CYBER SECURITY IN POWER SYSTEMS

A Thesis
Presented to
The Academic Faculty

by

Venkatraman Sridharan

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

Georgia Institute of Technology
May 2012

Approved by:

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

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

Dr. Henry Owen
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: 03/27/2012

To the students of the Georgia Institute of Technology

ACKNOWLEDGEMENTS

I would like to thank my research advisor Dr. John Copeland and Dr. Sakis Meliopoulous for providing me the opportunity to work with them and providing me research guidance. I could not even think of starting to work on my Masters thesis without their support and encouragements. I would also like to thank Dr. Henry Owen for being a part of my reading committee and for offering his valuable time on this.

I would like to thank NEETRAC and GTRI for offering me the opportunity to work with them on this project, and it has been a great learning experience ever since the beginning, and it has been a treat to meet so many different people from different backgrounds to offer their perspective on this research. I also thank all the members of the CSC lab for allowing me to work with them and share ideas and thoughts on improving the research work and learning the value of research work.

I wish to specially thank my mother, father, and my brother, without whose guidance I would have never even been able to do my graduate studies, and I thank them for their endless support, encouragement, and patience. I am eternally grateful.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

SCADA	Supervisory Control and Data Acquisition Systems
PLA	Programmable Logic Array
NIST	National Institute of Standards and Technology
DHS	Department of Homeland Security
DOE	Department of Energy
FERC	Federal Energy Regulatory Commission
NERC	North American Electric Reliability Corporation
CIP	Critical Infrastructure Protection
ISID	Industrial Security Incident Database
IED	Intelligent Electronic Device
DOS	Denial of Service
DFR	Digital Fault Recorder
PDU	Protocol Data Unit
SNMP	Simple Network Management Protocol
GE	General Electric
SEL	Schweitzer Engineering Laboratories
AES	Advanced Encryption System
RTU	Remote Terminal Unit
IEC	International Electro technical Commission
DNP	Distributed Network Protocol
PCS	Personal Communications Service
ISS	Internet Security Systems

SUMMARY

Many automation and power control systems are integrated into the 'Smart Grid' concept for efficiently managing and delivering electric power. This integrated approach created several challenges that need to be taken into consideration such as cyber security issues, information sharing, and regulatory compliance. There are several issues that need to be addressed in the area of cyber security. Currently, there are no metrics for evaluating cyber security and methodologies to detect cyber attacks are in their infancy. There is a perceived lack of security built into the smart grid systems, but there is no mechanism for information sharing on cyber security incidents. In this thesis, we discuss the vulnerabilities in power system devices, and present ideas and a proposal towards multiple-threat system intrusion detection. We propose to test the multiple-threat methods for cyber security monitoring on a multi-laboratory test bed, and aid the development of a SCADA test bed, to be constructed on the Georgia Tech Campus.

CHAPTER 1

INTRODUCTION

1.1 Background

Cyber Infrastructure refers to information and communications systems and services, which are composed of all hardware and software, that process, store, and communicate information, or any combination of all of these elements. The development of Smart Grids replacing the conventional power grids is envisioned as being great step for energy independence, global warming and emergency requirements. They use an intelligent two-way digital communication for monitoring and controlling the devices.

The Smart Grid plays an important role in responding to many conditions in supply and smart energy demand and can save over billions of dollars over the next 20 years, and this might be crucial to the economy of a country. The U.S. Government proposed that all critical infrastructure companies need to meet new cyber security standards and grant the president emergency powers over control of the grid systems and other infrastructure.

SCADA systems lie at the heart of power utility control networks. The devices allow utilities such as power plants, to remotely control and monitor power generation devices and substations over phone lines, radio links and, IP networks.

There have been IT-infrastructure failures in the past. All the failures were not due to any terrorist or Internet hacker attack; the failures were also because of unexpected mistakes,

poor design, and lack of a proper alert mechanism. Therefore, inadvertent compromises must also be addressed, and the focus must be an all-hazards approach. Figure 1 shows a general characterization of failure in an IT infrastructure based on source of failure.

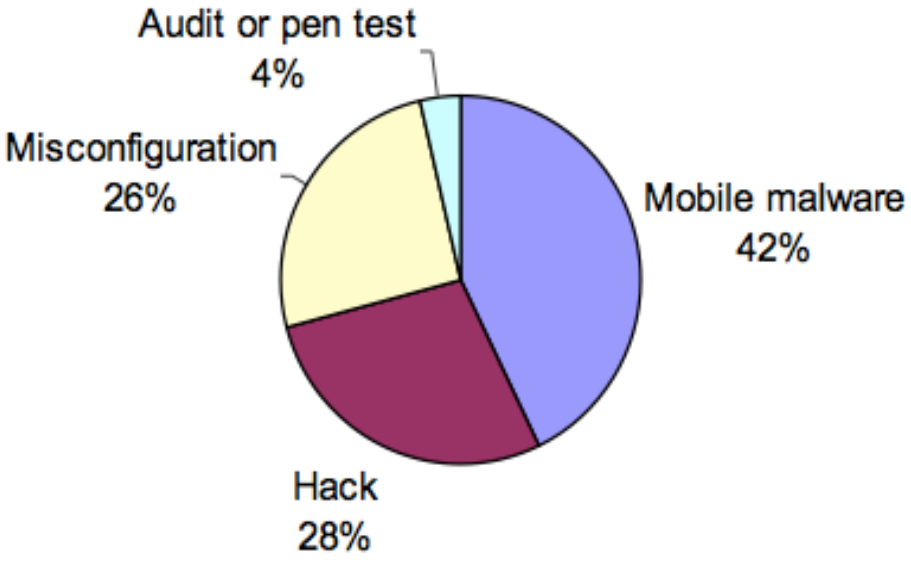

Figure 1: Pie Chart illustrating the percentage of incidents [6]

In an effort to obtain an accurate breakdown of the perpetrators background, the incidents were categorized as coming from malware authors, current employees, hackers, software vendors, former employees, current contractors, agents of foreign nations, competitors, and unknowns. This is shown in Figure 2.

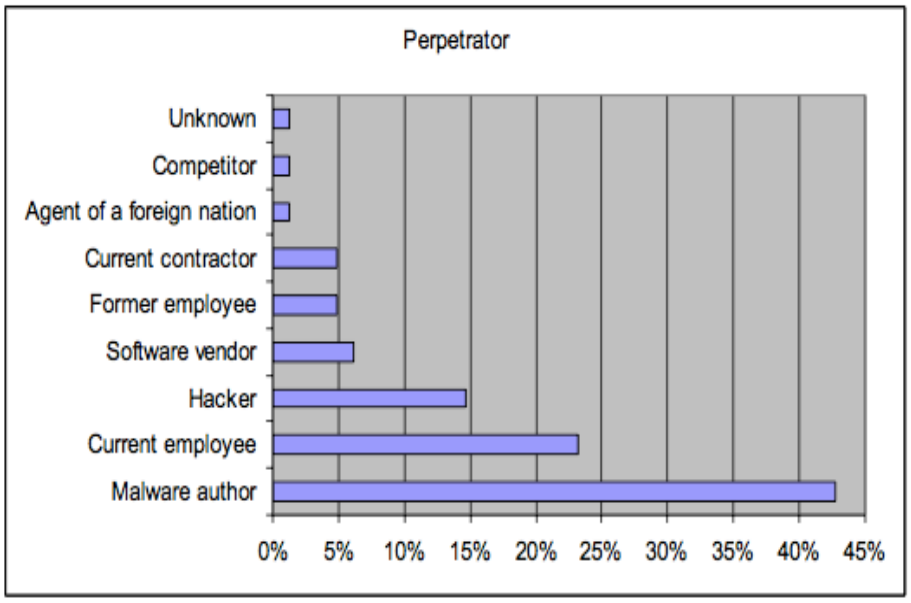

Figure 2: Bar chart illustrating the percentage of attacks based on the perpetrators [6].

In March 2000, an unauthorized access into the control system of a wastewater plant in Maroochy Shire, Queensland, Australia, had been the cause for the release of 1 million liters of sewage into the surrounding waterways. [27]

In January 2003, the "Slammer" *worm* entered Davis-Besse nuclear power plant network in Ohio by infecting the computer connected to it and disabled the computerized safety monitoring system by bypassing the firewall. [26]

In August 2003, the communication system of the U.S. railway company CSX Transportation was infected by a worm and the dispatching and signaling systems were affected. This caused traffic in Washington, D.C. and all passengers and freight traffic had to be stopped for 12 hours. [25]

Another incident that had impacted this research would be the blackout in April 2009, where Chinese PLA hackers are blamed to have accidentally triggered the power shortage in Florida [1].

In July 2010, the Windows computer worm, Stuxnet, was propagated in the industrial software and equipment. The worm was targeted only to Siemens SCADA with a highly specific payload to reprogram the operation of attached uranium refining centrifuges in Iranian facilities.

1.2 Problem Statement

The need to address potential vulnerabilities has been acknowledged across the United States federal government, including the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC). NISTIR 7628 also provides guidelines for smart grid cyber security and it is highly essential that all the security practices be in compliance with the standards. Cyber security requirements are implicitly recognized as critical in all of the priority action plans discussed in the Special Publication (SP), NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108), which was published in January 2010.

The Framework document describes a high-level reference model for the Smart Grid, identifies 75 existing standards that can be used now to support Smart Grid development, identifies 15 high-priority gaps and harmonization issues (in addition to cyber security).

Attackers will come up with new ways to compromise the computer controlling the control system, and it is necessary to devise new security standards to be followed by all organizations in order to secure the power-system environment from various attacks. All organizations should follow the Cyber Security Standards for communication and data acquisition.

1.3 Objective of the research

The research is partitioned into 5 tasks. First, a vulnerability assessment is done in order categorize the devices in terms of high risk and general vulnerabilities. Second, the vulnerability assessment is extended to attacks from an insider, attack on the computer monitoring and controlling the devices, attack on the SCADA network, and programming of malware into the control system devices. Third, a network monitoring solution is given, that can monitor the connections and payloads in a SCADA network and report any external or malicious connections. Fourth, The network monitoring solution is made to work along with State Estimation to provide a complete monitoring solution to report on malicious connections. Fifth, a proposal for SCADA test bed is presented.

1.4 Thesis outline

The thesis is organized as follows. Chapter 2 describes insider attacks and mitigation of such attacks. Chapter 3 describes the inherent vulnerabilities in SCADA systems. Chapter 4 presents the analysis in the vulnerabilities of the devices, and compares it with the specifications of the manufacturer. Chapter 5 discusses on our analysis and research. Chapter 6 provides the monitoring aspect of power control devices and general ways of safeguarding the SCADA systems. Chapter 7 discusses on the compliance of the devices with the NERC-CIP standards for providing cyber security in

the infrastructure. This includes the risks, technical aspects of the attacks and their consequences.

And finally, chapter 8 presents a proposal for a SCADA test-bed for future research in this area for safeguarding smart grids, and the conclusion is provided in chapter 9.

CHAPTER 2

RELATED WORK

SCADA security has become an important area of interest amongst researchers since the attack from Stuxnet, and it has led many researchers to publish interesting research papers and voice their claims in the need to improve the existing security standards in the area of power systems. There have been several research papers in the area of Cyber Security in SCADA networks, and their main contributions are presented in the paragraphs below.

A vulnerability assessment of cyber security for SCADA systems is presented by Ten et al in [2]. The paper provides the background information relating to SCADA attacks and explains the possible scenarios in which a system can be attacked, but does not provide information on the mitigation of the attacks. [4] provides information on the Data Integrity attacks and their impacts on SCADA control system, and gives a detailed analysis on the attack simulation and parameters that needs to be considered. But [5] suggests the use of a SCADA Security Test bed in order to test the security in all systems, and provides information on on-going research considering Denial of Service attacks and Man-in-the-Middle attacks. [6] presents information on Protocol attacks, Routing attacks, Intrusions, Worm/Malware attacks, and Denial of Service attacks on critical infrastructure such as power grids.

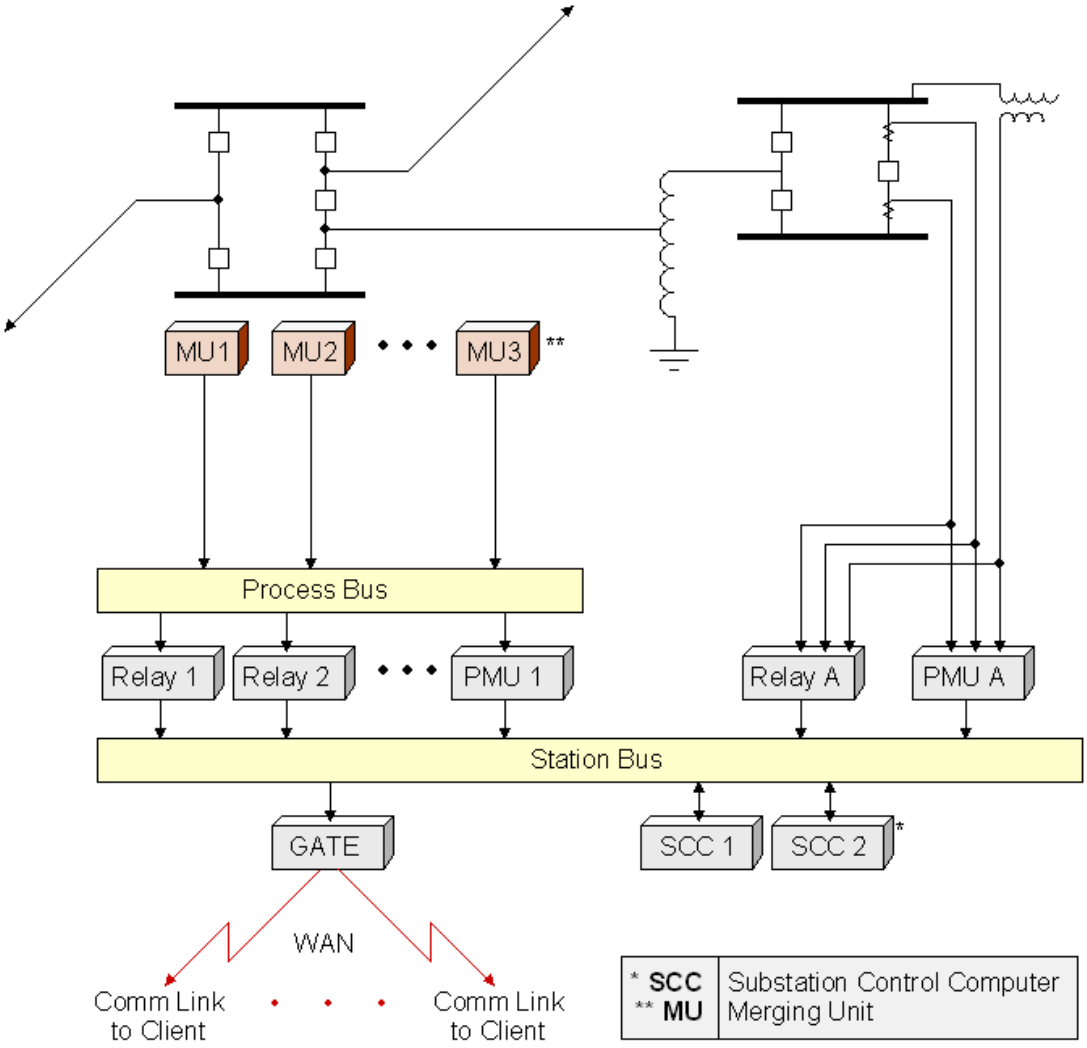

Figure 3: Smart Grid Infrastructure.

The Smart Grid Infrastructure is presented in Figure 3, which represents the topology of our current-day implementation, without the cyber security model. The Smart Grid Infrastructure with the cyber security model, will comprise 'network monitoring tools' which will check all the packets that are being sent in and out of the network and characterize them to see if they are legitimate or not. The block for monitoring networks

will be added as the last block of this model in order to reduce complexity and cost, and it will have to be written with a specific set of rules that apply to only power system devices.

A security model for the Cyber Security infrastructure is presented in [7] and the authors discuss on three types of vulnerabilities - system vulnerability, scenario vulnerability, and access point vulnerability. A case study on the electric substation and the possible consequences at the power station, and substation is presented in [11]. The paper provides a summary on the consequences of the attacks on the power grid, but does not provide details on the exact nature of attacks. Further, a case study corresponding to IEC 61508 standard is presented in [12], which provides top-priority technical recommendations to secure SCADA networks.

Risk analysis and recommended practices are discussed in [13] in order to improve the accessing capabilities of the existing networks, and comparing them to the "best practices". The authors recommend the cyber security assessment to be adjunct to other corporate security efforts rather than a standalone report. The authors from [14] compute the execution time of a specific code and compare it with the execution time during a legitimate operation, and look for an anomaly in their execution time to detect system compromise. They argue that execution times above, or below the respective bounds provide indications for a system compromise. Although this anomaly detection seems to work well in a controlled environment, there will be an increase in the number of false positives when implemented in a real-time network.

A complete list of past-attacks is specified in [15]. The author also describes the need for cyber-security in SCADA and the easiness of cracking the devices. This has been depicted in Figure 4.

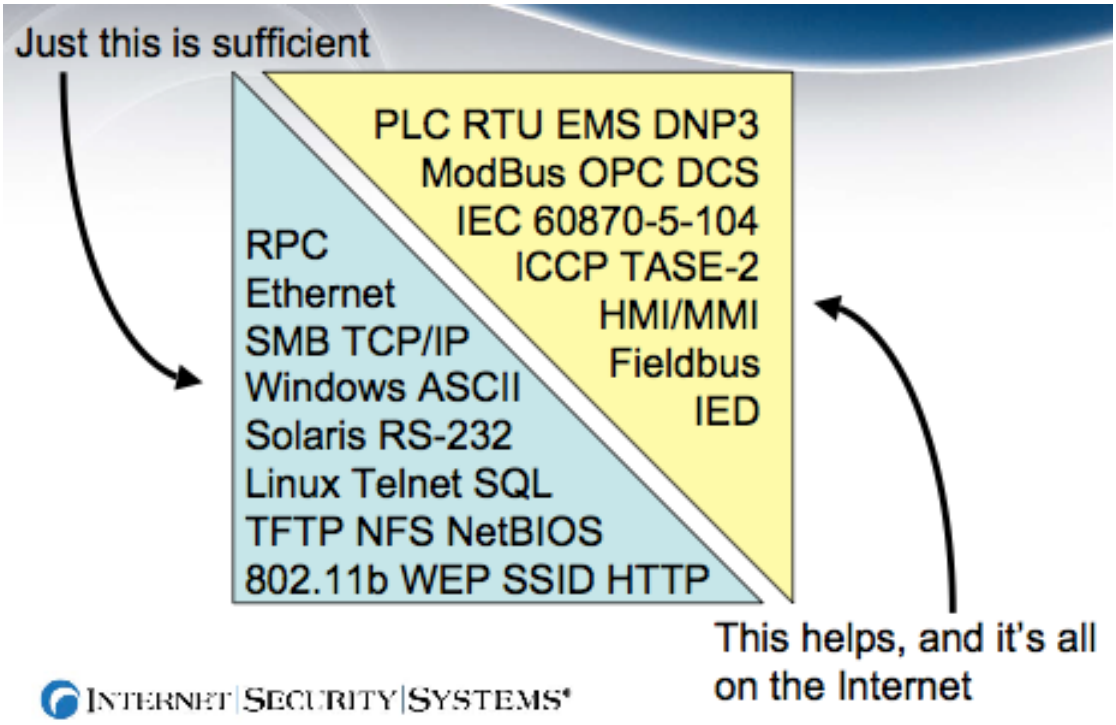

Figure 4: Diagram depicting the difficulty of an attack on SCADA systems

Information on the Security incidents and trends in SCADA and process industries is presented in [16]. The authors focus on the Industrial Security Incident Database (ISID) for highlighting the need for a control system security management system that is holistic and well designed, rather than a piecemeal approach to security.

An analytical framework for vulnerability assessment of SCADA systems is provided in [17]. The paper emphasizes the research on three substation–level models for a high level of cyber security and points to the need for a SCADA test bed. Programming of the SCADA systems requires the attacker to have knowledge on the internal working of the device. A comprehensive idea on the programming of the SCADA systems is provided by Carlo and Julian in [18]. The paper discusses on the idea of corrupting the memory of the devices at the programming level, and presents the memory access possibilities of the MODBUS protocol.

Ojeong-Dong et al provide an improvement in SCADA control system security with a software vulnerability analysis [19]. The authors provide an analysis on the software vulnerabilities and security concerns based on the their prototype for a SCADA security test bed and embed a script in the devices to change the state of the devices. This provides some information on the vulnerability, but the authors focus only on three types of attacks (sniffing, replay and spoofing). But they were not able to provide adequate results for their claims. Current efforts to secure SCADA networks and the technical aspects of launching a cyber attack is discussed by Rose Tsang in [20], and strategies for SCADA security, compliance and liability is further discussed in an article by Clint Boudungen et al [22].

CHAPTER 3

INSIDER ATTACKS

3.1 Past Attacks

In the past, insider attacks have been one of the major causes for concern for compromising control systems devices. In the event in Iran, Stuxnet infected project files belonging to Siemens WinCC/PCS7 SCADA control software and subverts a key communication library of WinCC called s7otbxdx.dll. Stuxnet also carried a zero-day exploit in the WinCC/SCADA database software in the form of a hard-coded database password [8]. The attacks seem designed to force a change in the centrifuge's rotor speed, which could have possibly destroyed the centrifuge, and the consequences would have been catastrophic. The worm is reported to have been plugged-in through an USB drive in order to infect the system. These events indicate the necessity to secure the control system from insider attacks and there are several ways this can be done.

1. Securing the computer from unwanted access through external drives.
2. Securing the Ethernet socket, which might allow access by a potential hacker.
3. Offering confidentiality (encryption) and integrity in the data sent between the computer and the Control System.

3.2 Authentication and Encryption

It is necessary to secure the data being transmitted between the Control System and the computer connected to it. In our work, we found in the power control devices that

encryption can be manually setup with PLA programmable logic, with AES 128bit encryption setup between them. There is also an option in some of the devices to setup up an encryption scheme through software provided by the manufacturer for encrypting the transmitted data. Figure 5 shows the options in G60, a generator protection device manufactured by GE. This can be setup as soon as the device is installed into the Smart Grid.

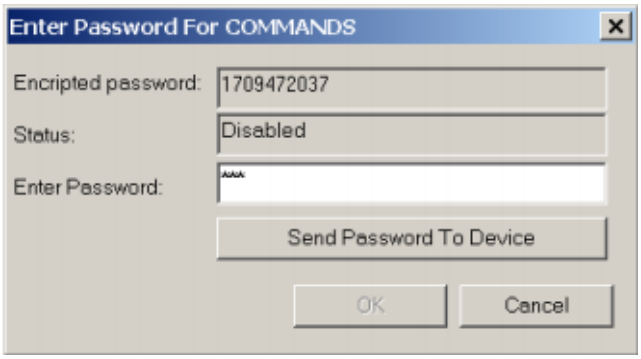

Figure 5: Encryption in G60 with the software, Enervista

The important requirements for the Smart Grid are listed below.

a) Operation of the power system must continue 24×7 with high availability
b) Power system operations must be able to continue during any security attack or compromise
c) Power system operations must recover quickly after a security attack or the compromise of an information system.
d) Testing of security measures cannot be allowed to impact power system operations.

CHAPTER 4

SCADA SYSTEM

The SCADA system is an industrial control system for monitoring and controlling a device or a process. The heart of the SCADA system lies in the communication protocols used for sending and receiving data.

4.1 Components of a SCADA system

A SCADA system has the following subsystems:

1) A Human-Computer Interface, that presents the data from the process to the display, and the human is able to monitor and control the process.
2) A computer (supervisor), which is responsible for the communication between the human and the process.
3) Remote Terminal Units (RTU) responsible for connecting to the sensors in the process, and converting the sensor signals to the digital data and sending it to the computer.
4) Programmable Logic Controllers (PLC).
5) Communication between the RTU and the computer.

The SCADA system monitors the entire power control system in real time. The data acquisition is handled locally at each site by sensors and electromechanical devices that are hard-wired to the RTU. Not only is data processed by the local RTU, but data is also compiled and formatted so that a control room operator using an HMI can monitor or adjust settings. Data is usually recorded and logged for analysis.

4.1 Common Vulnerabilities

It can be observed that there are three inherent problems in SCADA system.

a) SCADA networks are not authenticated.

b) SCADA networks are never patched. It takes quite a few years for the manufacturer to upgrade the operating system.

c) SCADA networks are provided uncontrolled interconnects.

A common list of vulnerabilities in Smart Grid systems is presented in Table 1.

Table 1: Common vulnerabilities in the SCADA systems in their specific category

Category	Common Vulnerability
Poor code Quality	Use of potentially dangerous functions in the code
Vulnerable Services	Poor authentication, Clear-text authentication, no password, weak password, Unauthenticated access to Web server,
Network Protocol Implementations (Modbus)	Buffer Overflow is possible, Lack of bounds checking in the service, Weak Authentication, No encryption
Poor Patch Management	Unpatched operating systems
Least User Privileges Violation	Unauthorized directory traversal allowed, Services running with unnecessary privileges
Information Disclosure	Unencrypted communication, unencrypted services, weak protection of user credentials, Man-in-the-middle attack
Network Design Vulnerabilities	Lack of network segmentation, No proper firewall for the Network Protocol implementation
Network Component Configuration Vulnerabilities	Access to specific ports on hosts not restricted to required IP address, Port security not implemented on network equipment

4.3 Communication Protocols.

SCADA protocols are designed to be very compact and they are designed to send information only when the master station polls the RTU. Typical legacy SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 60870-5-101 or 104, IEC 61850 and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors and many of these protocols now contain extensions to operate over TCP/IP.

The Modbus protocol is implemented in encoded protocol data units *(PDU)*, used in the SCADA system for communication. In another study, Bayindir et al.[22] present a Modbus aware firewall based on Linux Netfilter into the energy monitoring system, in order to prevent unauthorized access and certain Modbus function code.

Currently, the Modbus protocol used in the communication does not have a solution to its current problems over Ethernet links. Despite the inherent lack of security in the design of Modbus, no security tools exist that are geared toward the detection of malicious Modbus traffic. Despite efforts to improve and provide guidance to help ensure security, there are very few security tools that have been released for the exact purpose.

4.4 Security Issues

By conducting security assessments on a variety of Personal Communications Service (PCS) systems, IBM Internet Security Systems (ISS) consultants have identified some basic security issues impacting these devices [21]. The following provides a high level overview of the critical security issues surrounding the SCADA systems:

- Weak protocols leave systems vulnerable. The underlying field bus protocols were never designed for security. Testing shows that these devices are very prone to simple denial of service attacks and buffer overflows. Additionally, since field bus protocols do not have built-in authentication, the devices will accept connections from anyone, and legitimate packets will be processed without any additional user or system authentication.

- SCADA systems are not patched, or cannot be patched, as it will violate the vendor's service contract. The operating system of the device is upgraded only during the next phase of manufacturing.

- SCADA networks lack overall segmentation, and it is hard to configure the firewall distribution for the network, as the network can be easily breached in many places.

- SCADA systems lack antivirus protection. Many system vendors will not support antivirus applications, and it will be hard to update the anti-virus database without being

connected via Internet.

- Most SCADA systems communicate through the network and rely on unencrypted communications. This can cause eavesdropping, man-in-the-middle attacks, and session hijacking.

- SCADA systems do not have a database to store a log-file for security audits.

- Lack of physical security may lead to insider attacks.

These are only a few of the potential risks associated with SCADA and Process Control Systems. IBM ISS recommends that organizations look for these weaknesses in any assessment of SCADA vulnerabilities and/or an organization's broader security posture. But it is possible to handle these issues with virtual, ad-hoc patching, which was first brought up by IBM, in order to provide security to over thousand vulnerabilities [24].

CHAPTER 5

NETWORK ANALYSIS

5.1 Pen-testing

From our research by placing all the devices in a network we were able to find that the control system devices had several issues, which are listed below.

1. The operating systems are in the default configuration.
2. All devices are unpatched.
3. An external device can be connected without any authentication.
4. Services such as Telnet, and other unknown services run unencrypted sessions.
5. Password policies could be 'set' by the devices for confidentiality, but they can be shared with other devices without authentication.

Metasploit released a list of vulnerabilities on the VxWorks in 2010 regarding the VxWorks Debug Agent - WDB Agent [28]. The WDB agent is a system-level debugger for the VxWorks operating system that runs on UDP port 17185. This service is modeled on the SunRPC protocol and this allows anyone with access to this port to read memory, write memory, call functions, and manage tasks. Since the protocol is UDP and there is no authentication, handshake, or session ID, requests to the WDB agent can also be spoofed by an attacker.

Our test on the vulnerabilities on some GE devices such as G60 and N60 shows that they run the VxWorks Debug Agent on the port 17185, and it is vulnerable for exploits. With the use of an Embedded WindSH (or) Tornado Shell for VxWorks, it will allow us to connect the device and directly exploit it. A custom Nmap script was able to point out several key details about the service running on port UDP 17185.

Starting Nmap 5.51 (http://nmap.org) at 2011-04-24 21:53 Eastern Daylight Time

Nmap scan report for 192.168.0.55

Host is up (0.0010s latency).

PORT STATE SERVICE

17185/udp open wdb

| wdb-version2:

| VULNERABLE: Wind River Systems VxWorks debug service enabled. See http://www.kb.cert.org/vuls/id/362332

| Agent version: 1.0.1\x00

| Agent MTU: 1500

| VxWorks version: 5.3.1\x00

| CPU Type: 97

| Board Support Package: GE Multilin - Main CPU\x00

| Boot line: marondev1edcge:\bootrom\bootrom.vxworks\x00

| Memory Size: 33554432

|_ Memory base: 0

MAC Address: 00:A0:F4:00:38:86 (GE)

Nmap done: 1 IP address (1 host up) scanned in 4.00 seconds

Although the manufacturers of the GE devices do not disclose information on the microprocessors used, knowledge on the architecture of the microprocessor would make it possible to know the exact memory map of the device and reprogram it remotely. We were not able to ascertain what microprocessor was used.

5.2 Other means of exploit

Digital Fault Recorder (DFR) is an intelligent electronic device (IED) that records information about power system disturbances. It stores data in the digital format when certain conditions are triggered by the power systems, and the data captured is in the form of Harmonics, frequency, and voltage. In the power grid the DFR plays an important role with regards to analyzing the power grid and recording faults. But they run a vulnerable version of windows (Windows 2000 or Windows XP SP0) as their operating system, and they are connected to the power grid network. They can be easily compromised by attackers and can be used as a considerable source for launching exploits and launching denial of service attacks (DOS). In our power testing equipment, our analysis on the APP DFRs shows high-level vulnerabilities with regards to the SNMP server running with "public" community name. This can be exploited by an attacker with the *snmpwalk.exe*, and this can provide all *netstat* information and information on all the processes running in the devices with their process id number. This information can provide information

and access to all the PMUs that are connected along with the DFR, and the attacker would be successful with his reconnaissance and would be able to launch a denial of service. The details on such a denial of service with regards to the SNMP vulnerability is provided in [30].

5.3 Observed Vulnerabilities

A vulnerability assessment was performed over the SCADA network comprising of devices from Manufacturers – Rugged Com, Siemens PMU, GE, SEL, and APP Arbiter. The devices were connected in a network with IP address assigned to each of the device and a computer running WindowsXP as it's operating system was connected to it for transmitting and receiving messages from the devices. The network and connections were setup to simulate a power-grid environment where a large number of devices are connected to a single computer, which can be used to configure the devices and monitor the readings from the devices with the software provided by each manufacturer.

The network was scanned for known vulnerabilities and certain exploits were conducted on the device, and goal was to simulate the real-world environment where an attacker would typically conduct a network scan and perform a reconnaissance in order to learn about the type of devices, the operating system, and the open ports communicating in the network. The commonly used vulnerability and pen-testing tools such as Nessus, Nmap, Metasploit and Backtrack framework were used to learn about two key features:

a) The vulnerabilities in the devices (by conducting exploits based on existing vulnerabilities).

b) The behavior and response of the devices when networks scan is conducted.

The results of the scan are presented in the table below. High quality images could not be added in this document, and they have been present in [32] and [33].

Table 2. Vulnerability Assessment of Devices

Device	IP address	Severi	Details on Vulnerabilities	More Details On the Issue
RUGGED COM	192.168.0.1	LOW	1. All the details including the MACaddress and product serial number is available.	System Name: Australopithecus Location: Salt Mine Contact: Potatohead Product: RSG2100-R-RM-HI-XXX-TX01-TX01-TX01-TX01-CG01-XXXXX-XXXX-X
			2. Uses un encrypted telnet service.	An attacker may eavesdrop on a Telnet session and obtain credentials or
			3. Service detection.	A webserver is running through TLS v1
			4. Uses TFTP (Trivial File Transfer Protocol)	Used by routers to retreive information on configuration. Can be used to
			5. Common platforms can be enumerated	Matches with IBM AIX 5.2, Catalyst OS 6.3
			Unknown Service Detection: banner retreivel	Banner : 0x00: 47 45 54 20 00 03 48 D4 0A GET ..H..
			Ethernet card manufacturer detection	RuggedCOM
			Multiple Ethernet Driver Frame Padding Information Disclosure -- Should	Known as 'Etherleak', this information disclosure vulnerability may allow an
Computer Accessing all Machines	192.168.0.11	HIGH	1. SMB remote registry accessible.	
			2. Operating system information and remote LAN manager information is provided.	This is done by sending an authentication request to port 139, or 445
			3. *Arbitrary code can be executed in the system*	This is done by a buffer overrun in the server and this allows an attacker to execute an attack with 'Admin' privilages.
			4. ECHO service is running on the system.	This makes it possible to execute DoS attacks.
			5. StarWind control port has default credentials. (username:test, password:test)	
			6. Discard Service Detection.	
			7. Daytime Service Detection.	This can allow an attacker to perform timed-authentication to gain access.
			8. SMB Null Session Authentication	With no login and password, it is possible log into a null session
			9. Possible to login as a guest (remote service)	
			10. Echo Server, Chargen server	
			11. Runs Windows XP SP2	
			12. System can be easily crashed because of the SMB flaw.	
			13. SID value is available.	Remote SID value is 1-5-21-1390067357-1844823847-725345543. The host SID can then be used to get the list of local users.
			14. TCP/IP Timestamps Supported	The uptime of the remote host can sometimes be computed.
			ICMP Timestamp Request Remote Date Disclosure	The difference between the local and remote clocks is 635 seconds.
SIEMENS	192.168.0.30	LOW	Common platform enumeration	It is possibe that HP Jet Direct Pirnter matches the OS.
			Ethernet card manufacturer detection	ipcas GmbH
			Port 2010 & 4712 were open before scan, and closed right after scanning.	The scan might have stopped or freezed any service running.
G60	192.168.0.55	HIGH	Operating System can be guessed	60% Chance of A/UX 3.11
			VxWorks WDB Debug Service Detection -- Must be patched	Arbitrary commands can be run on this port, and there is no write protect in memory. THIS DEVICE CAN BE REPROGRAMMED. Memory Size : 33554432
			Ethernet card manufacturer detection	GE
			3. Service detection.	A webserver is running through TLS v1
			4. Uses TFTP (Trivial File Transfer Protocol)	Used by routers to retreive information on configuration. Can be used to
			HTTP protocol information disclosed	Protocol version : HTTP/1.0. This is not a vulnerability since it is not used for communication, but the information is disclosed to an attacker.
			ICMP Timestamp Request Remote Date Disclosure	The difference between the local and remote clocks is 59419 seconds.
N60	192.168.0.65	HIGH	Operating System can be guessed with ICMP packets	60 % chance of A/UX 3.11
			VxWorks WDB Debug Service Detection --Must be patched	Arbitrary commands can be run on this port, and there is no write protect in memory. THIS DEVICE CAN BE REPROGRAMMED. Memory Size : 33554432
			Ethernet card manufacturer detection	GE
			Unknown Service Detection: Banner Retrieval	On port 4712, 0x00: AA 01 00 24 00 08 4D 8B CD 40 00 0C B7 35 00 00 ...$..M..@...5.. 0x10: 00 00 00 00 00 00 00 00 00 00 00 00 15 A0 00 00
			ICMP Timestamp Request Remote Date Disclosure	This host returns non-standard timestamps (high bit is set)
SEL421	192.168.0.92	LOW	Service Detection	Service closed connection without sending any data. Might be protected by a
			Unencrypted Telnet Server is listening.	An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.
			FTP server is running	
			FTP server is running with clear Text Authentication	Possible to intercept credentials and use a MAN IN THE MIDDLE ATTACK.
			TCP/IP Timestamps Supported	The uptime of the remote host can sometimes be computed.
SEL-351-A	192.168.0.95	LOW	Common platform Enumeration	Platform matches with HP Office Jet Pro Printer. 70% match
			Ethernet card manufacturer detection	Schweitzer Engineering
			TCP/IP Timestamps Supported	The uptime of the remote host can sometimes be computed.
Arbiter	192.168.0.254	LOW	Possible to find the platforms similar to the system	The arbiter matches with IBM AIX4.3.2, IBM, AIX5.2, HP HP-UX 10.20
			Ethernet card manufacturer detection	Precision Electronic Manufacturing

Table 2 provides the list of vulnerabilities from known exploits with pen-testing devices, and the devices are marked as 'high' or 'low' in terms of the risk of getting exploited.

All devices had unauthenticated and unencrypted access running telnet/ftp/http and an attacker can see through the contents of the packet by using a packet sniffer with little difficulty. Some devices had highly vulnerable services in them that could be exploited with by running Metasploit or Backtrack.

It can be seen that the GE devices, in specific, G60 and N60 were running a vulnerable version of the VxWorks operating system, runs VxWorks WDB service that can be easily exploited with a Tornado Shell. Metasploit released the exact detail of this vulnerability earlier and an exploit on this enables us to perform a memory dump on the device, read memory, and write memory.

An attacker can perform the following attacks with requiring any authentication:

a) Remote memory dump.
b) Remote memory patch.
c) Remote calls to functions.
d) Remote task management.

The VxWorks vulnerability allows the attacker reprogram the device and modify the boot flag in the devices. For example, if the boot flag is set to 0x08, this would perform a quick auto-boot on the device, and if the boot flag is set to 0x20, this would disable login security. This has been described in detail in [31] with a list of boot flag commands for specific operation. An attacker could write a script to set the boot flag to any value that would be advantageous to him.

A vulnerability assessment was also performed on the main computer controlling the power system devices. The computer was running Windows XP, and this was chosen so

as to simulate the scenario in actual power grids as the main computers generally run either Windows 2000 or Windows XP. The smart grid community does not prefer to update the operating system and this is mainly because of the software compatibility issues with regards to the software that is provided by the device manufacturers along with the devices. The computer is highly vulnerable to existing exploits and an attacker would be able to root the device and learn about all the devices connected to it (reconnaissance) or exploit it to send a payload to the devices in its network to re-program it or perform malicious activities.

CHAPTER 6

MONITORING NETWORK

Power system monitoring, control and protection devices are thought to be in a separate network, but they have too many uncontrolled interconnects that provides the attackers numerous ways to get into the network. It is highly necessary that the cyber network be monitored in order to characterize the legitimate traffic from the illegitimate or malicious traffic.

The power monitoring, control and protection devices have a smaller set of connection requests and replies compared to the conventional networks. And so, it will be much easier to design a set of rules for providing the firewall or an intrusion detection system for detecting intrusions in the system.

6.1 Monitoring the control system environment

Monitoring of the devices can be done in two ways - by monitoring the network by analyzing the network traffic with the list of devices connected to the network, and by using state estimation approach to monitor the state of the system.

6.1.1 Monitoring the network

6.1.1.1 Active monitoring

Devices can be actively monitored by analyzing the network traffic that is flowing and looking for certain packets that are allowed in the set of rules. Any traffic that is

detected as abnormal will be dropped and will be reported for analysis. This approach requires us to develop specific protocol aware firewalls. Since many protocols are presently in use, one needs to target specific protocols that are mostly used. In this respect, DNP3, C37.118 and IEC 61850 should be targeted. In this research, Python is used as a programming tool with PyModbus library, which implements Modbus client and server communications. The usefulness of the libraries is provided in Appendix A.

6.1.1.2 Passive monitoring

Devices can be passively monitored by recording the traffic each day and then parsing the contents of the. pcap file (packet capture file). This would provide all the necessary information on traffic and then report all connections that were made and characterizing the legitimate traffic from illegitimate traffic.

6.1.2 State Estimation

State estimation is used in system monitoring to best estimate the power grid state through the analysis of meter measurement data and power system models. It is the process of eliminating unknown state variables on a power grid based on the measurement data. Hence by using the output of state estimation, one can determine whether a suspected batch of data is legitimate or could have been altered.

An attacker can determine the power system configuration and generate bad measurements in a way such that the bad measurements are not detected (*False Data Injection Attacks*). The attacker can also utilize small errors in measurements in State

Estimation algorithms and use that for increasing the chances of not being detected. Since an attacker will not have access (or it will be very difficult) to the real time model of the system, then the state estimation results will be an independent yardstick to determine authenticity of data. The theory of such attacks is explained by Yao Liu and Peng Ning in [29].

6.2 Monitoring model

The model for monitoring the network comprising of the networking monitoring tool and state estimation model is presented in Figure 6.

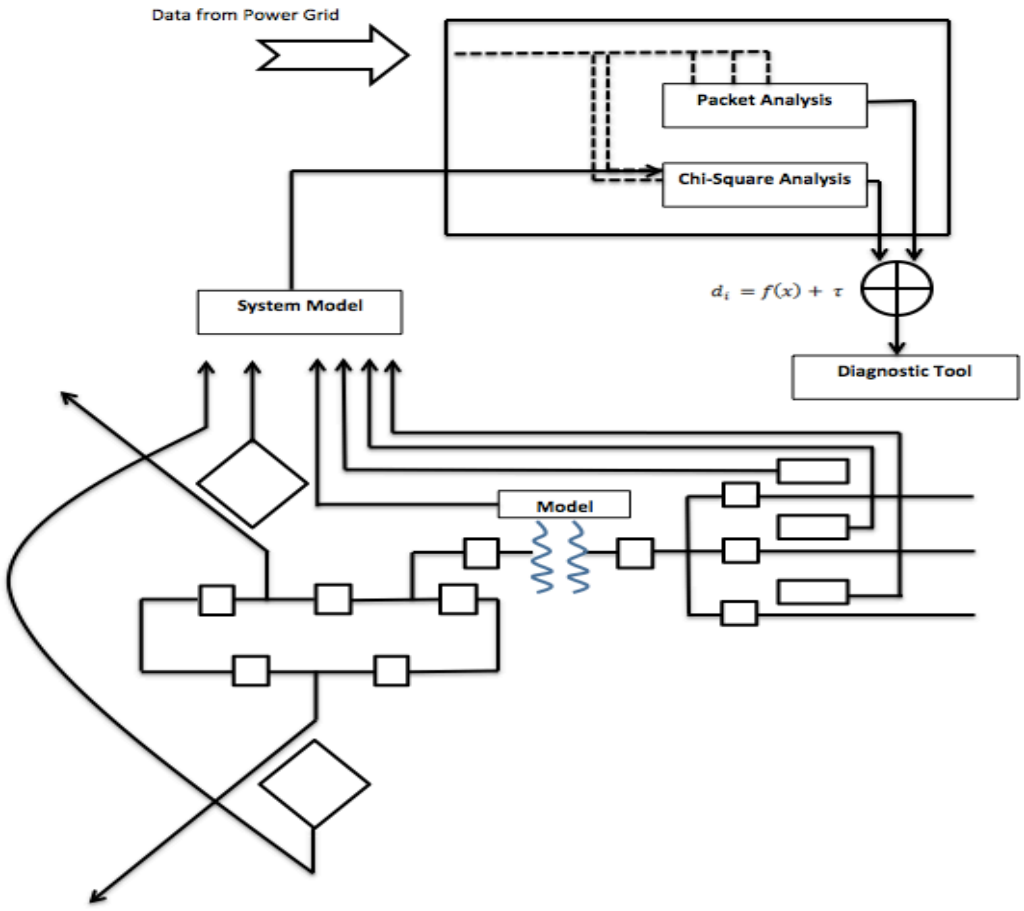

Figure 6. Model for monitoring the power grid network.

The data from the power grid is fed into the “Analysis” block for monitoring the network packets and analyzing the state of the network at that particular time. It consists of two blocks - the block for network-traffic analysis, and the block for Chi-Square analysis. The packet analysis consists of monitoring the network for malicious traffic and characterizing them from legitimate traffic. The characterization is done based on a specific set of rules for the protocol specific to the device which is being monitored, and the protocol used such as DNP3, C37.118 and IEC 61850.

The rules for characterizing the network traffic has several layers of security configured in it, and has simple rules that considers “good” traffic if it originates from the IP addresses which are allowed to communicate and establish SYN packets to the other devices. If the originating IP address is not present in the list of allowed devices, it is reported. The packets are further inspected for headers related to the protocol specific to the devices, and inspecting the commands that are sent and received such as ‘Brick’, etc.… The network monitoring script also scans for abnormal port scans and ping sweeps which is the first step for hacker to detect the devices in the network. Any abnormal port scans, ping sweeps, and ICMP requests are recorded and reported for further analysis on determining the location of the device conducting reconnaissance on the SCADA network. Besides the network monitoring side, state estimation is done to characterize “good” data from “bad” data and the detailed description of this methodology is given below.

State estimation is the process of eliminating unknown state variables on a power grid based on the measurement data, and one can determine whether a suspected batch of data is legitimate or could have been altered. The state estimation is done by considering a set of variables consisting of all bus voltage magnitudes and angles except the phase angle at an arbitrarily selected bus, which is zero. The data from the power grid is sampled and the state of the system is estimated based on the current state of the system, and this process is done in the Chi-Square Analysis block. The data is immediately compared with the legitimate set of data originating from the system model, which is characterized as "good" data. An attacker can determine the power system configuration and generate bad measurements (*False Data Injection* Attacks), the Chi-Square Analysis block will be able to compare it with the system model, and any inconsistencies obtained as a results of the comparison is noted and reported. The overall state of the network is characterized as a function of the state estimation results together with the results from monitoring the network. We believe that such a level of characterization will be of high standard and extremely accurate with regards to reporting malicious data and monitoring the network for abnormalities.

CHAPTER 7

COMPLIANCE WITH STANDARDS

Power system devices have a huge number of uncontrolled interconnects but are thought to be totally isolated. We had already visited a lot of events in which the smart grid systems were either accidentally or intentionally susceptible to attacks over the network. It is highly important that all the manufacturers are compliant with a set of standards that describe the security measures that ought to be met in the devices before they are installed as power grid equipments. NERC and NISTIR 7628 set some of the important standards, which provide detailed information on the requirements of power grid infrastructure. Our goal in this thesis is to highlight the requirements, and set the objectives of this research to be in par with the critical standards.

7.1 Current Standards and Guidelines

NERC and NISTIS7628 provide the critical infrastructure protection (CIP) requirements that ought to be followed while installing a power grid. This has been discussed in detail in [34]. Some of the key requirements are as follows:

a) Standards identification and selection – This is the first step, and it involves identification of the standards and guidelines that will match the setup for the infrastructure.

b) Policies and procedure analysis – After the first step, the policies and the procedures must be added along with the existing guidelines to make sure that they are compliant with the requirements.

c) Critical asset identification and classification – By following the standards, the critical assets have to be identified and classified based on risk management.

d) Security vulnerability assessment – It is required that a security vulnerability assessment is performed in order to understand the exact vulnerabilities in the devices.

e) Assessment validation – The results of the security vulnerability assessment have to be validated by a combination of analysis, penetration testing and interviews. It is also important to analyze false negatives and false positives, which could be critical for analysis and validation.

Besides all the above recommendations, it is important to draft mitigation, validation, legal, management and training requirements in order to be compliant with the standards.

7.2 Our goals

Our goal in this research is to work towards using and developing tools and creating an auditing environment in order to aid devices that operate in the SCADA network to be compliant with the standards set by NERC and NISTIR7628. In the previous chapters, the work done pertaining to this research was clearly explained with the need to the work on power control devices. It is necessary to detect all possibilities of attack and characterize them in terms of the risk involved in the existing configuration of the devices. This would enable identification of the critical assets and providing a detailed list of vulnerabilities that the manufacturers need to take account into.

This thesis also provides information on the monitoring aspect of power control devices and providing means of identifying threats that would be critical to the infrastructure. Although the work done in this is still in its infancy, it would be highly necessary that the community works towards improvement in the existing monitoring models, and provide control system devices with a high-level intrusion detection system, and enable them to be compliant with the standards and guidelines presented by NERC and NISTIR7628.

CHAPTER 8

FUTURE WORK

SCADA security is an emerging topic in the area of information security, and the work done is still in its infancy. The goal of this thesis is to expose some of the common vulnerabilities in the control system environment and monitor the network to prevent any exploits. From the past attacks, it is clear that it does not take too much effort for an attacker to compromise power control devices, and Stuxnet is probably the most advanced among all the previous exploits. The goal of this research is to work towards using and developing tools to create a SCADA test-bed in order to test various devices and explore the possibilities of securing the control system environment. The network monitoring solution provided in this thesis is still in its infancy, as it needs to be constantly changed and improved in order to accommodate the rules for different protocol standards used by different devices. The model also needs to be tested with all the devices in order to develop an ideal intrusion detection system that would work well in any environment. The work pertaining to this will be a future work and would greatly solve the need to develop a monitoring solution for each model. Further more, the idea of using State Estimation along with network analysis would help in offering a highly efficient monitoring model that could detect attacks in terms of both the control-system perspective, and the networking perspective. The development and testing of this complete model would be crucial to solving the requirement of an ideal intrusion detection system.

Chapter 5 presents the vulnerabilities that were observed in the devices, and they have been conducted to simulate the same environment an attacker would use to learn about the devices. With regards to the performing a memory dump on the VxWorks operating system, some knowledge on the specifications on the processor and the size of the memory would have helped in learning entirely about the possibilities of attack. But manufacturers do not reveal this information in order to safe guard their product. As a future work, the goal of this thesis is to perform a preliminary set of tests in order to develop a complete SCADA test-bed with an ideal monitoring model, and it will be necessary to partner with the manufacturers to learn complete details on the product in order to develop a robust test framework.

CHAPTER 9

CONCLUSION

Security research in the control system environment is still an on-going research topic when compared to the development in other areas of information security. The presence of security threats and exploitable weaknesses in the control system devices makes it easier for attackers to target them, and this could be potentially catastrophic for national security and nuclear or military sites if the control system devices get compromised. The thesis addresses four scenarios in which an attack can be performed on the devices – insider attacks, attack on the computer accessing the SCADA system, attack on the SCADA network, and direct exploit on the device by reprogramming it. A network-monitoring model has been proposed with state estimation theory, and network analysis to identify and report any malicious attacks on the SCADA network. However, this work is still in its infancy, and it is necessary to develop and maintain tools to offer an ideal solution to the SCADA environment, and that would be the future work of this thesis. The thesis has also addressed the importance of NERC and NISTIR7628 guidelines and the need for the smart grid to be compliant with those standards. The ultimate goal of this research would be to develop a highly robust SCADA test-bed, and hope this thesis would serve as the first bold step in identifying and reaching this goal.

APPENDIX A

NETWORK MONITORING SCRIPT FOR CONTROL SYSTEM ENVIRONMENT

The network monitoring script for the control system environment is written in Python, a popular programming language used by programmers and developers in the software industry. We will be discussing only a few specific libraries that aid the development of network monitoring script and the effectives of those libraries written in Python for specific protocols that control system devices use. These libraries are given as follows:

a) Pcapy (used along with IMPacket)

b) Scapy

c) Pymodbus

Pcapy is a Python extension module that interfaces with the packet capture library (libpcap) and it enables python to capture packets on the network. This would allow us to capture the network traffic of the SCADA network and perform a passive analysis on the network by parsing the captured data and learn a lot about even the tiniest events happening in the network. It is normally used along with IMPacket , which is a collection of Python classes focused on providing access to network packets. Packets can be constructed from scratch and parsed from raw data.

Scapy, is a powerful packet manipulation tool which can be used with Python scripts to forge or decode packets of a wide number of protocols and send them on wire, capture

them, match requests and replies, and much more. Scapy can be used to perform an active monitoring on the SCADA system and monitor all the fields of the packet such as the source, destination, and the payload. This helps us in characterizing the nature of the packet based on the source and frame a set of rules for the SCADA network such that only the authorized devices are allowed to communicate and other connections can be reported for unauthorized access.

Pymodbus is a full Modbus protocol implementation for asynchronous communications. It has both client and server features in order to fully simulate the working of the Modbus protocol, enabling the client to fully read/write protocol with asynchronous and synchronous payload builders. The server can be function as a Modbus server operating on port 502. Writing a monitoring script for thousands of devices does not seem like the most efficient way of testing, and using the Pymodbus allows us to test as many devices as the base operating system allows by exhausting the virtual IP addresses. The complete module and usage of this library is provided in [35].

REFERENCES

[1] http://online.wsj.com/article/SB123914805204099085.html (01/2011)

[2] C. Ten, C. C. Liu, and G. Manimaran, "Vulnerability assessment of cyber security for SCADA "

[3] http://cnls.lanl.gov/~chertkov/SmarterGrids/Talks/Govindarasu.pdf (01/2011)

[4] S. Siddharth and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system" IEEE PES General Meeting, 2010.

[5] A. Hahn, et. al., "Development of the Power Cyber SCADA Security Test bed", in Cyber Security and Information Intelligence Research (CSIIR) Workshop, Oak Ridge National Laboratory, 2010

[6] [General Accounting Office, CIP Reports, 2004 to 2010]; [NSA "Perfect Citizen", 2010]:

[7] http://www.inl.gov/technicalpublications/Documents/3480144.pdf (02/2011)

[8] http://www.gedigitalenergy.com/multilin/catalog/g60.htm#ss (03/2011)

[9] http://store.gedigitalenergy.com/download/download.asp?id=g60&file=4

(03/2011)

[10] http://www.ewics.org/attachments/security-subgroup-bps/Electric+Power+Systems+Cyber+Security++WP+5086+V1_1.pdf (03/2011)

[11] Zurakowski Z.: Task B1b: Identification and Preparation of Case Studies – Extra High Voltage Substation Software Interlocking Case Study. EC JRP CP94 1594

[12] ISAT, Technical Report TR ISAT 97/8, Institute of Power Systems Automation, December 1996, Updated: February and April 1997.

[13] http://www.andritzautomation.com/documents/industrialcybersecurity.pdf (04/2011)

[14] http://cimic.rutgers.edu/positionPapers/paper-FrankMueller.pdf (03/2011)

[15] http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf (05/2011)

[16] http://www.mtl-inst.com/images/uploads/datasheets/IEBook_May_07_SCADA_Security_Trends.pdf (03/2011)

[17] http://vulcan.ee.iastate.edu/~gmani/personal/papers/journals/IEEE-PS-08.pdf

[18]. http://www.cs.uiuc.edu/~jrrushi/old_IAW07.pdf (08/2011)

[19]. http://www.wseas.us/e-library/conferences/2010/Catania/ACMOS/ACMOS-69.pdf (08/2011)

[20] http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf (09/2011)

[21] http://www.iss.net/documents/whitepapers/SCADA.pdf (09/2011)

[22] Bayındır R., Sağıroğlu S., Colak I., Ozbilen A.(2009). Investigating Industrial Risks Based On Information Security For Observable Electrical Energy Distribution System And Suggestions. Journal of The Faculty of Engineering and Architecture of Gaza University. Cilt 24, No 4, 715-723, 2009 Vol 24, No 4, 715-723.

[23] http://www.cidgcorp.com/docs/SCADA-Security-Compliance-Liability-A-Survival-Guide-072408.pdf

[24] http://www.iss.avnetportal.ch/fileadmin/iss.avnetportal.ch/templates/pdf/downloadbereich/multifunction_series/multifunction_MX3006_sales_guide.pdf

[25] CSX Transportation, "Computer virus strikes CSX transportation computers—Freight and commuter service affected (press release),"Aug 2003.

[26] K. Poulsen. (2003, Aug.) Slammer worm crashed Ohio nuke plant net. [Online]. Available: http://www.securityfocus.com/news/6767.

[27] T. Smith. (2001, Oct.) Hacker jailed for revenge sewage attacks. The Register [Online]. Available: http://www.theregister.co.uk/content/4/22 579.html.

[28] http://blog.metasploit.com/2010/08/vxworks-vulnerabilities.html (08/2011)

[29] http://www.cs.unc.edu/~reiter/papers/2011/TISSEC2.pdf (10/2011)

[30] http://www.sans.org/security-resources/idfaq/snmp.php (10/2011)

[31] http://thesauceofutterpwnage.blogspot.com/2010/08/metasploit-vxworks-wdb-agent-attack.html (04/2011)

[32] http://cl.ly/1M3Y2B3h0t2p1X1E2r43

[33] http://cl.ly/2v3T0i3r1b1b0q1O0k3k

[34] http://www.nerc.com/page.php?cid=6|69

[35] Pymodbus github - https://github.com/bashwork/pymodbus