which should respond quickly user input. Also the design of the website is simplified to become a database driven website.

5.4 Server Application

The server application is responsible for changing the SEL-751 relay settings according to modifications queued in the update_list table. There server application is initiated by the event scheduler on Windows XP by executing a PHP script name process_queue.php. Figure 5.8 is a flow chart showing the relay update process the server application performs.

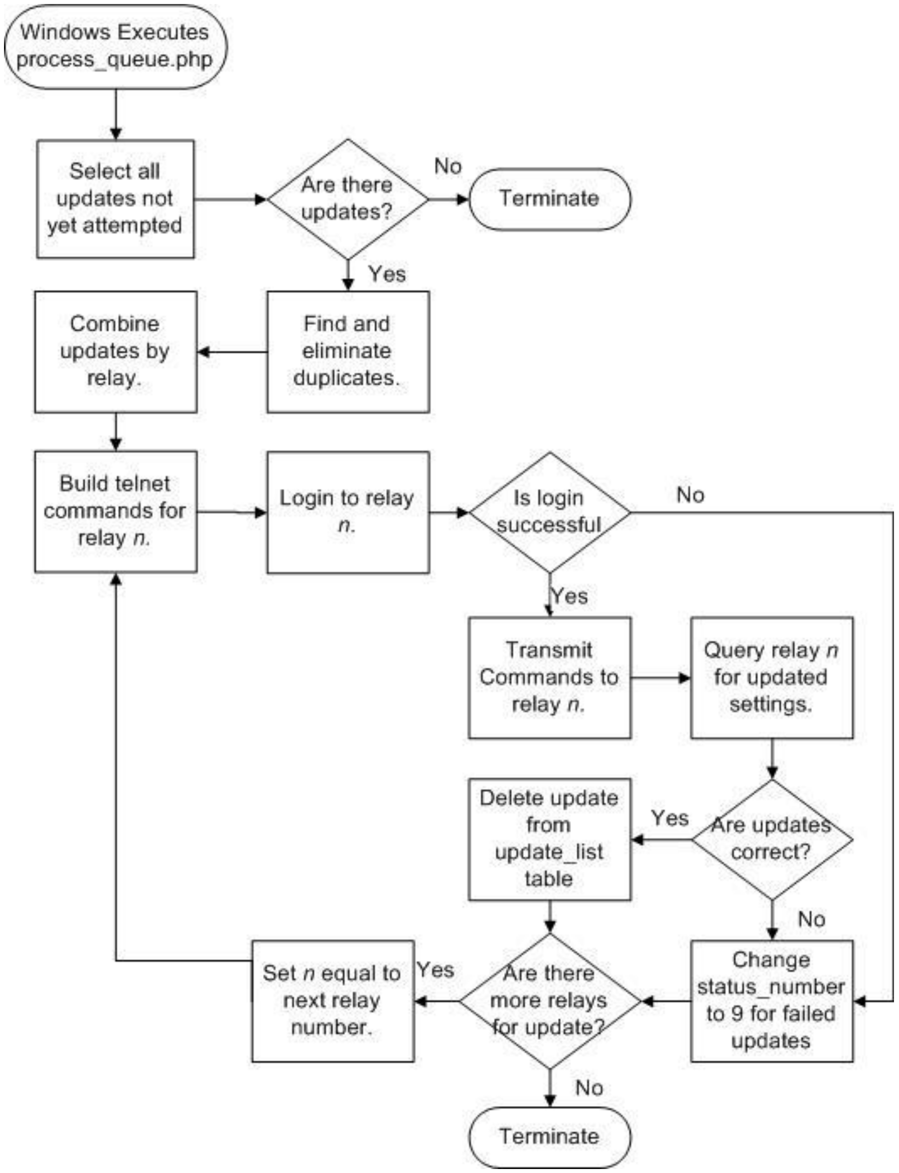

Windows Executes process_queue.php
Select all updates not yet attempted
Are there updates?
No
Terminate
Yes
Find and eliminate duplicates.
Combine updates by relay.
Build telnet commands for relay *n*.
Login to relay *n*.
Is login successful
No
Yes
Transmit Commands to relay *n*.
Query relay *n* for updated settings.
Are updates correct?
Yes
Delete update from update_list table
No
Change status_number to 9 for failed updates
Are there more relays for update?
Yes
Set *n* equal to next relay number.
No
Terminate

Figure 5.8 Application Server Flow Chart.

The server application first selects all of the untried updates from the update_list table and changes the status_number field to two for each update. Updates are then grouped with each other by the relay number. The first relay needing updates is accessed through a telnet connection (Appendix A) created by PHP. PHP then sends commands to the relay to enable setting modification to take place. Next, the commands for changing each settings are sent to the relay and status_number is updated to three for each change. Then a command to query the relay is sent and a response is returned with the new setting. The new setting is checked against each attempted change to verify that it is correct. If so, the update row is removed from update_list. The process is repeated until all relay updates have been processed. If the login fails or an update is not performed correctly, status_number is changed to nine and the server application continues until all other changes are attempted. This process can be time consuming depending on the number of changes needed. Table 5.2 contains the range of times for each action.

Table 5.2 Relay Action Response Times.

Action	Time(Seconds)
Relay Login	5
Update Setting	4
Verify Setting	4

For example, a user submits two updates for relay one and one update for relay two. There is only one login for each relay updated, so two total logins. Also, there is one update and one verify for each setting for a total of three. Assuming the times for update and verify are at the minimum of their respective ranges.

$$update\ time = (2 * 5) + \left(3 * (4 + 4)\right) = 34\ seconds$$

So, there will be a noticeable delay between relay update submission and the actual update.

5.6 System Logging

A system of logs is used to track actions performed on the website. CIP-7 section R5.1.2 requires that adequate logs are kept to create an audit trail for user accounts and actions [21]. The table below contains a list of logs and their data.

Table 5.3 Log Files.

Log Name	Data Logged
device_update.log	Records time, date, device, setting name, and user for each attempted device update by the server application. If no devices are updated then 0 updates is written to this log. If a user enters an invalid setting then it is also logged here.
access.log	Shows the time, date, source IP, and web page file name for each web page served.
user.log	Records the time, template size, pass/fail, and username from each attempted log. The logout time and username is also recorded.
error.log	Records errors from Apache and PHP. Timestamps are included.
sql.log	Records all SQL (Structured Query Language) statements performed on MySQL. Timestamps are included.

The information in these logs should be adequate to track user behavior, view the number of login attempts, asses the quality of fingerprint matches, check for SQL Injection attacks, (Section 6.3) and view relay setting changes.

5.7 Web Browser and Client Computer

This section describes the interactions that take place on the user's workstation while logging into the WRMS. The web browser is responsible for data encryption, web page viewing, web data submission, and displaying the finscan.dll ActiveX object. Figure 5.9 shows these relationships along with finscan.dll's relationship with grfinger.dll (Griaule SDK).

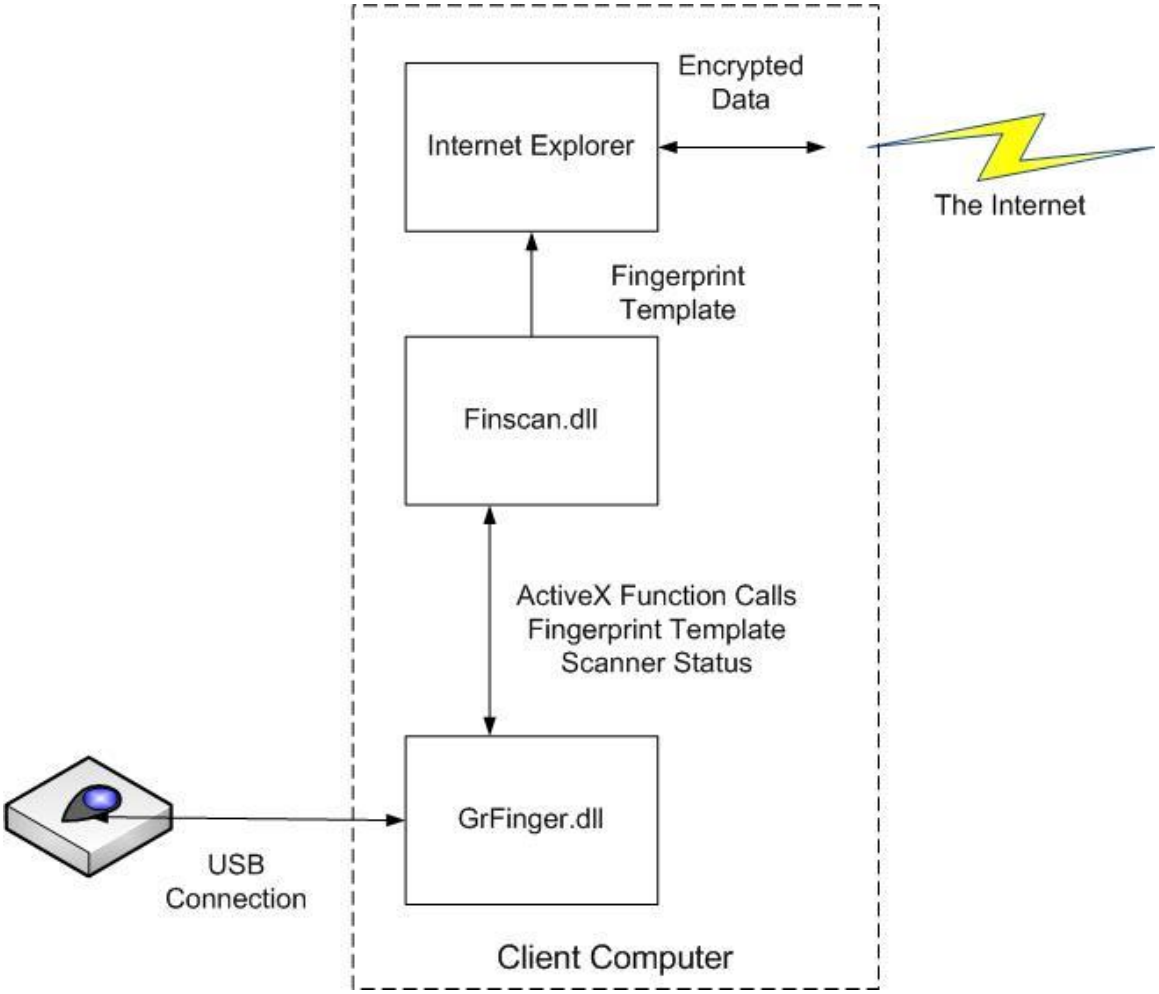


Figure 5.9 Client Computer Block Diagram.

When the login website is requested, internet explorer establishes an SSL connection with the web server. Then the web page and finscan.dll are sent to Internet Explorer. The web page loads along with finscan. Griaule SDK must be installed on the client computer for finscan to function. Finscan uses the functions in the following table to correctly capture and encode a fingerprint supplied by the user.

Table 5.4 GrFinger Function Used by Finscan [33].

Function Name	Action Performed
Initialize	Establishes a connection to the GrFinger Library.
CreateContext	Creates a context in which extraction, verification and identification may be performed.
CapInitialize	Instructs a device to capture a fingerprint.
Extract	Convert a captured image to a template.
CapRawImageToHandle	Convert a raw captured image to a Windows displayable format.
BiometricDisplay	Converts a raw captured image to Windows displayable format and includes minutiae, segment, and minutiae direction.
CapStopCapture	Stops the fingerprint capture device.
CapFinalize	Stops the capture module and frees used memory.

Figure 4.3 shows the finscan process flow but does not elaborate about the initialize scanner step. This step includes the Initialize, Create Context, and CapInitialize functions.

Chapter 6
Results and Website Vulnerability Assessment

6.1 Introduction

This chapter demonstrates the capabilities of the WRMS using two methods. The first section is a test case where a user demonstrated the capabilities of the WRMS on a relay in a test environment. The status of the relay and device are monitored while the setting is changed. The second test is a walkthrough of a top ten list of website vulnerabilities and a description of how the web application handles each one. A test of the biometric and password authentication system is not discussed since no formal testing was completed for this information. Experimental data on this subject is presented in Section 2.6 to support the strengths of the chosen authentication process. As a note, at no time during the implementation and testing of the WRMS did an invalid authentication (wrong fingerprint) cause the system to grant access.

6.1 Relay Modification Test Cases

This section outlines the tests performed to demonstrate the capabilities of the WRMS. The first test is to demonstrate the access control system while the second demonstrates the relay setting modification. Each section includes the appropriate results.

6.1.1 Access Control Test Case

1. The user accesses the WRMS login page.
2. The user supplies an incorrect password.
3. The user supplies an incorrect fingerprint.
4. The user supplies the correct password and fingerprint.

Test two and three both result in failed logs while four grants the user access. The following is the data from user.log.

```
11.10.08 08:09:26 FAILED LOGIN PASSWORD brian
11.10.08 08:10:30 FAILED LOGIN FINGERPRINT brian
11.10.08 08:17:15 Logged in User: brian Feature Size: 150
```

6.1.2 Relay Setting Modification Test Case

The following diagram shows the electrical connections made for this test.

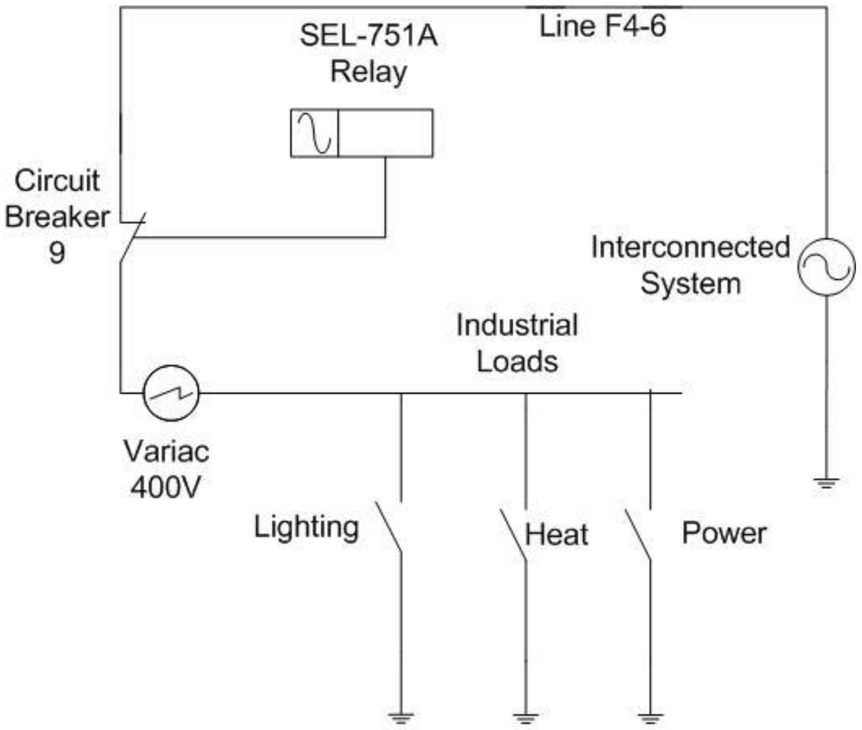


Figure 6.1 Test Case Connections.

Table 6.1 Current Draw for Industrial Loads .

Load	Current Draw
Lighting	0.8
Heat	1.3
Power	0.5

The limits for all of the overcurrent values should be set to 5A to protect the relays. The relay settings are set to the following values.

Table 6.2 Test Case Relay Settings.

Setting	Value
Overcurrent A	1.5
Overcurrent B	1.5
Overcurrent C	1.5
Time OC A	2.2
Time OC B	2.2
Time OC C	2.2
Overvoltage	1.06

Also, the relay is setup to use Time Overcurrent Curves. These curves allow the maximum current setting to be exceeded for a number of AC cycles depending on the magnitude of the overcurrent. The SEL-751A has six different curve shapes for time overcurrent. U.S. Inverse Curve with TD=4.00 is selected as the curve for this test. This curve is defined by the following equation [34]:

$$t_p = TD * (0.180 + \frac{5.95}{M^2-1})$$

$$t_p = operating\ time\ in\ seconds$$

$$TD = time\ dial\ setting$$

$$M = applied\ multiples\ of\ pickup\ current$$

The following chart shows the resulting curve.

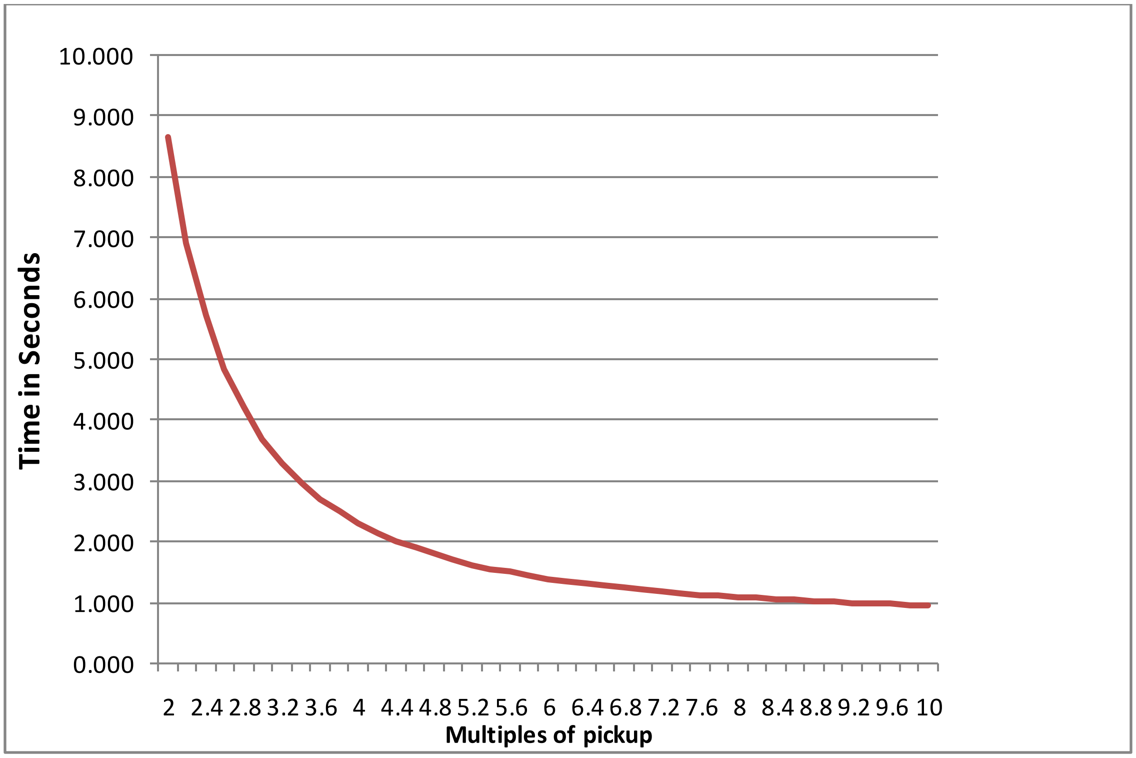


Figure 6.2 Time Overcurrent - Curve-US Inverse TD=4.

For example, a current value of 4 A would trip a breaker in 8.5 seconds if the relay is using the curve above with the time overcurrent value to 2 A.

The test case follows this list of steps.

1. Connect the Interconnect System through Line F4-6 to Substation 4 and the Industrial Regulator.
2. Adjust the regulator until the industrial distribution panel reads 400 V.
3. Attempt to Change Overcurrent A to 10 A.
4. Verify the change was not made in the relay and WRMS.
5. Add the Heat load. Observe Ia.
6. Add the Power load. Breaker 9 should trip.
7. Disconnect all loads, reset the relay, and reset the breaker.
8. Change Overcurrents A, B and C to 2.1 A in the WRMS.
9. Verify the changes are complete in the WRMS.
10. Reconnect the Heat Load. Observe Ia.

11. Add the Power Load. Observe Ia.
12. Verify the Overcurrent settings 50P1P,50P2P, and 50P3P are 2.1A
13. Change Overcurrents A, B, C to 3 A in the WRMS.
14. Change Time OC A,B and C to 1.8A in the WRMS.
15. Add the Lighting Load. Observe time and Ia.
16. Wait for breaker 9 to trip and record time.

The start time for this test is 05:41:00. The first action taken is the invalid entry attempt. The data logged for this attempt is displayed below.

```
11.10.08 05:41:59 User: brian Attempted invalid change Relay 2 Overcurrent A=10.00
```

The relay was checked and did not receive the invalid setting update.

The heat load is added at step 5 to give 1.3 A which is below the threshold of 1.5 A. Adding the power load pushes the current up to 1.8 A causing the relay to trip the breaker. After the system is reset, the relay overcurrent settings are changed to 2.1 A to accommodate more load. Below is the log information from this change.

```
11.10.08 05:50:02 Processing 3 updates.
11.10.08 05:50:06 Successfully connected to Device 2
11.10.08 05:50:08 Level 1
11.10.08 05:50:10 Level 2
11.10.08 05:50:10 Updating Field 50P1P Value=2.10
11.10.08 05:50:16 Update Command Completed Succesfully for Field 50P1P Value 2.10
11.10.08 05:50:22 Successfully completed updating Device 2 Setting 50P1P Value 2 User
Request: brian
11.10.08 05:50:25 Updating Field 50P2P Value=2.10
11.10.08 05:50:31 Update Command Completed Succesfully for Field 50P2P Value 2.10
11.10.08 05:50:37 Successfully completed updating Device 2 Setting 50P2P Value 2 User
Request: brian
11.10.08 05:50:40 Updating Field 50P3P Value=2.10
11.10.08 05:50:46 Update Command Completed Succesfully for Field 50P3P Value 2.10
11.10.08 05:50:52 Successfully completed updating Device 2 Setting 50P3P Value 2 User
Request: brian
11.10.08 05:50:55 Disconnecting from  Device 2
11.10.08 05:50:56 Completed Updating Device 2
11.10.08 05:50:56 Completed Updating Devices Exiting
```

A success message exists for 50P1P, 50P2P, and 50P3P which correspond to the Overcurrent A, B, and C settings.

Adding the power and heat loads brings the current up to 1.8 A. The breaker does not trip this time indicating the relay settings are updated. Steps 13 and 14 change all overcurrent settings to accommodate the addition of the lighting load. Below is the log data from this change.

```
11.10.08 05:54:02 Processing 6 updates.
11.10.08 05:54:06 Successfully connected to Device 2
11.10.08 05:54:08 Level 1
11.10.08 05:54:10 Level 2
11.10.08 05:54:10 Updating Field 50P1P Value=3.00
11.10.08 05:54:16 Update Command Completed Succesfully for Field 50P1P Value 3.00
11.10.08 05:54:22 Successfully completed updating Device 2 Setting 50P1P Value 3 User
Request: brian
11.10.08 05:54:25 Updating Field 50P2P Value=3.00
11.10.08 05:54:31 Update Command Completed Succesfully for Field 50P2P Value 3.00
11.10.08 05:54:37 Successfully completed updating Device 2 Setting 50P2P Value 3 User
Request: brian
11.10.08 05:54:40 Updating Field 50P3P Value=3.00
11.10.08 05:54:46 Update Command Completed Succesfully for Field 50P3P Value 3.00
11.10.08 05:54:52 Successfully completed updating Device 2 Setting 50P3P Value 3 User
Request: brian
11.10.08 05:54:55 Updating Field 51AP Value=1.80
11.10.08 05:55:01 Update Command Completed Succesfully for Field 51AP Value 1.80
11.10.08 05:55:07 Successfully completed updating Device 2 Setting 51AP Value 1 User Request:
brian
11.10.08 05:55:10 Updating Field 51BP Value=1.80
11.10.08 05:55:16 Update Command Completed Succesfully for Field 51BP Value 1.80
11.10.08 05:55:22 Successfully completed updating Device 2 Setting 51BP Value 1 User Request:
brian
11.10.08 05:55:25 Updating Field 51CP Value=1.80
11.10.08 05:55:31 Update Command Completed Succesfully for Field 51CP Value 1.80
11.10.08 05:55:37 Successfully completed updating Device 2 Setting 51CP Value 1 User
Request: brian
11.10.08 05:55:40 Disconnecting from  Device 2
11.10.08 05:55:41 Completed Updating Device 2
11.10.08 05:55:41 Completed Updating Devices Exiting
```

There is a success message for all six of the changes. The lighting load is added at 5:56:00. The current read measures 2.6 A which exceeds the time overcurrent values. The relay trips the breaker 25 seconds later. Below is the value of t_d for this setup using 2.6 A as the measured value.

$$M = \frac{measure\,current}{pickup\,current} = \frac{2.6}{1.8} = 1.44$$

$t_p = TD * (0.180 + \frac{5.95}{M^2-1})$ where TD=4

$$t_p = 22.7\ seconds$$

This value is very close to the measured time of 25 seconds. This verifies that the new time overcurrent settings are applied to the relay.

6.2 Website Vulnerability Assessment

Below is a list of the top ten Website vulnerabilities in 2007 listed by WhiteHat security [36].

Table 6.3 Top Ten Website Vulnerabilities.

1. Cross-Site Scripting.
2. Information Leakage.
3. Content Spoofing.
4. Predictable Resource Location (PRL).
5. SQL Injection.
6. Insufficient Authentication.
7. Insufficient Authorization.
8. Abuse of Functionality.
9. Directory Indexing.
10. HTTP Response Splitting.

Each of the following sections defines a vulnerability and then list the steps the WRMS takes against them, if any.

6.2.1 Cross Site Scripting

Cross site scripting (XSS) involves a web application wrongfully collecting entered data from a user. XSS is commonly disguised as links in suspicious emails. Hidden within these links is code that is sent to a web application and returned to the user. This code can redirect the user to an invalid site or even access locally stored browser information [37]. The WRMS checks all submitted data for special characters such as <,>, and % and rejects it. These are commonly used to embed tags and disguise malicious data.

6.2.2 Information Leakage

This vulnerability occurs when the web application show sensitive data such as user IP's, system software, code comments, and error codes that can help attackers find exploits to attack the system [38]. Apache is configured on the WRMS to show blank web pages for all HTML errors encountered. All connections to the MySQL database are handled with the same connection function, which returns a general error if the database is not operational revealing nothing about the database. All PHP errors are written to logs files and not web pages. The only error reported in a web page exists when an authenticated user makes an invalid change to a relay setting.

6.2.3 Content Spoofing

Content spoofing is the presentation of invalid information as a legitimate. The deployment of content spoofing is similar to XSS attacks; get a user to follow a disguised link. This link takes the user to a website that looks legitimate, but is actually a fake. The user logs in and submits data to this fake site and this data is used for identity theft and other illegal activity [36]. The WRMS uses a fingerprint scanner application (finscan.dll) which can be stolen and used by another fake website. The only defense the WRMS has against this attack is that it users need to be educated on accessing the website properly.

6.2.4 Predictable Resource Location

This vulnerability is based on web developers and administrators leaving data of any type in predictably named files that are accessible to the web server. A scanning program makes guesses about these file names and attempts to access potentially important data [36]. The web server only has the ability to read files under the WRMS path. Only the necessary files are available and all development files versions have been removed.

6.2.5 SQL Injection

SQL Injection takes advantage of Simple Query Language (SQL) to alter the response to the queries coded in the web application. If the web application does not carefully use data sent to it by a user, large amounts of data can be revealed to hackers. SQL injection attack utilizes special characters such as a “tick” to modify the intended query to return different results [36]. MySQL interprets some of these special characters and language constructs instead of just text. PHP includes a function name my_sql_real_escape_string which puts a "\" in front of all the MySQL special characters making them interpreted as text [39]. See Appendix B for an example.

6.2.6 Insufficient Authentication, Insufficient Authorization, and Abuse of Functionality

These three vulnerabilities are similar. In short, website data and functionality can become available to unauthorized users through flaws in the code of the website [36]. The WRMS is a very small website which reduces the complexity of the code. As a measure of protection, each time a page is requested, the user's access level is checked against that web page. This protects low level users from using higher security web pages such as Update Devices.

6.2.7 Directory Indexing

Directory indexing is listing of all files and folders available under a directory structure. This gives users easy access to data which would otherwise be hidden [36]. Directory indexing is disabled in Apache in the WRMS.

6.2.8 HTTP Response Splitting

This attack attempts to send an HTTP request that appear as two to the web server. The second response is under the attacker's control and can be used with other exploits to gain session access or deface web pages [36]. This vulnerability was not considered during the development of the WRMS so no special concessions were made for it. PHP 5.1.2 contains a bug fix for HTTP Response Splitting [39]. This patch is applied to the WRMS.

Chapter 7
Conclusion and Recommendations

7.1 Conclusion

The power industry is expanding current technologies such as distributed generation and pursing future concepts like the Modern Grid to meet the growing demand for cheap, reliable, and clean energy. These technologies require more advanced communications, control, monitoring to achieve these goals. The Web-Based Relay Management System provides advanced control of devices that offer little security by themselves. The following points are the main accomplishments of this system:

1. The implementation of biometric authentication through a web browser to increase the access control of the system.

2. The use of a database driven website design as a bridge between users and slower reacting devices such as relays. This makes the web interface operate quickly for a better user experience.

3. The creation of a setting update validation step to increase the security of the system by making sure the change is within an acceptable range.

4. The use of user based restrictions on the content and functionality of the website.

These highlights work together to establish a layered security approach for protecting the relay settings that are responsible for preventing equipment failure. The hope is that some of these concepts can be used to secure other critical cyber security assets.

7.2 Recommendations for Future Research and Development

1. The WRMS is designed to only exist in one substation. Utilities often utilize multiple substations. It may not be economical to administer separate User databases or even web servers in each substation. A scheme implementing the WRMS in multiply locations while reducing the administrative effort needed may be investigated.

2. The algorithm used to validate relay settings is a very simple one based on a range of acceptable values. This method was easy to implement, but no method is available to find this

range. A better validation may be a load flow analysis of the substation to assure the new relay limit does not cause problems with other devices.

Appendix A

SEL-751A

This device is a digital feeder protection relay. The relay provides a variety of over-current protections, frequency protection, breaker failure protection, under/over voltage protection, and power factor protection. This device has a front mounted user interface that allows complete control of settings from the device's physical locations. The 751A also has a selection of communications ports including EIA-232, Ethernet, and fiber-optic ports on the rear panel. This device supports TCP/IP, Ethernet FTP, Telnet, and DeviceNet [34].

Firewall and Switch

The firewall and switch used for demonstration and development of the WRMS is a D-Link 624 router. It has four 10/100 Mb/s Ethernet LAN Ports and a 10/100 Mb/s Ethernet WAN port. The firewall is a static packet filter firewall indicating that it only has the capability to operate on the network layer. This firewall can only accept or deny packets based on source and destination IP's and ports [40]. The D-Link also supports port forwarding which is setup to send port 443 traffic to the web server IP.

Application Server

This server is a Compaq Presario Model R3000 Laptop Computer with Windows XP Home Edition installed. The following is a list of hardware components.

Intel Pentium 4 2.66 GHz Processor

512 MB DDR RAM

40 GB IDE HDD

10/100 Mb/s Ethernet Port

Open SSL

OpenSSL is a free implementation of the SSL protocol. SSL is a key component in secure web applications because of the encryption it provides for traffic on public networks. OpenSSL supports Windows, Linux, BSD, and other OSs. OpenSSL is responsible for the encryption and decryption of the information passed between the web browser and application server. It is configured with the Apache HTTP Server and is fully supported by modern web browsers. SSL is transparent to the other aspects of this project since they either handle data before they are encrypted or after they are decrypted [41].

Windows XP

Windows XP is the operating system installed on the Web Server. The Griaule SDK supports Windows XP making it a good choice for the operating system of the Web Server [33]. Window XP also supports task scheduling which is a necessary for the Server Application to operate. The install of XP was fully patched prior to and during development of the WRMS.

MySQL Server

MySQL is a relational database management system. The program runs as a Windows XP service and provides multi-user access to databases. The MySQL Server is available as free software under the GNU General Public License. It provides the features necessary to serve as a back-end for the WRMS. The MySQL Server allows for installation of only the necessary database components, thereby keeping the amount of storage needed to a minimum. Eliminating unnecessary features reduces the potential entry points for exploitation.

MySQL server is the most commonly used database software in web environments. Open source web server and scripting languages have been developed to support MySQL server. This significantly eases the setup and maintenance of systems deploying MySQL server [42].

PHP

PHP is a commonly used web scripting language and is available for free. It has built in support for sessions, hashing (for password protection), MySQL database connectivity, telnet (telecommunications network), and Win32 calls. PHP also has predefined functions for cleaning HTML input fields before introducing data to database queries [39]. All of these features make it an excellent choice for developing the WRMS.

Internet Explorer 7.0

The WRMS uses a username, password, and fingerprint to grant users access to its features. Fingerprint scanning cannot be performed by web browsers directly, so a browser plug-in must be used. Internet Explorer 7 supports ActiveX plugins which can be built to interface with a fingerprint scanner. This browser also supports SSL (Secure Socketss Layer) v2.0 which is required to safely transmit data to the web server.

Griaule SDK (GrFinger.dll)

The Griaule SDK provide the fingerprint scanning, encoding, and matching functionality needed for user authentication in the WRMS system. This SDK supports the U.are.U 4000B Fingerprint Reader used for this project [33].

U.are.U 4000B Fingerprint Reader

This device is a USB optical fingerprint reader. It offers a list of security features that include fingerprint encryption, latent fingerprint rejection, and counterfeit finger rejections. The scans from this device are recorded at 512 dots per inch (dpi) and are 8-bit grayscale. The operating temperature for this device is 0-40 degrees Celsius which is well beyond the range found in office and home environments where users are likely to use this product [43].

Appendix B

Web Sessions

Web sessions are used to store information about a user on the web server. On the user’s machine a cookie is created which stores a session id (SID). On the web server a file is created and named by the SID. This file contains all the variables used by the website to interact with the user. The WRMS stores the username and access level of the user. This allows the user to operate the website without having to login each time a new page is accessed. When a webpage is requested, the user’s SID is sent to the web server and matched up with the session file which identifies the user.

SQL Injection Example

Below is an example of a query that could be used for a web login page.

SELECT username FROM users WHERE password=‘letmein’;

Letmein is a text field that comes from the login page submission. With the current values, this query will execute as designed. A SQL injection attack could take advantage of this query to give different results. Below is an example of the same query, but with the password *dontknow’ OR ‘p’=’p*.

SELECT username FROM users WHERE password=’dontknow’ OR ‘p’=’p’

There are now two conditional statements in this query instead of just the one that it was designed to have. The first one is just a guess by the attacker and will likely not be true. The attacker then inserts a “tick” or ‘ to close the text field *‘dontknow’* and adds a second conditional of the type OR. This indicates that either condition can be true for the query to return data. The second condition is always true. Now the query will return a list of all usernames in the *users* table. Below is the same hacked query and password, only now the password has been passed through the PHP function *my_sql_real_escape_string*.

SELECT username FROM users WHERE password=’dontknow\’ OR \‘p\’=\’p’

The “\” forces the next character to be interpreted as text. Now the password field contains all of the data after the “=” including the OR and second conditional statement. This will return nothing unless the password matches the SQL injection attack.

Telnet

Telnet is a bi-directional communications protocol that uses the ASCII character set. It is used primarily as a remote terminal protocol [44]. The SEL 751A supports telnet and this protocol is used in the WRMS to communicate update and query commands. This protocol does not use any encryption, so it is not safe to connect directly to the relays remotely.

HTTP Request

An HTTP request is a specially formatted text message that is sent to web servers to request a web page. An HTTP request for www.google.com would look like.

```
GET / HTTP/1.1
host: www.google.com
```

The “GET /” tells the web server to retrieve the information at the root of the website. HTTP/1.1 is the HTTP version that the request conforms to and host shows the hostname of the request’s destination [45].

The GET option can also be used to pass information in a Uniform Resource Locator (URL). For example, the following path shows the URL used by the WRMS.

https://192.168.1.67/index.php?page=up

The browser sends the following request.

```
GET /index.php?page=up HTTP/1.1
host: 192.168.1.67
```

PHP reads the URL above and uses the information after the “?” as the variable $_GET[‘page’]=up. This variable is used by PHP to select the Update Devices web page as a response. This is more secure than using the full URL below.

https://192.168.1.67/menu/Update%20Devices.php

The method used by WRMS hides the directory structure of the website.

HTTP POST’s are also used to transmit data from the browser to the web server. This is commonly used to submit form data such as the Update Devices page. The following is an example of an HTTP POST by the WRMS.

```
POST /index.php?page=up HTTP1.1
Host: 192.168.1.67
Content-Length: 8
Content-Type: text/plain
device=1
```

PHP receives this HTTP request and creates the variable $_POST[‘device’]=1 which is used to determine the device number to edit. The Login and Update Device web pages transmit information to the web server this way.

Secure Sockets Layer (SSL)

SSL is commonly used by E-commerce sites to create an encrypted connection from website to remote connections. A certificate is distributed to remote users upon connection indicating the validity of the website. This certificate contains a public key that is used by the web browser for encryption and decryption, while the server keeps a private key for the same reason. This encrypted connection protects the data passed between the client and server [41].

SHA-1

SHA-1 stands for US Secure Hash Algorithm 1. This is the encryption algorithm used by OpenSSL to secure the data that the WRMS transmits. It is currently known to take 2^69 (5.9 *10^21) steps to break SHA-1. There are currently more secure encryption algorithms such as SHA-256 [46].

ActiveX and Windows COM

COM stands for Component Object Model. COM is a Windows feature that allows pieces software to communicate in a standard manner. ActiveX is subset of COM for the web [47]. PHP supports this standard connection to COM objects which allows it to communicate with the Griaule SDK.

List of Abbreviations

AEPR – Alarm and event processing

ATM – Automatic teller machine

CEI – Computer Economic Incorporated

CIP – Critical Infrastructure Protection

DDOS – Distributed denial of service

DG – Distributed generator

DOE – US Department of Energy

DOS – Denial of service

DPI – Dots per inch

EMS – Energy management system

FERC – Federal Energy Reliability Council

FMR – False match rate

HTTP – Hypertext transport protocol

HTTPS – Secure hypertext transport protocol

ICS – Industrial control system

IT – Information technology

NERC – North American Reliability Council

NIST – National Institute of Standards and Technology

PIN – Personal identification number

RTU – Remote terminal unit

SCADA – Supervisory control and data acquisition

SDK – Software development kit

SEL – Schweitzer Engineering Laboratory

SHA – Secure hashing algorithm

SID – Session id

SQL – Simple query language

SSL – Secure sockets layer

URL – Uniform resource locator

USB – Universal serial bus

WRMS – Web-base relay management system

XSS – Cross site scripting

Bibliography

[1] "IDC: antivirus market growth will continue," WHIR News Website, Sept. 2, 2003, [Online]. Available: http://www.thewhir.com/marketwatch/idc090203.cfm. [Accessed Nov 5, 2008].

[2] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," *Congressional Research Service*, Apr. 1, 2004 [Online]. Available: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf. [Accessed Oct. 27, 2008].

[3] R. Richardson, "2008 CSI computer crime and security survey," *Computer Security Institute,* [Online]. Available: http://www.gocsi.com. [Accessed Oct. 17, 2008].

[4] B. Krebs, "A short history of computer viruses and attacks," *The Washington Post,* Feb. 15, 2003. [Online]. Available: http://www.washingtonpost.com/wp-dyn/articles/A50636-2002Jun26.html. [Accessed Oct. 20, 2008].

[5] T. G. Lewis, *Critical Infrastructure Protection in Homeland Security.* Hoboken, NJ: Wiley, 2006.

[6] M. McDowell, "Cyber security tip ST04-015 understanding denial-of-service attacks," *US-CERT,* Aug. 1, 2007. [Online]. Available: http://www.us-cert.gov/cas/tips/ST04-015.html. [Accessed Oct 24, 2008].

[7] D. Abel and J. Abelson, "11 charged with massive id theft," *The Boston Globe,* Aug. 6, 2008, [Online]. Available: http://www.boston.com/business/articles/2008/08/06/11_charged_with_massive_id_theft/. [Accessed Oct. 24, 2008].

[8] R. Mangalamra, "List of world best top hackers of all time," *Zimbio,* Jan. 24, 2008. [Online]. Available: http://www.zimbio.com/Hacking+Resources/articles/9/List+World+Best+Top+Hackers+Time.[Accessed Oct 24, 2008].

[9] "UK teen avoids jail for nuclear hacking," *ZDNET Australia,* Feb. 4, 2004, [Online]. Available: http://www.zdnet.com.au. [Accessed Oct 26, 2008].

[10] A. Greenburg, "America's hackable backbone," *Forbes,* Aug. 22 2007. [Online]. Available: http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html. [Accessed Oct 18, 2008].

[11] "Technical analysis of the August 14, 2003, blackout: what happened, why, and what did we learn," *NERC*, July 13, 2004. [Online]. Available: http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf. [Accessed Oct. 23, 2008].

[12] G. N. Erricson and A. Torkilseng, "Management of information security for an electric power utility-on security domains and use of ISO/IEC17799 standard," *IEEE Trans. On Power Delivery,* vol 20, no. 2, Apr. 2005. [Online] Available: http://ieeexplore.ieee.org. [Accessed Oct. 29, 2008].

[13] K. Barnes and B. Johnson, "Introduction to SCADA protection and vulnerabilities," *Idaho National Engineering and Environmental Laboratory,* Mar. 2004, [Online]. Available: http://www.inl.gov/technicalpublications/Documents/3310860.pdf. [Accessed Oct. 27, 2008].

[14] "Transformers and switchgear: where is it all going", *power-technology.com,* Aug. 27, 2008, [Online]. Available: http://www.power-technology.com/features/feature40480/. [Accessed Oct 20, 2008].

[15] "Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations," *NERC,* Apr. 2004, [Online]. Available: https://reports.energy.gov/BlackoutFinal-Web.pdf. [Accessed Oct 23, 2008].

[16] K. H. LaCommare and J. J Eto, "Understanding the cost of power interruptions to U.S. electricity consumers," *Ernest Orlando Lawrence Berkeley National Laboratory,* Sept. 2004, Available: http://certs.lbl.gov/pdf/55718.pdf. [Accessed Oct 22, 2008].

[17] "The value of energy when it is not available," *The National Renewable Energy Laboratory,* May 2003, [Online]. Available: http://www.netl.doe.gov/moderngrid/. [Accessed Nov. 3 2008].

[18] Federal Energy Regulatory Commission, "What FERC does," *Federal Energy Regulatory Commission,* July 31, 2008, [Online]. Available: http://www.ferc.gov. [Accessed Oct. 23, 2008].

[19] North America Electric Reliability Corporation, "Company overview," *North America Electric Reliability Corporation*, [Online]. Available: http://www.nerc.com. [Accessed Oct. 23, 2008].

[20] Federal Energy Regulatory Commission, "FERC approves new reliability standards for cyber security," *Federal Energy Regulatory Commission*, Jan. 17, 2008. [Online].

Available: http://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp. [Access Oct. 23 2008].

[21] North America Electric Reliability Corporation, “Reliability Standards for the Bulk Electric Systems of North America,” *North America Electric Reliability Corporation*, July 21, 2008, [Online]. Available: http://www.nerc.com/files/Reliability_Standards_Complete_Set_21Jul08.pdf. [Accessed Oct. 24, 2008].

[22] U.S Department of Energy, “Electric power,” *U.S Department of Energy*, [Online]. Available: http://www.energy.gov/energysources/electricpower.htm. [Accessed Oct. 23 2008].

[23] Energetics Incorporated, “Roadmap to secure control systems in the energy sector,” *U.S Department of Energy*, Jan. 2006, [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/Roadmap_to_Secure_Control_Systems_in_the_Energy_Sector.pdf. [Accessed Oct. 25, 2008].

[24] K. Stouffer, J. Falco, K. Scarfone, “Guide to inductrial control systems (ICS) security,” *National Institute of Standards and Technology*, Sept 2008, [Online] Available: http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf. [Accessed Oct 25, 2008].

[25] A. Singal, T. Winograd, and K. Scarfone, “Guide to secure web services,” *National Institute of Standards and Technology*, Aug 2007, [Online] Available: http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf. [Accessed Oct 25, 2008].

[26] J. Chirillo and S. Blaul, *Implementing Biometric Security*, Indianapolis, IN: Wiley 2003.

[27] B. Schneier, “Biometrics: uses and abuses,” *schneier.com*, Aug 1999. [Online]. Available: http://www.schneier.com/essay-019.html. [Accessed Oct. 16, 2008].

[28] L. O’Gorman, “Comparing passwords, tokens, and biometrics for authentication,” *Proceeding of the IEEE*. Vol. 91, No. 12, Dec. 2003. [Online]. Available: http://ieeexplore.ieee.org. [Accessed Oct. 16, 2008].

[29] K. Barnes and B. Johnson, “Introduction to SCADA protection and vulnerabilities,” *Idaho National Engineering and Environmental Laboratory*, Mar. 2004, [Online]. Available: http://www.inl.gov/technicalpublications/Documents/3310860.pdf. [Accessed Oct. 27, 2008].

[30] Congressional Budget Office, “Prospects for distributed electricity generation,” *Congressional Budget Office,* Sept. 2003, [Online]. Available: http://www.cbo.gov/doc.cfm?index=4552. [Accessed Oct. 6, 2008].

[31] F. Katiraei and M.R. Iranani, “Power management strategies for a Microgrid with multiple distributed generation units,” *IEEE Trans. On Power Systems,* Vol. 21, No. 4, Nov. 2006, [Online], Available: http://ieeexplore.ieee.org. [Accessed Oct. 31, 2008].

[32] “Fingerprint,” *Forensic Fact Website,* Mar. 31, 2008, [Online]. Available: http://forensicfact.wordpress.com/2008/02/01/finger-printing/finger-print/. [Accessed Nov. 1, 2008].

[33] “GrFinger 4.2 developers manual,” *Griaule,* 2006, [Online] Available: http://www.griaulebiometrics.com. [Accessed May 2006].

[34] Schweitzer Engineering Laboratories, *SEL 751A Instruction Manual,* Aug. 6, 2008.

[35] A. K. Jain, S. Prabhakar, and A. Ross, “Biometrics-based web access,” *Homepage of Arun Ross,* [Online]. Available: http://www.csee.wvu.edu/~ross/pubs/RossWebAccess_MSUTR98-33.pdf. [Accessed Apr. 14, 2008].

[36] J. Grossman, “WhiteHat website security statistics report,” *WhiteHat Security,* Oct. 2007, [Online] Available: http://www.whitehatsec.com/home/assets/WPStatsreport_100107.pdf. [Accessed Nov. 3, 2008].

[37] R. C. Barnett, “Mitigating the WASC web security threat classification with apache,” in *Preventing Web Attacks with Apache,* Addison-Wesley, 2006, pp. 181-254.

[38] “Information leakage,” *Web Application Security Consortium,* [Online]. Available: http://www.webappsec.org/projects/threat/classes/information_leakage.shtml. [Accessed Nov. 3, 20].

[39] *PHP: Hypertext Processor Website,* [Online]. Available: http://us3.php.net/ [Accessed Nov. 3, 2008].

[40] H. F. Tipton and M. Krause, *Information Security Management Handbook,* 5th ed., vol. 2, Boca Raton, FL: CRC Press, 2003.

[41] *OpenSSL Website,* [Online]. Available: http://www.openssl.org/ [Accessed Nov. 3, 2008].

[42] *MySQL Website,* [Online]. Available http://www.mysql.com/ [Accessed Nov. 3, 2008].

[43] "U.are.U 4000B reader," *Digital Persona Website*, 2005, [Online]. Available: http://www.digitalpersona.com/resources/downloads/4000BReader10-05.pdf. [Accessed Nov. 3, 2008].

[44] J. Postel and J. Reynolds, *Telnet Protocol Specification*, RFC 854, May 1983, [Online]. Available: http://www.faqs.org/rfcs/rfc854.html. [Accessed Nov 3, 2008].

[45] "HTTP/1.1: Request," *W3.org Website*, [Online]. Available: http://www.w3.org/Protocols/rfc2616/rfc2616-sec5.html. [Accessed Nov. 6, 2008].

[46] P. Zimmerman, "SHA-1 broken," *FileCryptSDK Website*, [Online]. Available: http://www.filecryptsdk.com/content/view/17/33/. [Accessed Nov. 3, 2008].

[47] "COM: component object model technologies," *Microsoft Website*, [Online]. Available: http://www.microsoft.com/com/default.mspx. [Accessed Nov. 5, 2008].

[48] J. L. Blackburn and T. J. Domin, *Protective Relaying Principles and Applications*, 3rd Ed., Boca Raton, FL: CRC Press, 2007.

[49] "The smart grid: an introduction," *US Department of Energy Website*, [Online]. Available: http://www.oe.energy.gov/1165.htm. [Accessed Nov 3, 2008].