2009

Information Security Analysis and Auditing of IEC61850 Automated Substations

Upeka Kanchana Premaratne

Information Security Analysis and Auditing of IEC61850 Automated Substations

(Spine title: Security Auditing of IEC61850 Automated Substations)

(Thesis format: Monograph)

by

Upeka Kanchana Premaratne

Graduate Program
in
Engineering Science
Electrical and Computer Engineering

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Engineering Science

School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

Abstract

This thesis is about issues related to the security of electric substations automated by IEC61850, an Ethernet (IEEE 802.3) based protocol. It is about a comprehensive security analysis and development of a viable method of auditing the security of this protocol. The security analysis focuses on the possible threats to an electric substation based on the possible motives of an attacker. Existing methods and metrics for assessing the security of computer networks are explored and examined for suitability of use with IEC61850. Existing methods and metrics focus on conventional computers used in computer networks which are fundamentally different from Intelligent Electronic Devices (IED's) of substations in terms of technical composition and functionality. Hence, there is a need to develop a new method of assessing the security of such devices. The security analysis is then used to derive a new metric scheme to assess the security of IED's that use IEC61850. This metric scheme is then tested out in a sample audit on a real IEC61850 network and compared with two other commonly used security metrics. The results show that the new metric is good in assessing the security of IED's themselves. Further analysis on IED security is done by conducting simulated cyber attacks. The results are then used to develop an Intrusion Detection System (IDS) to guard against such attacks. The temporal risk of intrusion on an electric substation is also evaluated.

Keywords:
Information security, security analysis, security auditing, security metrics, IEC61850, security tools, substation automation, simulated attacks, intrusion detection

Acknowledgements

First and foremost I acknowledge the invaluable guidance and sincere encouragement from my supervisors Prof. Jagath Samarabandu and Prof. Tarlochan Singh Sidhu. My heartiest gratitude goes to Prof. Samarabandu for going out of the way to arrange this project with Prof. Sidhu.

I express my gratitude to Kinectrics, Inc. of Toronto for funding the research project and providing laboratory facilities to test the newly developed audit scheme. I deeply appreciate the kind cooporation of Bob Beresh, Principal Engineer, Protection and Control, Vince Green, Department Manager of Substations and Dr. Jian-Cheng Tan, Principal Engineer, Interoperability Testing Lab. I would also like to thank Harry Ou for his support and assistance during the sample audit at the Interoperability Lab and the support given by Yujie Yin and Babak Jamali.

I thank the Chair of the Department of Electrical and Computer Engineering for providing the research facilities. I gratefully acknowledge Prof. Ken MacIsaac for allowing to use his wireless communication equipment; Prof. Serguei Primak and Prof. Adballah Shami for allowing me to conduct sample security audits on their laboratory network; Prof. Luiz Capretz for providing the networking equipment for experimental setups. Also I am thankful to Tim Hunt, Network Administrator of the Spencer Engineering Building and the Information Technology Services of the University of Western Ontario for seeing to all networking needs of the project. I thankful to Sandra Vilovski, the Graduate Affairs Assistant of the department for her support and cooperation.

My gratitude goes to the Instructors of the courses I took for the M.E.Sc. program, Prof. Jagath Samarabandu, Prof. Tarlochan Sidhu, Prof. Abdallah Shami, Prof. Olga Veksler, Prof. Areski Nait-Abdallah and Prof. Charles Ling for their invaluable knowledge which on numerous occasions was helpful to my research.

Many thanks go to my colleagues of the Mobile Robotics and Computer Vision Laboratory; Eranga Ukwatta, Mehnaz Zouqi, Akila Subasinghe, Mahnaz Ahmadian, Mehdi Delroba, Duane Jaquies, Erik Webber, Bryan Godbolt and David Mickal and the Power System Protection Laboratory; Mitalkumar Kanabar, Palak Parikh, Injeti Shrichand and Nima Hejazi for the various helps provided to make this research a success. I appreciate the assistance provided by Mohammad Dadash Zadeh in familiarizing with the protection relays and Dan James Dechene for providing his advice and LaTeX style files used to write this thesis.

I take this opportunity to thank my home university, the University of Moratuwa, Sri Lanka for granting me leave to pursue this research degree. My sincere gratitude

goes to the Head of the Department of Electronic and Telecommunication Engineering, Eng. Kithsiri Samarasinghe and Dr. Rohan Munasinghe for recommending me for this project.

My thanks should especially go to Dr. Ranga Rodrigo, first for helping with finding accommodation in London. Had it not been so, finding a place to stay would have been the most difficult task for a newcomer to London after the commencement of a term. Secondly I must thank him for generously providing with all the necessary needs for accommodation. I also appreciate the helpful advice given by Dr. Nuwan Nanayakkara on life in London and at Western. I gratefully acknowledge my father Dr. Lalith Premaratne for proofreading the thesis manuscript. I would also like to thank the Sinhalese community of London for making my stay in London a pleasant one. I must also thank Manel and Gamini Premachandra of Toronto for providing accommodation during my visits to Kinectrics, Toronto.

My heartiest gratitude must go to my parents for their untiring guidance, encouragement and commitment. Last but not least my sincere thanks go to Uthpala Premarathne for her sincere encouragement.

Table of Contents

List of Tables

List of Figures

Acronyms

ARP	*Address Resolution Protocol*
CAM	*Content Addressable Memory*
CB	*Circuit Breaker*
CBR	*Constant Bit Rate*
CIP	*Critical Infrastructure Protection*
CL	*Connectionless*
CO	*Connection Oriented*
CPU	*Central Processing Unit*
CVE	*Common Vulnerabilities and Exposures*
CVSS	*Common Vulnerability Scoring System*
DLL	*Data Link Layer*
DoS	*Denial of Service*
FTP	*File Transfer Protocol*
GSSE	*Generic Substation Status Event*
GOOSE	*Generic Object Oriented Substation Event*
GUI	*Graphical User Interface*
HTTP	*Hyper Text Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
HMI	*Human Machine Interface*
ICMP	*Internet Control Message Protocol*
ID	*Intrusion Detection*
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IED	*Intelligent Electronic Device*
IRIS	*Image Recognition and Intelligent Systems*
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
MAC	*Medium Access Control*

MAC	*Message Authentication Code*
MMS	*Manufacturing Message Specification*
MTTC	*Mean Time to Compromise*
MU	*Merger Unit*
NERC	*North American Electrical Reliability Corporation*
NTP	*Network Time Protocol*
OLTC	*On Load Tap Changer*
OS	*Operating System*
OSI	*Open Systems Interconnection*
OTcL	*Object Oriented Tool Command Language*
PC	*Protection and Control Relay*
RMS	*Root Mean Square*
RSH	*Remote Shell*
SCADA	*Supervisory Control and Data Acquisition*
SFTP	*Secure File Transfer Protocol*
SNTP	*Simple Network Time Protocol*
SV	*Sample Value*
TCP/IP	*Transfer Control Protocol/Internet Protocol*
TFTP	*Trivial File Transfer Protocol*
TLS	*Transport Layer Security*
UCA	*Utility Communication Architecture*
UDP	*User Datagram Protocol*
UWO	*University of Western Ontario*
VEA-bility	*Vulnerability Exploitability Attackability*
VLAN	*Virtual Local Area Network*
WAN	*Wide Area Network*
WLAN	*Wireless Local Area Network*

Chapter 1 Introduction

1.1 Problem Statement

This thesis addresses the issue of analyzing the security of the IEC61850 protocol and coming up with a viable method of auditing the security aspects of this protocol.

IEC61850 is an Ethernet (IEEE 802.3) based protocol used for control and automation of electric substations. Since electric substations are critical installations in the electric power grid, they are a prime target for malicious attacks. Hence, there is a need to assure the safety and security of such substations. This is the motivation behind developing a scheme to audit the information security of such substations.

Existing schemes for auditing information security are tailored for conventional computer networks. The inherent technical differences of computers and Intelligent Electronic Devices (IED's) used in substation automation calls for a possible adaptation of such schemes or the development of an entirely new scheme. The development of such a scheme also requires a comprehensive threat assessment for electric substations based upon security analysis and simulated attacks on IED's. It is also necessary to assess the impact of such a scheme on the safety of the network. The final stage would be to test the auditing scheme on a real IEC61850 network. Data obtained during the launch of simulated attacks on IED's can be used to develop effective countermeasures for IEC61850.

1.2 Contributions

The contributions of this thesis include:

- Security analysis of IEC61850 automated substations using a defence oriented [1] and offence oriented [2] assessment.
- A metric scheme for assessing the security of an IED based. upon the goals of the attacker, vulnerabilities of the device and available countermeasures.

- Investigation of the effect of network security tools on the safety of IEC61850 networks.
- An Intrusion Detection System (IDS) for threats of IEC61850. networks based upon data obtained by launching simulated attacks on IED's.

1.3 Outline of Thesis

Chapter 2 gives an overview of the IEC61850 protocol. This is followed by a comprehensive security analysis in Chapter 3. The process of analyzing existing security metrics and designing a novel metric for IED's is given in Chapter 4. The design of the audit process and simulation of the impact of the security tools used for auditing on an IEC61850 network is detailed in the next chapter (Chapter 5). This is followed by the details of a sample audit (Chapter 6) carried out at the Interoperability Laboratory of Kinectrics, Inc. Chapter 7 presents the results of the findings on the security of IED's by performing simulated attacks. The next chapter (Chapter 8) assesses the possible temporal risk of intrusion while Chapter 9 details the development of an IDS based on the results of Chapter 7. This is followed by the conclusions in Chapter 10.

Chapter 2 Overview of IEC61850

2.1 Introduction

IEC61850 is an Ethernet (IEEE 802.3) based communication protocol used for control and automation of electric substations using microprocessor based Intelligent Electronic Devices (IED's). It was developed jointly by the IEC (International Electrotechnical Commission) and the IEEE with the aim of providing a flexible and interpretable communication system which could be easily integrated into the infrastructure of existing substations [3]. The entire standard is defined in a ten chapter document [4]. This chapter provides an overview of this protocol.

2.1.1 Power System Communication

Modern electric power systems are highly communication intensive, involving communication between numerous entities. A basic power system consists of generation, transmission and distribution. For reliable, efficient and safe operation of the power system, precise coordination is needed between these sections. With the proliferation of renewable energy sources, comes distributed generation where the power sources are scattered around a wide geographic area instead of being centralized as in traditional fossil fuel, nuclear or hydroelectric sources. Such coordination is also paramount for the emerging concept of microgrids where smaller distributed power sources are used to independently control *islands* of small loads at times of power outages. These technologies further increase the demand for reliable inter-entity communication.

An electric substation is a part of the distribution network which handles the stage between transmission from the power source and the distribution to the customer. It contains the stepping down transformers for reducing the high voltage of the transmission lines to the lower voltage needed for distribution. Along with this, there are the numerous equipment needed to regulate the voltage as the power demand fluctuates. In addition substations have protection equipment for safety. IEC61850 is a protocol used for control and automation of substations.

2.1.2 Deployment of IEC61850

The first multivendor IEC61850 automated substations in North America were the Bradley 500kV Substation owned by the Tennessee Valley Authority (Holback *et al.* [5]) and the La Venta II substation (Flores *et al.* [6]) of Mexico. Currently it is widely used in numerous European countries as well as in Latin America.

2.1.3 Research on IEC61850

One of the main focal points of research in IEC61850 is improving the capability to integrate it with devices that use legacy protocols (Prakash *et al.* [7] and Yi *et al.* [8]). Research is also carried out on the reliability of this protocol (Sidhu and Yin [9]) and improving configuration or modeling of systems (Zhanjun *et al.* [10] and Biel and Lian-shunl [11]). Another high interest area is integrating IEC61850 into a larger protocol suite for automation of the entire power grid (Chen *et al.* [12], Hughes [13] and Xu and Ma [14]).

2.2 IEC61850 Protocol Stack

The IEC61850 protocol is based upon the OSI model (Figure 2.1) with the majority of the real time process data and supervisory control information being transferred by the message format ISO 9506 also known as Manufacturing Message Specification (MMS). The IEC61850 protocol stack consists of five message formats.

1. Sample Value (SV) messages are used for transferring raw data values such as from instrument transformers. SV messages are time critical and directly map into the Ethernet hardware to reduce transfer times.

2. Generic Object Oriented Substation Event (GOOSE) messages are used for time critical peer to peer communication between IED's. Like SV messages, GOOSE messages are also time critical, typically requiring a transfer time of less than 4ms and map directly to the Ethernet hardware. It is possible to either broadcast or multicast GOOSE messages. Typically events such as the tripping of a protection relay use this message format.

3. TimeSync messages use UDP (User Datagram Protocol) and transfers time synchronization information for IED's.

4. Manufacturing Message Specification (MMS) allows communication on a client server basis using mappings between TCP/IP and IEC61850. This message format can operate over the connection-oriented OSI protocol stack as well and was used by Utility Communication Architecture (UCA), the predecessor of IEC61850.

5. Generic Substation Status Event (GSSE) messages are connectionless messages used to obtain status information of IED's. Like MMS this message format was also used by UCA and is designed to operate over connectionless OSI.

Figure 2.2 shows the stack of the four message formats that use Ethernet. IEC61850 is also designed to be used on IEEE 802.1Q Virtual LAN (VLAN) technology. Using this it is possible to form virtual groups of IED's according to their function and implement features such as priority tagging for GOOSE messages.

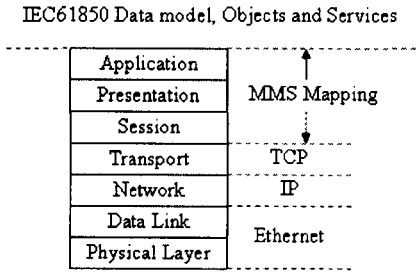


Figure 2.1: IEC61850 Mapping to OSI

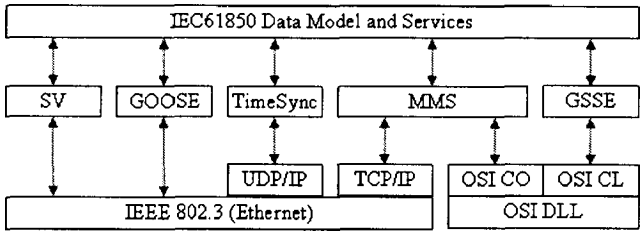


Figure 2.2: IEC61850 Protocol Stack

IEC61850 also categorizes messages according to time criticality. Based on this, 6 types of messages are defined [15].

1. Type 1 (Fast Messages) which carry critical messages which should be delivered within 3-100ms depending on the application. An IED is supposed to immediately react to a time critical message such as in the case of a relay being tripped.

2. Type 2 (Medium Speed Messages) which are clocked by the internal clocks of IED's and require a transmission time of less than 100ms. Transferred root mean square measurements of voltages and currents are typically of this type.

3. Type 3 (Low Speed Messages) messages are used for event recording and complex messages. These require a transfer time of less than 500ms.

4. Type 4 (Raw Data) messages are sampled data values (such as from current or potential transformers) transmitted as a stream of digitized data.

5. Type 5 (File Transfer) which are used for transferring files of data.

6. Type 6 (Time Synchronization) messages are used for time synchronization of IED's of a network based on a timestamp obtained from a global positioning system.

2.3 IEC61850 Based Automation

2.3.1 Basic Operation

In a substation automated by IEC61850, the IED's communicate via this protocol. An IED could be a measuring instrument such as a current transformer or voltage transformer, a switching device such as a voltage regulating transformer or a protection device such as a relay. During operation, they will communicate with each other on a peer to peer, broadcast or client server basis. For example, a current transformer may sense a dangerous increase in current and broadcast the value, resulting in the tripping of safety devices.

2.3.2 Device Organization

2.3.2.1 Physical Device

The physical device is the actual device connected to the power system and the network. This can be a measuring device, protective device or switching device.

2.3.2.2 Logical Device

A logical device makes the logical connection to the network. IEC61850 is defined in such a way that multiple physical devices can map into a single logical device (Figure 2.3). In such a scheme the main physical device will act as a proxy to the remaining devices.

2.3.2.3 Logical Node

The logical devices are then mapped into logical nodes. Each logical node will contain a collection of standard data classes. The logical nodes are grouped according to a common functionality. Hence, it is possible for a single logical device to have multiple logical nodes if the physical device has multiple functions (Figure 2.3). The arrangement of the system of logical nodes could be on a client-server basis in the case of data recording or master-slave basis for automatic or supervisory control.

Figure 2.4 gives an example practical arrangement for voltage regulation using a transformer protection IED. The labeled logical nodes of the setup include those that provide data outputs such as the disturbance record (RDRE) and the RMS demand (MMXU). There are also logical nodes that give outputs for protection control such as overcurrent protection (PIOC), under voltage protection (PTUV) and over voltage protection (PTOV). The logical nodes labeled ATTC and YLTC are used to control the tap changer (OLTC) for regulating the voltage while CILO, CSW1 and XCBR1 handle the breaker and devices that depend on it. The current measurement input for the IED corresponds to logical node TCTR1 while the TVTR1 and TVTR2 correspond to the voltage inputs for the high voltage and low voltage buses respectively.

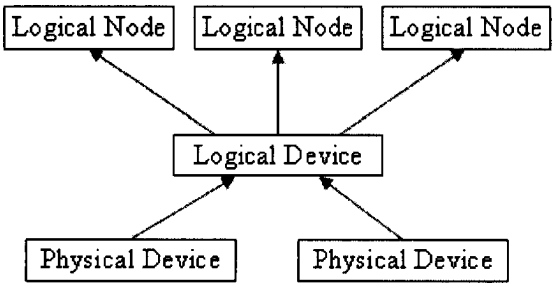


Figure 2.3: Device Topology

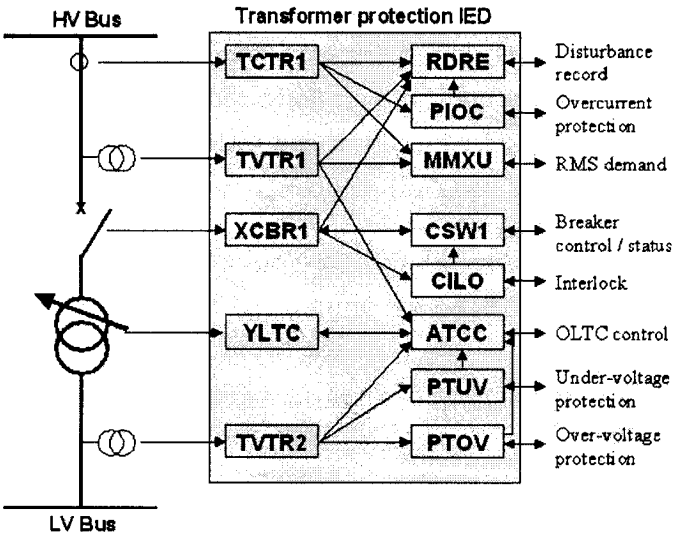


Figure 2.4: A Practical Device
Taken from Sidhu and Gangadharan [15]

2.3.2.4 Object Name Structure

The IEC61850 object name structure consists of the logical device that needs to be addressed, the logical node, the functional constraint, the data and the attribute. A sample object name of a protective relay is given by Figure 2.5 in which the logical node is the circuit breaker labeled XCBR1. The functional constraint is the status of the relay labeled ST.

Logical Device	Logical Node	Functional Constraint	Data	Attribute
Relay1	*XCBR1*	*ST*	*Loc*	*stVal*

Figure 2.5: IEC61850 Object Name Structure

2.3.3 Topologies

The network of IED's within a substation contains two main components known as busses.

1. Process Bus - which transfers unprocessed power system information to the processing IED's. This data is then used by the respective IED's and used for decision making. A substation may contain several such busses. Since the amount of traffic in a process bus tends to be high due to the large amount of unprocessed data, partitioning reduces the overall burden of the network.

2. Station Bus (System Bus) - the system bus integrates all process buses together and provides the interface to external networks. Generally, the HMI (Human Machine Interface) of the substations are also connected to the system bus. In addition, it may contain data logging and backup servers. The system bus could either be connected directly to a WAN through a gateway or indirectly through another LAN within the substation.

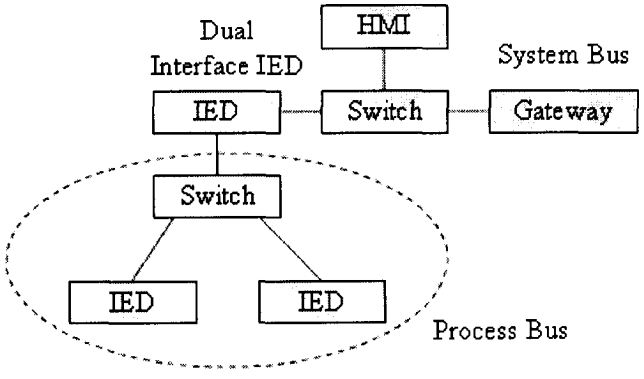


Figure 2.6: Segmented Process Bus Topology

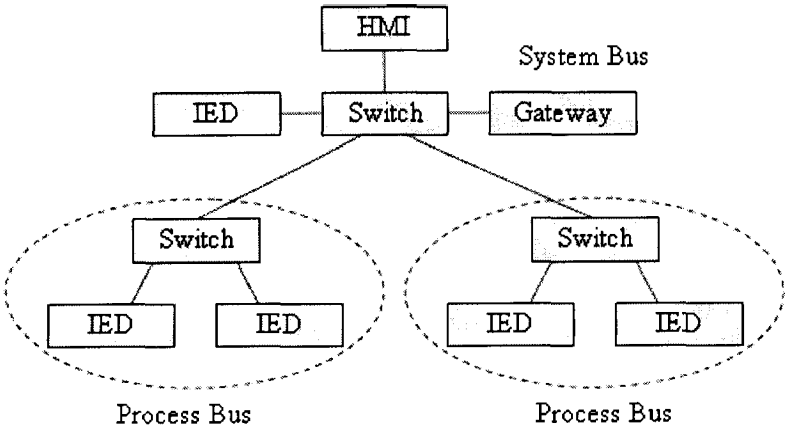


Figure 2.7: Merged Process Bus Topology

The common topologies used include the segmented process bus and the merged process and system bus [16]. In the segmented topology (Figure 2.6), the process bus and system bus are isolated from one another through an IED which has two Ethernet interfaces. This decreases network traffic but reduces the capability to control and monitor the process bus. In the merged topology (Figure 2.7), each process bus is isolated via a switch which is in turn directly connected to the switch of the system bus. This increases network traffic but allows better control and monitoring of IED's.

2.3.4 Future Wireless Extensions

Research is currently underway to include wireless extensions to IEC61850 based systems. In the future it is very likely that IED's could be connected to the system via wireless access points based upon IEEE 802.11 (WiFi) for flexibility and additional redundancy. The inclusion of wireless local area networks (WLAN's) adds new dimensions to the system.

Chapter 3 Security Threats to IEC61850

3.1 Introduction

Electric substations are critical installations in the electric power grid. Hence a possible prime target for malicious activity by various parties. Therefore, it is vital to look into a viable security scheme to mitigate the effect of such attacks on a substation automated by IEC61850. This chapter describes the security analysis done on this protocol.

3.2 Basic IEEE 802.3 Ethernet Issues

According to Dolezilek [16] the main security issues of IEC61850 automated substations due to the use of IEEE 802.3 can be summarized as:

1. Operation of the network during Ethernet failure.
2. Information security of the network.
3. Network overload caused by newly connected IED's, test devices or technical laptops.
4. IED CPU (Central Processing Unit) overload due to network communication.

Out of these, the second issue falls within the scope of information security. The first and third issues fall within the scope of reliability [17], [9] while the fourth issue falls within the design and construction of the IED itself.

3.3 Security Analysis

The purpose of security analysis is to identify the possible threats to a IEC61850 automated substation. Numerous schemes exist for the identification of various aspects of information and network security. These schemes can be separated into two main categories; which are, identification according to the perspective of a defender or an attacker.

3.3.1 Defender Perspective

Security analysis in the perspective of the defender involves looking at the security requirements of the defender. This leads to a security policy which in turn requires security mechanisms to enforce [1]. The enforceability of a security policy depends on the mechanisms used [18] which should be selected in a manner that they do not compromise the performance of the system [19], [20].

3.3.2 Attacker Perspective

The other method of security design involves looking at the problem through the perspective of the attacker [2]. Intuitively, this perspective is more effective because an attacker is always motivated to achieve the set goal. Research in this context is more realistic because, realistic data can be obtained through simulated attacks [21] and by setting up bait networks known as Honeypots [22]. In a Honeypot, a network is set up with the intent of luring and recording the behavior of hackers. It is probably the most realistic because intrusions on them are made by real world attackers [23]. Attack scenarios can also be simulated by using game theory [24].

3.3.3 Application to IEC61850

The next step would be to apply the analysis technique to the IEC61850 based system. The main challenge is that a network of a IEC61850 automated substation is not structured and utilized like a computer network of an organization.

A typical network of a substation is shown in Figure 3.1. It is complete with wireless access points. Figure 3.2 shows the interconnection of substations with the central office via a WAN. Analysis of a conventional network can be done simply by using the scheme proposed by Ohta and Chikaraishi [25]. In this method, a

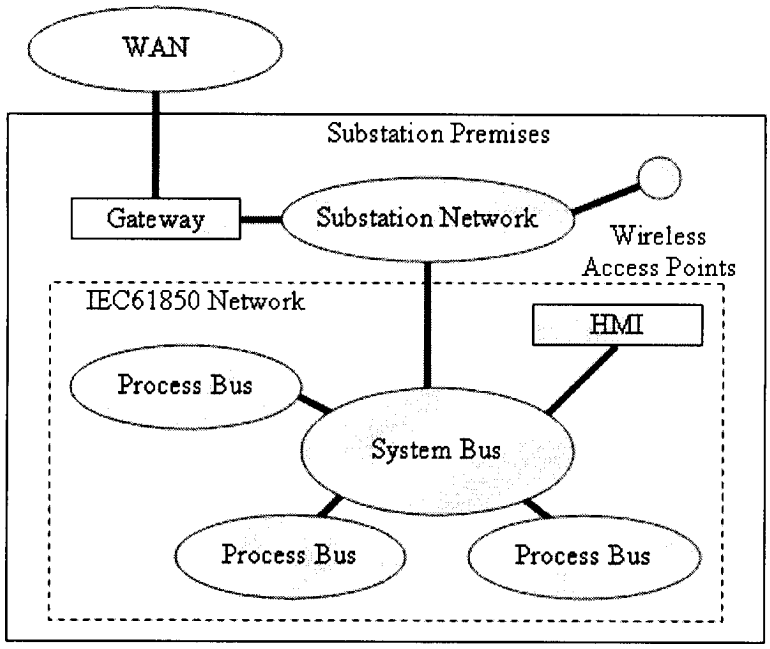


Figure 3.1: Substation Network

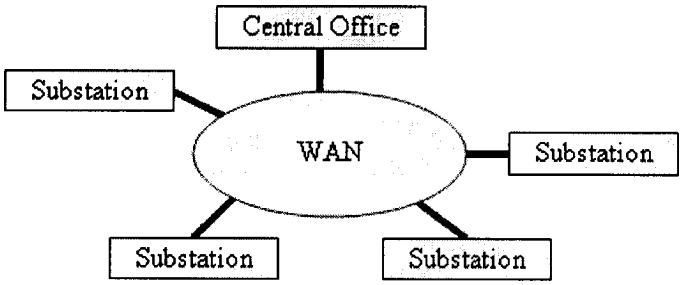


Figure 3.2: Substation Interconnection

network is broken up into four layers, the data layer, the node layer, the LAN layer and the internetworking (WAN) layer (Figure 3.3). Not all nodes of a network may contain data (e.g. printers). Once these layers have been identified, the interfaces and methods of access can be analyzed (Figure 3.4).

An alternative to this method is *security domain analysis* proposed by Ericsson

and Torkilseng [26]. However, this method is more suited to security analysis of an entire utility on a macro scale. In security domain analysis the entire substation is taken as a security domain with the power plants, real time control, telecommunication section etc. being the other domains.

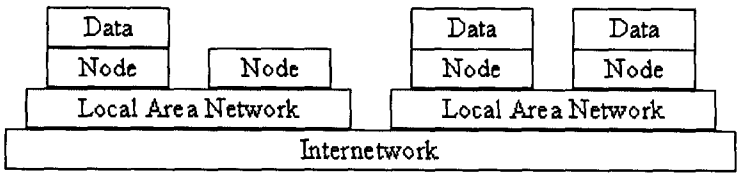


Figure 3.3: Model of a Computer Network

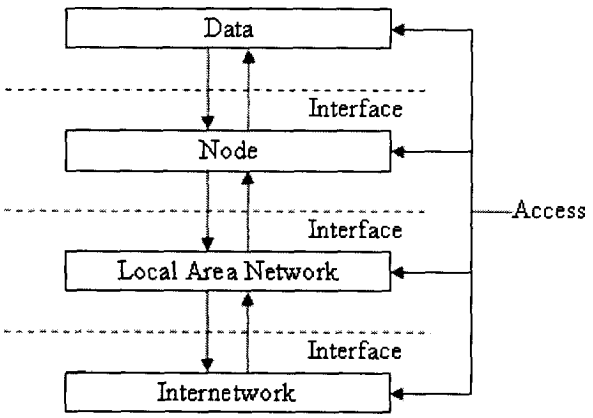


Figure 3.4: Computer Network Layer Interfaces

An IEC61850 network mainly consists of IED nodes that do not contain data similar to that of a network terminal. The nodes that would contain data would be data storage and backup servers connected to the system bus. The IED nodes may also not have explicit access similar to that of a network terminal, such access would be included only in the HMI and servers of the system bus.

3.3.4 Threat Identification

Stallings [27] lists four types of attacks on information security which are:

1. Interruption (attack on availability) where legitimate users are denied the availability of the information or services.

2. Interception (attack on confidentiality) where an unauthorized user gains access to the information content.

3. Fabrication (attack on authenticity) where fabricated information generated by the attacker is used to mislead other legitimate users.

4. Modification (attack on integrity) where an attacker modifies the information content with the intent of misleading.

In the context of a substation, two main attacker goals can be identified using the attacker perspective approach [2]. These are:

1. Disruption of the utility service (an attack on availability).

2. Gaining access to confidential information for malicious purposes such as unfair competition, blackmail etc (a breach on confidentiality).

When compared to the types of attacks listed by Stalling [27], only two of the four are listed. This is because unlike in for example a financial institution such as a bank where modification and fabrication would be likely goals of the attacker, in a substation both modification and fabrication would be used as techniques to fulfill the two main goals. For example, an attacker may send false information or modify existing information to confuse a substation into shutting down, hence achieving the goal of disrupting the service. It is also possible for an attacker to gain confidential information by fabrication or modification attacks.

These two goals can then be analyzed in detail to identify the methods an attacker can use to achieve them. These can be identified using the approach of Ohta and Chikaraishi [25].

Layer	Attack	Security Mechanisms
Node	Access to node to gain confidential information	Access control Encryption Authentication Integrity checking Intrusion detection
	False command	Authentication Integrity Checking
LAN	Access to the LAN or WLAN infrastructure to intercept confidential information	Access control (both physical and logical) Encryption Authentication Integrity checking Intrusion detection
	False command	Authentication Integrity Checking
WAN	Interception of confidential information en route on the WAN	Encryption Authentication Integrity checking
	False command	Authentication Integrity Checking

Table 3.1: Attacks on Confidentiality

3.3.4.1 Types of Attacks

An attack on confidentiality can be inflicted at the node, LAN or WAN levels. Table 3.1 shows the attack scenarios and security mechanisms to counter such attacks. These include, accessing the confidential information at a node, intercepting it while in transit or the use of a false command (masquerade) to trick the system into divulging the information. Disruption of services can take place at all levels (Table 3.2) and can consist of DoS or false command attacks. Since the WAN is out of the control of the parties that use it, the security mechanisms available for attacks on the WAN are limited.

3.3.4.2 Collateral Damage

There is also the possibility that the substation may have to face collateral damage. In such a case, the substation is not the intended target or a specific target of the attack. Examples include, a malware infection where there is no clear target or a

Layer	Attack	Security Mechanisms
Data	Data destruction	Backup procedure
Node	Using a node for a DoS attack	Access control Authentication Integrity checking Intrusion detection
	DoS attack on a critical node	Access control Authentication Integrity checking Intrusion detection Redundancy
	False command	Authentication Integrity Checking
LAN	DoS attack on LAN or WLAN infrastructure	Access control (both physical and logical) Authentication Integrity checking Intrusion detection Redundancy
	False command	Authentication Integrity Checking
WAN	DoS attack on WAN infrastructure	Redundancy
	False command	Authentication Integrity Checking

Table 3.2: Disruption of Service

general attack on a WAN used by substations for communication, where all traffic on the WAN will be affected.

3.3.4.3 Social Engineering Threats

Another major aspect of security that cannot be taken for granted is the social engineering (back door entry) risk. The attack scenarios of Tables 3.1 and 3.2 all deal with attacks directly on the network infrastructure. In a social engineering attack, the human operator is either tempted or deceived into compromising security. Attacks from bad security practice also fall into this category. In such an attack, the intruder takes advantage of bad practice to obtain information on compromising the system. Hence, this aspect also warrants serious consideration and scrutiny.

3.4 IEC61850 Security Mechanisms

Supervisory Control and Data Acquisition (SCADA) networks tend to have low levels of security. The first reason is the bandwidth and computational constraints of industrial networks [28] which are geared towards reliability. The second is due to the *false sense of security* that occurred because in the recent past, most industrial networks were isolated from the enterprize networks of the same organization [29], [30], [31]. This is however rapidly changing with increased interconnection of industrial and enterprize networks, paving way for an attacker to compromise the insecure industrial network.

IEC61850 was a protocol designed with security in mind. The existing security mechanisms of IEC61850 are mentioned in IEC62351-4 and IEC62351-6 [32]. These include:

1. IEC62351-4 specifies the ciphers used by IEC61850 for encryption. In addition, IEC62351-6 specifies the use of Transport Layer Security (TLS) using TLS_DH_RSA_WITH_AES_128_SHA.

2. Security for IEC61850 profiles using VLAN's. Partitioning of the network into VLAN's prevent unauthorized access of IED's outside the designated VLAN.

3. Security for Simple Network Time Protocol (SNTP) via the mandatory use of the authentication algorithms of RFC2030. This prevents tampering via false time stamp packets.

4. Explicit countering of man-in-the-middle attacks and tampering using the Message Authentication Code (MAC) of IEC62351-6.

5. Explicit countering of replay attacks via the specialized processing state machines mentioned in IEC62351-4.

These mechanisms would counter a significant amount of threats mentioned in Tables 3.1 and 3.2. In addition, the North American Electrical Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard for the protection of critical cyber assets [33], requires the incorporation of firewalls and anti-malware for compliance. This would counter a significant proportion of the remaining threats. However, over time a determined attacker is bound to innovate new methods to compromise these existing security mechanisms. This is especially true in the case of DoS

attacks since the mechanisms offer only limited protection which does not rank to the degree of a powerful security mechanism such as an Intrusion Detection System (IDS).

Chapter 4 Security Metric Analysis

4.1 Introduction

This chapter focusses on the analysis of existing metric schemes developed for assessing the security of computer networks. It also describes the development of a novel metric scheme for assessing the security of IED's.

4.1.1 Motivation

The main motivation behind research into obtaining metrics for network security is to provide people involved with secure netorks with a tangible means of measuring the security of a network [34]. This would have different implications on different types of jobs and people. For example, to a system designer it would provide a reasonable method to analyze the costs and benefits of a security mechanism. For a security auditor it would provide a means to assess and convey the security of a network to a client.

4.1.2 Existing Metric Schemes

Numerous authors have proposed different types of metrics to assess the security of a system focussing on the attacker. These include Pamula *et al.* [35] who express the security of a metric in terms of the weakest adversary that can compromise it. Another proposed metric is the Mean Time to Compromise (MTTC), proposed by Leversage and Byres [36] and McQueen *et al.* [37]. The Common Vulnerability Scoring System (CVSS) [38] is a widely used scheme in the field. It is used as the basis for security metric systems such as VEA-bility [39] and was cited as an emerging standard in IEEE Security and Privacy [40]. Out of these metric schemes, the MTTC and the VEA-bility metric are chosen for testing on IEC61850.

4.2 Metric Calculation

4.2.1 Mean Time to Compromise Metric

The MTTC metric is obtained by breaking up the actions of the attacker into three statistical processes. The time to compromise is the total time taken for the three processes which is given by:

$$T = t_1 P_1 + t_2(1 - P_1)(1 - u) + t_3 u(1 - P_1) \tag{4.1}$$

Where the periods t_1, t_2 and t_3 are taken in days. The value of T can be calculated either by the McQueen method [37] or the Leversage and Byres method [36]. The value t_1 is taken as 1 day based upon the stipulation of McQueen *et al.* [37]. The value P_1 is obtained from Equation 4.2. Similarly t_2 is calculated from Equation 4.3. The values of u and t_3 are obtained from Equations 4.6 and 4.7 respectively for the Leversage and Byres method or from Equations 4.8 and 4.9 respectively for the McQueen method.

4.2.1.1 Process 1

Process 1 is the process where the attacker has identified one or more known vulnerabilities and has one or more exploits on hand. The probability of the attacker being in this process is given by:

$$P_1 = 1 - e^{-\frac{\alpha m V}{k}} \tag{4.2}$$

where V is the number of vulnerabilities, α is the visibility factor, m is the number of readily available exploits to the attacker depending on the skill of the attacker. The value k is the total number of non-duplicate known vulnerabilities. The values of α, m and k are given in Table 4.1.

When considering the skill of an attacker, a beginner is an attacker only capable of utilizing existing code, tools and attack methods. An intermediate is an attacker capable of modifying existing code, tools and attack methods while an expert is capable of creating new code, tools and attack methods.

Variable	Definition	Value	Source
k	Total number of non-duplicate known vulnerabilities	9447	ICAT Database [37]
α	Visibility reduction factor of vulnerabilities due to boundary devices such as firewalls (depends on the number of security reviews conducted during a year)	1 (no reviews) 0.3 (semi annual) 0.12 (quarterly) 0.05 (monthly)	Leversage and Byres [36]
s	Variable to quantify the skill level of an attacker	0.5 (beginner) 0.9 (intermediate) 1 (expert)	Leversage and Byres [36]
m	Number of readily available exploits (McQueen method)	150 (beginner) 250 (intermediate) 450 (expert)	McQueen *et al.* [37]
m	Number of readily available exploits (Leversage and Byres method)	450s	Leversage and Byres [36]
$\frac{V_A}{V}$	Ratio of the average number of vulnerabilities which the attacker can exploit at the given skill level to the total number of available vulnerabilities.	0.3 (beginner) 0.55 (intermediate) 1 (expert)	McQueen *et al.* [37]

Table 4.1: Variables and Constants for MTTC Calculation

4.2.1.2 Process 2

This process is when the attacker has identified one or more known vulnerabilities but does not have an exploit on hand. The time spend for this is given by:

$$t_2 = 5.8N \tag{4.3}$$

where N is the expected number of tries. The expected number of tries is given by:

$$N = \left(\frac{V_A}{V}\right)\left[1 + \sum_{n=2}^{V-V_A+1}\left[n\prod_{i=2}^{n}\left(\frac{V_M - i + 2}{V - i + 1}\right)\right]\right] \tag{4.4}$$

where V_A is the average number of vulnerabilities the attacker can exploit for the given skill level. V_M is the number of vulnerabilities that the attacker cannot exploit.

It is related to V and V_A by the equation:

$$V = V_A + V_M \tag{4.5}$$

The value of V_A is given in terms of the ratio $\frac{V_A}{V}$ (Table 4.1). The derivation of Equation 4.4 is given in detail in McQueen *et al.* [37].

4.2.1.3 Process 3

Process 3 occurs when there are no known exploits or vulnerabilities available. This depends on the success of Process 2. According to the Leversage and Byres method, the probability of Process 2 being unsuccessful is given by:

$$u = (1-s)^{\alpha V} \tag{4.6}$$

where s is a variable that indicates the skill level of the attacker. The possible values of s are given in Table 4.1. The time spent on Process 3 is given by:

$$t_3 = 30.42\left[\left(\frac{1}{s}\right) - 1\right] + 5.8 \tag{4.7}$$

When the McQueen method is used, the values of u and t_3 are obtained in terms of $\frac{V_A}{V}$. Therefore the respective equations become:

$$u = \left[1 - \left(\frac{V_A}{V}\right)\right]^{\alpha V} \tag{4.8}$$

$$t_3 = 30.42\left[\left(\frac{V}{V_A}\right) - 1\right] + 5.8 \tag{4.9}$$

4.2.1.4 Final Equations

By substituting Equations 4.2, 4.3, 4.8 and 4.9 to Equation 4.1 the final equation for T' according to the McQueen method becomes:

$$T = \left(1 - e^{-\frac{\alpha m V}{k}}\right) + 5.8Ne^{-\frac{\alpha m V}{k}}\left[1 - \left[1 - \left(\frac{V_A}{V}\right)\right]^{\alpha V}\right] + \left[30.42\left[\left(\frac{V}{V_A}\right) - 1\right] + 5.8\right]\left[1 - \left(\frac{V_A}{V}\right)\right]^{\alpha V} e^{-\frac{\alpha m V}{k}} \tag{4.10}$$

The final equation for T according to the Leversage and Byres method is obtained by substituting Equations 4.2, 4.3, 4.8 and 4.9to Equation 4.1. This yields:

$$\begin{aligned} T &= \left(1 - e^{-\frac{\alpha m V}{k}}\right) + 5.8Ne^{-\frac{\alpha m V}{k}}\left[1 - (1-s)^{\alpha V}\right] \\ &\quad + \left[30.42\left[\left(\frac{1}{s}\right) - 1\right] + 5.8\right](1-s)^{\alpha V}e^{-\frac{\alpha m V}{k}} \end{aligned} \tag{4.11}$$

4.2.1.5 Feasibility

When T for a given number of vulnerabilities obtained from both methods are plotted using Equations 4.10 and 4.11, it becomes apparent that the results from the McQueen method (Figure 4.1) are highly realistic. The oscillations in the graph are due to the rounding up of fractional values of $\frac{V_A}{V}$. The results from the Leversage and Byres method (Figure 4.2) appear to be inconsistent, especially for the case of an intermediate user (Figure 4.2b) where the MTTC increases for less than 20 vulnerabilities, when it should decrease. Therefore, for future calculations, the McQueen method is used since it is more realistic.

4.2.2 VEA-bility Metric

The VEA-bility metric is based upon the CVSS system [38] proposed by Tupper and Zincir-Heywood [39]. This system begins by evaluating the known vulnerabilities of each individual node of the network. For each vulnerability, the impact score ($I_S(v)$), temporal score ($T_S(v)$) and exploitability score ($E_S(v)$) are obtained. From this, the severity of the vulnerability is obtained from:

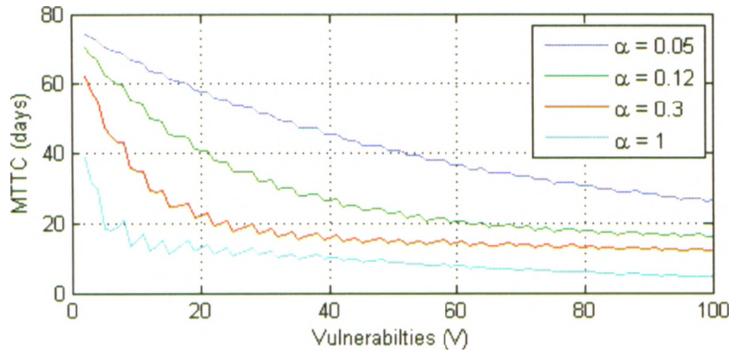
$$S(v) = \frac{I_S(v) + T_S(v)}{2} \tag{4.12}$$

This is then used to find the metrics for the host due to the total number of vulnerabilities. The metrics include the host vulnerability,

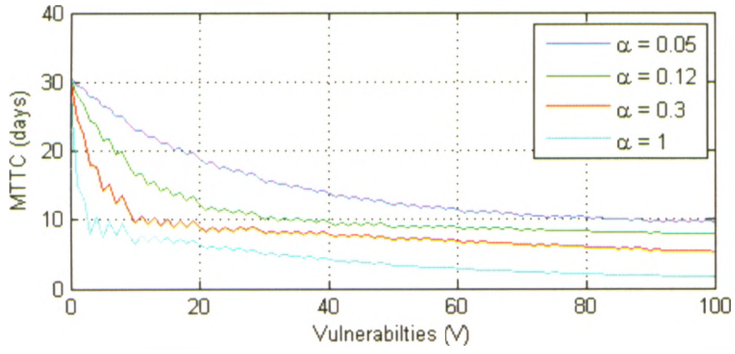
$$V(h) = min\left(10, ln\left[\sum e^{S(v)}\right]\right) \tag{4.13}$$

and the host exploitability,

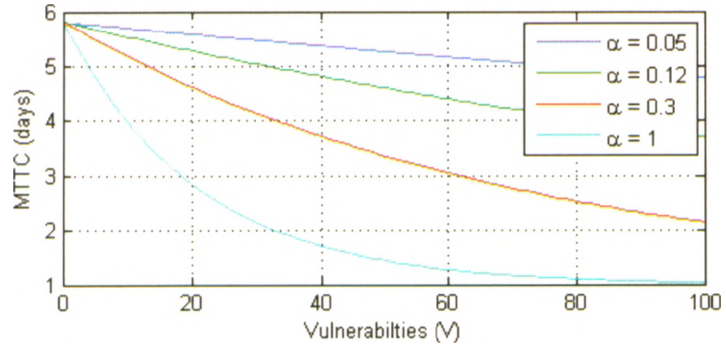
$$E(h) = \frac{u_h}{u_N} min\left(10, ln\left[\sum e^{E_S(v)}\right]\right) \tag{4.14}$$



(a)



(b)

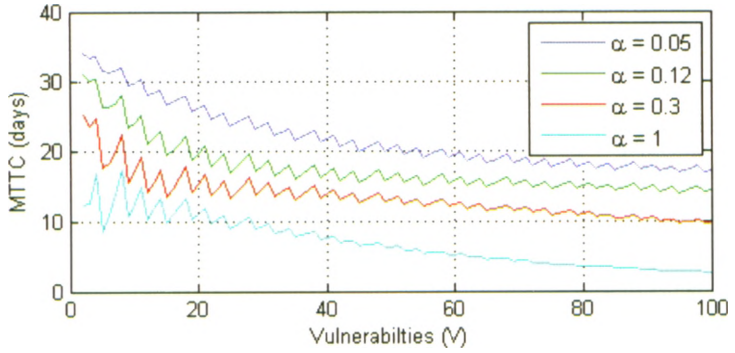


(c)

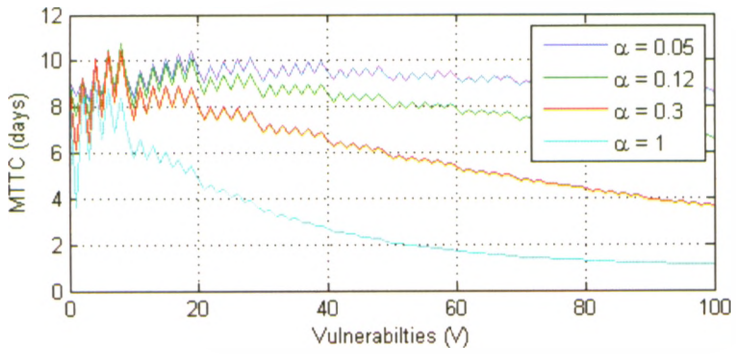
Figure 4.1: MTTC Estimate vs. Number of Vulnerabilities (McQueen Method) An estimate of the time a (a) beginner (b) intermediate (c) expert will take to compromise a host depending on the number of vulnerabilities.

where u_h and u_N are the number of services on the host and network respectively. The attackability of the host is given by:

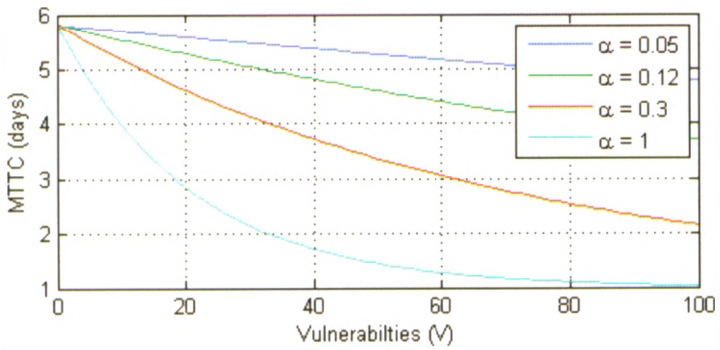
$$A(h) = \frac{10p_A}{p_N} \tag{4.15}$$



(a)



(b)



(c)

Figure 4.2: MTTC Estimate vs. Number of Vulnerabilities (Leversage-Byre Method) An estimate of the time a (a) beginner (b) intermediate (c) expert will take to compromise a host depending on the number of vulnerabilities.

where p_A is the number of attack paths and p_N is the number of network paths. Upon calculating the scores for each host, the corresponding values for the entire network

are obtained from:

$$V(n) = min\left(10, ln\left[\sum e^{E(h)}\right]\right) \quad (4.16)$$

$$E(n) = \sum E(h) \quad (4.17)$$

$$A(n) = \sum A(h) \quad (4.18)$$

From this the final VEA-bility score of the network ($R(n)$) is calculated from:

$$R(n) = 10 - \left(\frac{V(n) + E(n) + A(n)}{3}\right) \quad (4.19)$$

4.3 Preliminary Analysis

4.3.1 Sample Data

In order to test the two metric systems on real data, both metrics are tested on the hosts of the IRIS network (Figure 4.3) of the Computer Vision and Mobile Robotics Laboratory of the University of Western Ontario. The network consists of 9 hosts of which all run different types of services. The details of each host are given in Table 4.2. All of the hosts are scanned using the security tool *Nessus 3.2.1* [41]

Host ID	Host Name	Operating System
Host 1	Amila	Gentoo Linux (Kernel 2.6)
Host 2	Nilwala	Windows XP SP2
Host 3	Mahaweli	Gentoo Linux (Kernel 2.6)
Host 4	Deduru	Windows XP SP2
Host 5	Asela	Gentoo Linux (Kernel 2.6)
Host 6	Kala	Gentoo Linux (Kernel 2.6)
Host 7	Kalu	Windows XP SP2
Host 8	Mee	Windows XP Professional
Host 9	Kelani	Windows XP SP2

Table 4.2: IRIS Host Details

for vulnerabilities. Table 4.3 contains the number of open ports and vulnerabilities of each host as detected by *Nessus 3.2.1*. Table 4.4 contains the CVSS scores of the important vulnerabilities of each host as detected by *Nessus 3.2.1*. Hosts 5, 6 and 8 contain no vulnerabilities with CVSS scores. The data from the scan is then entered

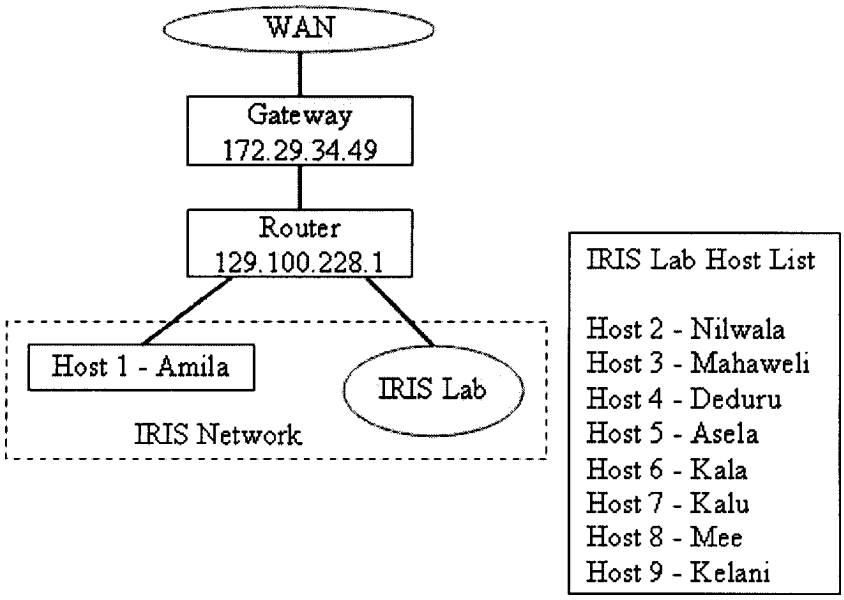


Figure 4.3: IRIS Network

into a Microsoft Access database and the calculation of the metrics are done using MATLAB.

Host	Open Ports	Vulnerabilities		
		Low Risk	Medium Risk	High Risk
Host 1	2	13	2	0
Host 2	7	24	3	1
Host 3	7	27	2	2
Host 4	13	35	3	1
Host 5	2	12	1	0
Host 6	5	18	5	0
Host 7	3	21	2	0
Host 8	3	9	1	0
Host 9	4	22	3	1

Table 4.3: IRIS Host Vulnerabilities

Host	CVE	Score		
		Base	Impact	Exploit
Host 2	CVE-1999-0505	7.2	10	3.9
	CVE-2002-1117	5	2.9	10
	CVE-2005-1794	6.4	4.9	10
Host 3	CVE-2002-1117	5	2.9	10
	CVE-2007-2446	10	10	10
Host 4	CVE-1999-0505	7.2	10	3.9
	CVE-2002-1117	5	2.9	10
	CVE-2005-1794	6.4	4.9	10
Host 7	CVE-1999-0505	7.2	10	3.9
	CVE-2002-1117	5	2.9	10
Host 9	CVE-1999-0505	7.2	10	3.9
	CVE-2002-1117	5	2.9	10
	CVE-2005-1794	6.4	4.9	10

Table 4.4: IRIS Host Vulnerability CVSS Scores

4.3.2 Sample Calculation

For the sample calculation of the MTTC, the total vulnerabilities for a host is obtained by the formula:

$$V = 0.1V_{LR} + 0.5V_{MR} + V_{HR} \tag{4.20}$$

where V_{LR}, V_{MR} and V_{HR} are respectively the number of low, medium and high risk vulnerabilities. After the MTTC is calculated for all hosts, the mean is taken as the MTTC score of the entire network. The McQueen method is used. In order to obtain the VEA-bility metric, the host attackability is taken as zero since the entire network is protected from external threats by a firewall [39]. The assumption that the host attackability becomes zero in the presence of a firewall is based upon the fact that a firewall can counter a majority of the attack paths an attacker may follow.

4.3.3 Results

The scan results are then used to calculate the MTTC. Table 4.5 shows the MTTC for the network for the *worst case* (expert attacker) for no firewall updates ($\alpha = 1$) and monthly updates ($\alpha = 0.05$). In either case, the value is calculated for the initial

network condition (*before*) and after the vulnerabilities are mitigated by patching the high risk vulnerabilities (*after*). The VEA-bility score of the network is also calculated (Table 4.6). The initial VEA-bility score of the network is 4.2029. After the vulnerabilities are mitigated, it increases to 10.

Host	MTTC (days)			
	$\alpha = 1$		$\alpha = 0.05$	
	Before	After	Before	After
Host 1	5.4	5.4	5.8	5.8
Host 2	4.8	5.0	5.7	5.8
Host 3	4.6	5.0	5.7	5.8
Host 4	4.6	4.8	5.7	5.7
Host 5	5.4	5.4	5.8	5.8
Host 6	5.0	5.0	5.8	5.8
Host 7	5.2	5.2	5.8	5.8
Host 8	5.6	5.6	5.8	5.8
Host 9	4.8	5.0	5.7	5.8
MTTC (days)	5.0	5.1	5.8	5.8

Table 4.5: IRIS MTTC Results

Host	$V(h)$	$E(h)$
Host 1	0	0
Host 2	10	1.5217
Host 3	10	1.5217
Host 4	10	2.8261
Host 5	0	0
Host 6	0	0
Host 7	10	0.6522
Host 8	0	0
Host 9	10	0.8696
VEA-bility Score		4.2029

Table 4.6: IRIS VEA-bility Results

4.3.4 Interpretation of Results

After mitigating the vulnerabilities, the VEA-bility score of the network increases from 4.2029 to 10. However, the MTTC does not change significantly. On the other

hand, since the network attackability, exploitability and vulnerability scores do not exceed 10, it would not be able to indicate the risk of a highly insecure network with many vulnerabilities. However, the results of the the MTTC (Figure 4.1) would be able to indicate this, especially if the number of vulnerabilities of the network were greater than 10 and the firewalls of the network were not updated.

4.3.5 Alternative MTTC Formula

The low resolution of the MTTC when the total number of vulnerabilities per host is calculated using Equation 4.20, appears to be impractically low. Hence an alternative form is tried out. In it, the total number of vulnerabilities of the entire network of N_H hosts is calculated. This is then used to calculate the MTTC of the entire network directly. For this, Equation 4.20 would become:

$$V = \sum_{i=0}^{N_H} \left[0.1V_{LR_i} + 0.5V_{MR_i} + V_{HR_i} \right] \tag{4.21}$$

When the alternative MTTC is calculated, the results (Table 4.7) show more variation especially when α is unity. Therefore, it is reasonable to consider α to be unity throughout the calculations. If its value is less than this, the MTTC calculation would become meaningless as a security metric. This is because the difference between an insecure network (before vulnerabilities are fixed) and secure network (after vulnerabilities are fixed) would be insignificantly small.

Network	MTTC (days)	
	Before Mitigation	After Mitigation
No Updates ($\alpha = 1$)	1.9	2.2
Monthly Updates ($\alpha = 0.05$)	5.4	5.5

Table 4.7: Alternative MTTC for the Entire IRIS Network

Even this MTTC calculation is unrealistic when considering the fact that in real life attackers usually take an attack path. For example, in order to compromise a particular machine, the attacker may have to look for a particular stepping stone vulnerability within another machine of the network. Hence, using Equation 4.21 can also be considered unrealistic.

This leads to the attack path MTTC approach taken by Leversage and Byres [36]. In this case the MTTC is calculated for each path and the total MTTC is obtained by summing up the products of the MTTC of probable path and the likelihood of taking that path based on its relative difficulty. The likelihood and difficulty can be obtained from statistical data of real attacks. However, the ability to utilize statistical data obtained from a real or simulated attack is highly doubtful. This is because the scenarios and paths for the attack are highly case specific. Hence, using data from one attack to model another may be unreasonable in most cases. This could be the reason behind McQueen [37] explicitly stating that this metric can be interpreted as a measure of relative risk.

4.4 Security Metric for IED's

Due to the difference in functionality of an IED from a standard computer, it may be necessary to come up with an entirely new metric scheme for IED's. The main difference between a computer and an IED is that IED's are usually dedicated devices which measure, monitor and react.

4.4.1 Basic Properties

When looking at an IED from an attackers perspective, different categories of IED's will have different levels of importance depending on the goal of the attacker. For example, an attacker hoping to sabotage the grid may focus on tripping a relay while someone seeking confidential information may target a data logging unit. Also, depending on their importance different units will have different levels of security. Therefore, a security metric for IED's should have the following properties:

- The ability to quantify the threat to the IED based upon the goal of the attacker.
- It should quantify the vulnerability of an IED based upon its security features.
- It should be capable of contrasting between a secure and insecure network similar to the VEA-bility metric.

4.4.2 Threat Identification

The first step is to identify the threats to different categories of IED's. This is done by taking categories of IED's according to their designated function category and identifying the possible attack scenarios both physical and logical. When taken into broad categories, the possible scenarios include:

1. Unauthorized Access (UA) - the IED is accessed in order to give a false command, change the settings or access sensitive data
2. Denial of Service (DoS) - knocking out the IED from the network by disabling it or overwhelming it
3. Spoof (SP) - the IED is spoofed either physically or logically to mislead other devices
4. Data Interception (DI) - sensitive data is intercepted and manipulated
5. Stepping Stone (SS) - the IED can be logically used as a stepping stone to launch an attack on another target

4.4.3 Countermeasure Identification

Once the threats to an IED have been identified, it is now possible to check if the device has the appropriate security countermeasures. If a particular threat has the appropriate countermeasure it can be nulled (i.e. eliminated) from the threat list.

4.4.4 Susceptibility

Each threat can also be adjusted according to its relative susceptibility. For example, in order to spoof a particular IED it may be required to physically manipulate the device, hence such an attack can be considered unlikely. On the other hand, the same device may be susceptible to remote false commands or false inputs which are far more likely. This parameter defines likeliness of the attack based upon the location of the attacker.

4.4.5 Metric Formula and Calculation

From this, it is possible to come up with a formula to quantify the security of an IED and the IEC61850 network. The procedure for calculation involves:

1. Identification of the threats to each individual IED (m threats).
2. Identification of the available countermeasures for each threat. If a particular threat has one or more countermeasures, its countermeasure factor (c_i) is made one. The value of c_i is made zero if no countermeasures exist.
3. Identification of the susceptibility (s_i) of each threat where:
   (a) If the attack can be executed on the IED remotely from a WAN connected to the IEC61850 network, $s_i = 1$
   (b) If it has to be executed from within the IEC61850 (LAN) network, $s_i = 0.2$
   (c) If physical manipulation is needed for launching the attack, $s_i = 0.1$

   The values are selected such that the relative risk between a node, LAN or WAN based attack are contrasted
4. Based on this a score can be calculated for each threat
5. From this, the score for each IED can be calculated
6. Finally, the score for the entire network can be obtained

The formula for calculating the score for a particular threat (t_i) is based upon its susceptibility (s_i) and countermeasure factor (c_i).

$$t_i = s_i(1 - c_i) \tag{4.22}$$

The score for a particular IED j with m_j threats would hence be:

$$E_j = \sum_{i=1}^{m_j} t_i \tag{4.23}$$

Finally the overall score of the network with n IED's can be calculated from:

$$R = 10 - min(10, \sum_{j=1}^{n} E_j) \tag{4.24}$$

Using this formula, the score for a highly secure network would tend towards 10 while an insecure network with too many vulnerabilities would tend towards 0.

4.4.6 Generic Countermeasures

The countermeasures for threats can be categorized as *generic countermeasures* which are generally common to all IED's, servers and network infrastructure. In addition, each node of the network will have unique *specific countermeasures*. Depending on the location of the attacker the available countermeasures would differ. The possible attacker locations are the same for the case of susceptibility. Table 4.8 gives the generic countermeasures for a network.

Attack	Attacker Location		
	Node	LAN	WAN
UA	Access Control Physical Protection	MAC Address Control	Firewall IDS
DoS	Access Control Physical Protection	MAC Address Control	Firewall IDS Anti-Malware
SP	Physical Protection	MAC Address Control	Firewall IDS Anti-Malware
DI	Access Control Physical Protection	Switches MAC Address Control Anti-ARP IDS	Firewall IDS
SS	Access Control Physical Protection Software Patches Host-based IDS	MAC Address Control Software Patches	Firewall IDS Software Patches

Table 4.8: Generic Countermeasures

4.4.7 Countermeasure Overheads

Security countermeasures for IEC61850 networks and IED's will inevitably result in additional overheads. The effect would depend on the nature of the device and countermeasure. These can be summarized as:

- Possible increase in traffic and traffic delay at a network level due to the additional analysis carried out by countermeasures such as network based IDS, firewalls and anti-malware.
- Increased burden on the CPU of resource constrained IED's due to host based security mechanisms such as host based IDS and encryption. The overhead due to an anomaly detection IDS would be greater than a rule based IDS in terms of both computational power and cycles. In the case of encryption additional hardware and computational cycles will be needed. There will also be a need for additional mechanisms for key management if public key encryption is used.
- Reduced user friendliness due to increased use of access control.

Chapter 5 Security Auditing

5.1 Introduction

Security auditing is the process of assessing the security of a computer system and making recommendations to the client. This chapter develops an auditing procedure for the IEC61850 protocol.

5.2 Auditing Procedure Design

5.2.1 Existing Auditing Procedures

Numerous procedures exist for information security auditing. There is no industry standard auditing procedure. This is in one way advantageous because having a standard auditing procedure can also result in an opponent formulating a procedure to compromise a system which can be undetected by such a standard auditing procedure. Davis *et al.* [42] outline the stages of an audit as:

1. Planning - planning the audit by conducting a preliminary survey, reviewing critical assets of the organization and customer requests.
2. Fieldwork and documentation - acquiring the necessary data on the infrastructure and on security practice.
3. Issue discovery and validation - reviewing the data to discover the security issues of the organization and validating such issues.
4. Solution development
5. Report drafting and issuance
6. Issue tracking - tracking the issues to see if the recommended solutions are implemented and effective.

5.2.2 Priority Based Auditing

When assessing the information security of a large organization, it may be necessary to prioritize certain parts. According to Johansson and Johnson [43], improper prioritization can lead to problems such as:

1. Different parties defining the same area differently such as inclusion of physical security within the scope of information security by some and its exclusion by others.

2. Conflicts due to different opinions of different parties. Some may emphasize more on preventing social engineering while others may emphasize better technical countermeasures such as intrusion detection.

3. Conflicts due to the context of the organization. This is because some organizations such as financial institutions may become targets due to theft while others such as utilities may become targets due to sabotage. There may be other organizations which draw attackers due to factors such as prestige based upon the mere challenge of intrusion.

In addition, prioritization can lead to the overlooking of certain critical vulnerabilities in low priority areas. For example, an organization would deploy extensive intrusion detection and access control mechanisms but neglect the possibility of all of it being bypassed through social engineering.

5.3 Proposed Auditing Scheme for IEC61850

The proposed audit scheme for IEC61850 consists of the following stages:

1. Preliminary survey of the network and organization

2. Security assessment of the network and organization

3. Disclosing the results and recommendations to the client

4. Verification of implementation of recommendations

Out of these stages, the main focus of this research is on the security assessment. The main components of this stage along with their objectives and results are given in Table 5.1.

Component	Objective	Result
Security Tool Assessment	Uncover vulnerabilities of the network that may be visible to an attacker	VEA-bility Score
IED Assessment	Uncover the vulnerabilities of each IED	IED Score
Infrastructure Audit	Uncover both physical and logical vulnerabilities of the network infrastructure	Report
Comprehensive Assessment	A comprehensive assessment of the software used in the network which should include, 1. The operating systems of IED's, servers, gateways and engineering stations. 2. The software used to control and change settings of IED's, especially the communication protocols used.	Report

Table 5.1: Components of the Security Assessment Scheme

5.4 Security Tool Traffic

Since the delivery time for certain packets of IEC61850 is critical, it is necessary to assess the impact of the traffic generated by the security tool used on the network. This requires data collection, simulation and testing of available network security tools and weigh them against their benefits.

5.4.1 Data Collection

Data is collected using *Ethereal*, an open source network analyzer running on both Windows and Linux (as *Tcpdump*) platforms. While *Ethereal* is running, the security tool under test is used to scan a target machine. The resulting traffic is then captured and used for analysis. A total of 10 target machines are tested of which 5 have Windows based operating systems and the rest have Linux based operating systems. The network tools tested were *Nessus 3.2.1* [41] and *NMap 4.68* [44]. Both tools are tested while running on Windows and Linux platforms.

NMap 4.68 is a tool capable of identifying the operating system and listing a limited number of vulnerabilities. *Nessus 3.2.1* is the most advanced tool capable of giving a comprehensive list of vulnerabilities which can be used to calculate the

VEA-bility metric. The main disadvantages of *Nessus 3.2.1* are that unlike NMap which is open source, the security tests performed to uncover security vulnerabilities by the tool are not listed and its comprehensive assessment generates a large amount of traffic. Nessus was originally an open source tool. However, due to the possibility of attackers misusing the code, it is no longer open source. Hence, hence it is not possible to determine the tests performed by this tool.

5.4.2 Data Analysis

The collected data is then analyzed using MATLAB. The instantaneous traffic rate in packets per second for each scan is first calculated. Based on this, the time during which the generated traffic is high is obtained. If the instantaneous traffic rate is greater than 100 packets/s, it is considered high. From this the average time during which the security tool generates high traffic can be obtained.

Tool (Platform)	Mean Traffic Rates (packets/s)			Mean Scan Time (s)	
	Mean	Maximum	High (%)	Total	High
Nessus 3.2.1 (Windows)	377.0	11360.0	5.67	861.2	48.9
Nessus 3.2.1 (Linux)	145.4	3079.2	13.74	225.8	31.0
NMap 4.68 (Windows)	58.6	1073.2	11.96	90.0	10.8
NMap 4.68 (Linux)	172.2	919.2	29.18	42.4	12.4

Table 5.2: Security Tool Traffic Statistics - Windows

Tool (Platform)	Mean Traffic Rates (packets/s)			Mean Scan Time (s)	
	Mean	Maximum	High (%)	Total	High
Nessus 3.2.1 (Windows)	208.2	2750.2	17.13	188.2	32.2
Nessus 3.2.1 (Linux)	677.7	8760.4	39.45	75.2	29.7
NMap 4.68 (Windows)	125.7	2634.0	7.75	32.0	2.4
NMap 4.68 (Linux)	157.8	1957.2	9.58	33.2	3.2

Table 5.3: Security Tool Traffic Statistics - Linux

Figures 5.1 and 5.2 show profiles of typical traffic generated by the security tools. The graphs clearly show that at times the tools generate a large amount of traffic. According to the results of Tables 5.2 and 5.3, *Nessus* which does a more comprehensive set of tests takes longer to assess a Windows machine than a Linux machine. The same can be said of Nmap. When comparing the platform on which

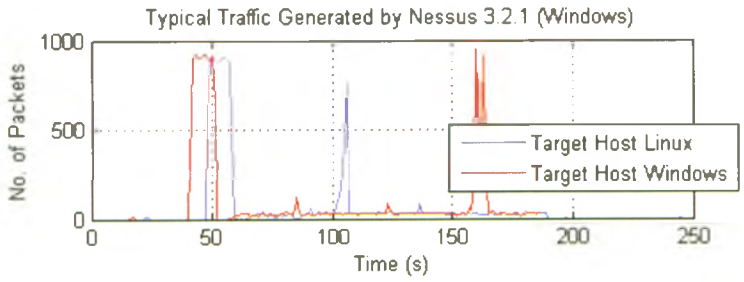


Figure 5.1: Typical Traffic Generated by Nessus 3.2.1 (Windows)

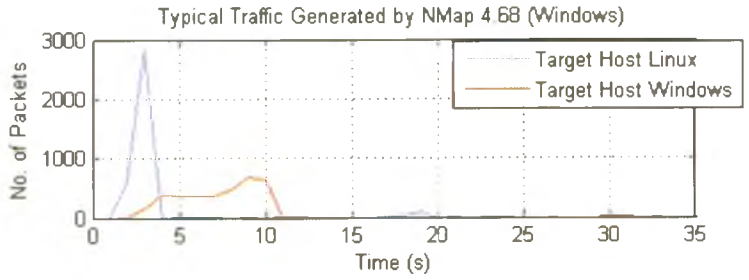


Figure 5.2: Typical Traffic Generated by NMap 4.68 (Windows)

the security tool is run, in general running the tool on a Linux platform results in a significantly less scanning time than on Windows.

The important factor to be considered is the amount of time during which the tool generates high traffic. Table 5.4 shows the summary of high loading for different tools and target machines. These results are approximated to the nearest multiple of 5 for convenience. Further study is needed to investigate if this loading will seriously compromise the safety of the IEC61850 network.

Tool	Loading Time (s)	
	Windows	Linux
Nessus 3.2.1 (Windows)	50	30
Nessus 3.2.1 (Linux)	30	30
NMap 4.68 (Windows)	15	5
NMap 4.68 (Linux)	15	5

Table 5.4: Security Tool High Traffic Loading Time (Approximate)

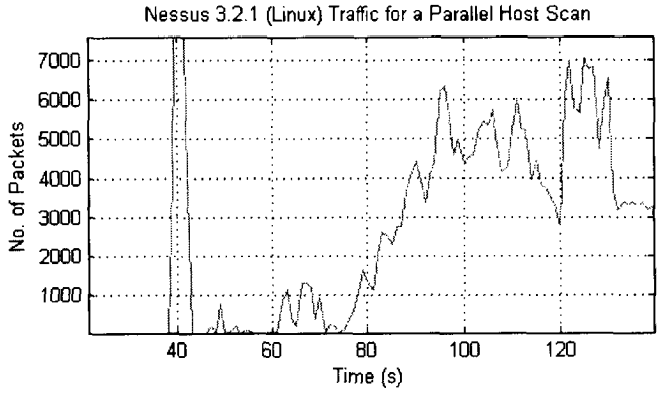


Figure 5.3: Traffic Generated by Nessus 3.2.1 (Linux) for a Parallel Host Scan

5.4.3 Parallel Scans

Nessus 3.2.1 allows multiple hosts to be scanned in parallel. The next step was to investigate the loading effect of the tool when multiple hosts are scanned in parallel. Figure 5.3 shows the traffic generated when 5 hosts are scanned in parallel. The scan time is approximately 140s but the average traffic is around 3000 packets/s, which is nearly 5 times greater than the maximum value for the mean traffic rate for a single host in Tables 5.2 and 5.3. For nearly 80% of the scan time (110s) the traffic is significantly greater than 100 packets/s.

5.4.4 Simulation

Simulation of the effect of the security tool is done using the open source simulator *Network Simulator 2.33* (*NS 2.33* commonly known as *NS-2*) [45]. *NS-2* is written in C++ and provides its interface in OTcl (Object Oriented Tool Command Language). Using the simulation, the delay of packets are analyzed and compared to the standards of IEC61850-5 (Table 5.5).

5.4.4.1 IED Model

NS-2 logically abstracts a network node (Figure 5.4) into a *node* which contains the data link and physical layers of the OSI model. The network and transport layers are handled by an entity known as an *agent* while the application layer is handled by an *application*. *Connection* elements are used to connect nodes together.

Type	Category	Maximum Delay (ms)
1A	Fast Messages - Trip	10 (Performance Class P1) 3 (Performance Class P2/3)
1B	Fast Messages - Other	100 (Performance Class P1) 20 (Performance Class P2/3)
2	Medium Speed	100
3	Low Speed	500
5	File Transfer	1000
7	Commands with Access Control	500

Table 5.5: Message Delay Standards According to IEC61850-5

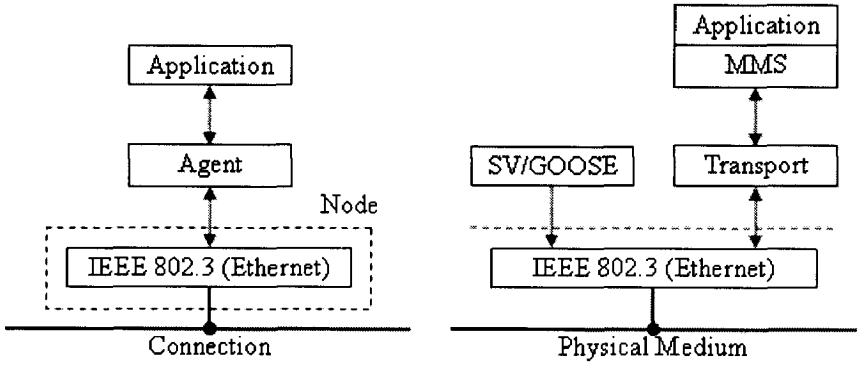


Figure 5.4: NS-2 Logical Model

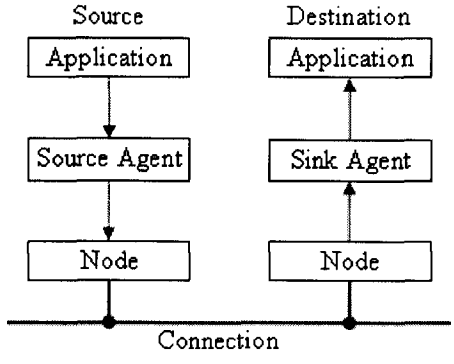


Figure 5.5: NS-2 Communication Model

In order for two nodes to communicate (Figure 5.5), the sending node should have the relevant source agent to transmit the data according to the required protocol and application. The receiving node must have a sink agent to receives the transmitted data, process it and record it for subsequent processing. For bidirectional communication both nodes must have source and sink agents. The sink agent can have an application attached to it, used for data collection or both.

When modeling an IED using *NS-2*, it is possible to model a packet that bypasses the TCP/IP stack as a UDP agent with constant bit rate (CBR) traffic. Other packets which use the TCP/IP protocol stack can be modeled using different TCP agents.

5.4.4.2 Substation Network

For simulation the IED's corresponding to a transformer bay and feeder bay have to be constructed. A feeder bay would consist of a Merging Unit (MU) taking raw data samples, two Protection and Control Relays (PC) to monitor the raw data and a Circuit Breaker (CB) to act according to the fault. The transformer bay would consist of a MU, two PC's and two CB's.

All of the IED's of a particular bay will be connected to a single switch. Figure 5.6 shows the physical and logical connection of a bay network. Each bay switch will in turn be connected to the central station switch. The server collecting data from the substation and the HMI would also be connected to this switch. The entire topology of the station network is shown in Figure 5.7.

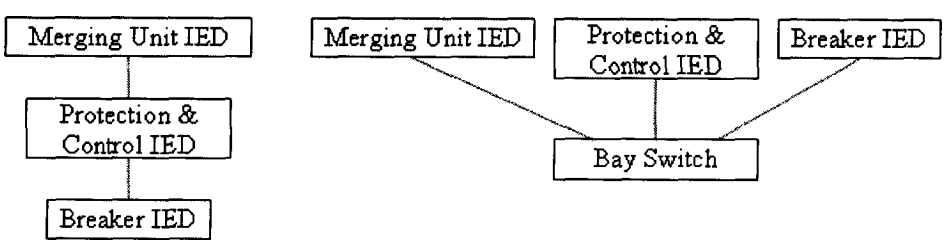


Figure 5.6: Physical and Logical Connection of a Bay Network

For the simulation, a substation consisting of two transformer bays and two to six transformer bays are used. Each MU is assumed to take 1920 raw data samples

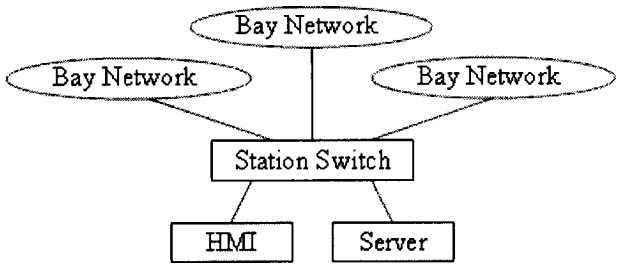


Figure 5.7: Topology of Entire Substation Network

per second to achieve class P3 protection [4] needed for a transmission bay with top performance synchronizing feature and breaker differential. A fault is simulated every 0.5s. During such a fault, the PC IED's send GOOSE packets to the CB while the CB returns a reply to confirm reception. Four packets are exchanged either way. In addition, each PC IED uploads a 2kb status report to the server every 2s.

5.4.4.3 Security Tool Model

The next stage of the simulation involves developing a model for the security tool. It is assumed that during a security audit, it will be connected to the station switch via a laptop.

The security tool is modeled as a burst of high traffic, lasting the duration of the load time (Table 5.4). Due to constraints of simulation time and in order to generalize the situation, the burst duration is restricted to 30s during which a traffic of 1000 packets per second are generated. A UDP agent with Pareto traffic is used to produce the traffic of the security tool.

5.4.4.4 Results

Tables 5.6 and 5.7 show the results of the simulation for 10Mbps and 100Mbps Ethernet respectively in terms of packet delay and drop rate. The simulation is done for the following scenarios:

1. Nothing (only sample values)
2. System with FTP transfers
3. System with security tool running

4. Both FTP transfers and security tool running
5. System with fault
6. Fault with FTP transfers
7. Fault with security tool running
8. Fault with both FTP transfers and security tool running

Out of these scenarios 3, 4, 7 and 8 have high traffic due to the running of the security tool.

Scenario	2 Feeder Bays		4 Feeder Bays		6 Feeder Bays	
	Delay (ms)	Drop (%)	Delay (ms)	Drop (%)	Delay (ms)	Drop (%)
1	9.81	3.79	10.10	3.97	9.49	3.78
2	11.15	4.75	10.33	4.08	10.45	4.60
3	5.76	34.46	7.04	26.55	9.04	36.07
4	7.35	41.43	8.10	23.97	8.20	25.05
5	12.24	10.80	9.73	6.50	10.52	6.05
6	10.57	8.58	11.54	6.85	9.94	6.60
7	7.45	43.05	7.78	28.23	8.70	25.72
8	7.73	32.36	8.68	15.11	9.39	33.64

Table 5.6: Simulation Results - 10Mbps Ethernet

Scenario	2 Feeder Bays		4 Feeder Bays		6 Feeder Bays	
	Delay (ms)	Drop (%)	Delay (ms)	Drop (%)	Delay (ms)	Drop (%)
1	1.17	1.35	1.21	1.52	1.17	1.40
2	1.15	1.72	1.20	1.61	1.15	1.70
3	1.23	14.02	1.21	7.57	1.15	6.76
4	1.23	10.53	1.25	9.41	1.19	8.06
5	1.19	1.94	1.16	1.50	1.17	1.50
6	1.16	1.91	1.25	1.82	1.16	1.95
7	1.20	10.45	1.24	8.44	1.21	5.77
8	1.22	7.85	1.21	11.51	1.19	6.60

Table 5.7: Simulation Results - 100Mbps Ethernet

The results of the simulation (Tables 5.6 and 5.7) show that there is no correlation between the packet delay and scenario traffic. However all scenarios with heavy

traffic have significantly high packet drop rates. The delay of dropped packets cannot be defined. Therefore, this could explain the reason behind not having a correlation between packet delay and scenario traffic.

Nevertheless, the high drop rates indicate that the security tool will have a significant effect on the safety of the network. This is because the dropping of a critical packet such as a GOOSE packet is unacceptable. The drop rate results are consistent for the number of feeder bays as well as both 10Mbps and 100Mbps simulations. The delay for 10Mbps networks is however, clearly above the recommended safe limits for IEC61850.

Chapter 6 Sample Audit

6.1 Introduction

This chapter documents sample audits using the proposed auditing scheme conducted on sample networks. This is done to test the feasibility of the scheme and compare it against the MTTC and VEA-bility metric schemes.

6.2 Kinectrics IEC61850 Network

The IEC61850 network owned by Kinectrics, Inc. is a model network used mainly for testing, certification, research and teaching purposes. Currently it is an island network (not connected to the Internet) which consists of 7 models of IED's, an SMP gateway and an engineering station running with a remote data logger (Figure 6.1). Table 6.1 lists the models IED's and other devices of it. The nodes of the network use non-routable IP addresses.

Model and manufacturer details of all IED's are withheld for confidentiality reasons. The groups IED1-IED4 (GROUP2), IED5-IED6 (GROUP1) and IED7 (GROUP3) come from three different manufacturers and tend to have common characteristics. The network switches come in two models, SWITCH1 and SWITCH2 from the same manufacturer.

6.3 Security Tool Assessment

6.3.1 Security Tool Scan Results

The security tools reveal the open ports and services of each IED during the scan. When looking at the results (Table 6.2) it becomes apparent that *Nessus 3.2.1* has a better capability of identifying open ports and services such as Modbus, NTP and TFTP. *NMap 4.68* on the other hand can identify most key ports and services but fails to identify the critical protocol Modbus as well as UDP based services.

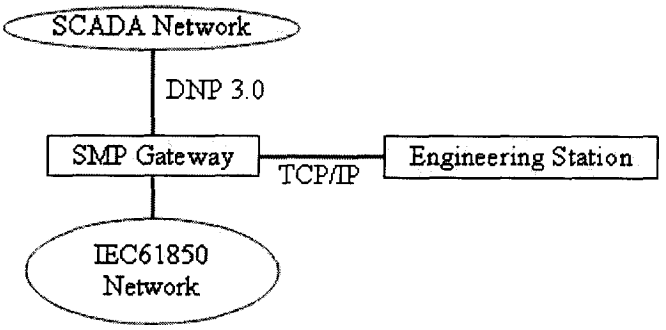


Figure 6.1: Kinectrics IEC61850 Network

Device	Qty	Description
IED1	1	Controller system
IED2	2	Breaker protection system
IED3	6	Feeder protection relay
IED4	2	Transformer protection relay
IED5	1	Protection and control system
IED6	3	Protection and control system
IED7	2	Differential protection relay
Firewall	1	Gateway to DNP3 and TCP/IP WAN
Database	1	Database server
Switch	6	Ethernet LAN network switches

Table 6.1: Kinectrics IEC61850 Network Devices

Despite identifying more vulnerabilities, *Nessus* takes a long time to scan a single device when compared to *NMap*. It was also observed that *Nessus* would take an excessive amount of time when scanning TCP ports 102 and 502. However, when compared to a computer (Tables 5.2 and 5.3), the time during which the security tool loads the network with more than 100 packets is much less for either security tool. On average, for *Nessus* (Table 6.3) it is just around 0.5s and for *NMap* (Table 6.4) it is around 0.15s.

6.3.2 MTTC Calculation

Table 6.5 shows the MTTC for the hosts of the network based upon individual vulnerabilities. The MTTC for the entire network is 1.8806 days according to Equation

Device	Nessus 3.2.1	NMap 4.68
IED1-4	69 (TFTP - UDP) 80 (HTTP) 102 (iso-tsap) 502 (Modbus)	80 (HTTP)
IED5-6	21 (FTP) 23 (Telnet) 102 (iso-tsap) 1024 (kdm)	21 (FTP) 23 (Telnet) 1024 (kdm)
IED7	21 (FTP) 80 (HTTP) 102 (iso-tsap) 161 (SNMP/UDP)	21 (FTP) 80 (HTTP)
Firewall	123 (NTP - UDP) 443 (HTTPS) 20000 (DNP)	123 (NTP - UDP) 443 (HTTPS) 20000 (DNP)
Database	123 (NTP - UDP) 135 (epmap) 137 (netbios-ns - UDP) 139 (netbios-ssn) 445 (microsoft-ds) 1106 (isoipsigport-1) 2701 (sms-xfer) 2702 (sms-rcinfo) 3389 (ms-wbt-server)	135 (msrpc) 139 (netbios-ssn) 445 (microsoft-ds) 1106 1723 (pptp) 2701 (landesk-rc) 2702 3389 (ms-term-serv)
Switch	22 (SSH) 23 (Telnet) 69 (TFTP - UDP) 80 (HTTP) 123 (NTP - UDP) 443 (HTTPS) 502 (Modbus) 514 (RSH)	22 (SSH) 23 (Telnet) 80 (HTTP) 443 (HTTPS) 514

Table 6.2: Security Tool Scan Results - Open Ports

4.21 which yields a total of 35.6 vulnerabilities. However, none of the vulnerabilities can be mitigated unless the services such as Telnet are completely disabled. This is not feasible. Hence, the MTTC of the network will not change.

Tool	Traffic Rates (packets/s)			Scan Time (s)	
	Mean	Maximum	High (%)	Total	High
IED1	50.498	641	0.090	949.442	0.850
IED2	51.411	851	0.080	924.721	0.738
IED3	66.259	641	0.107	237.768	0.255
IED4	57.279	641	0.100	297.428	0.296
IED5	69.077	644	0.119	182.083	0.216
IED6	51.251	641	0.117	250.019	0.292
IED7	64.995	642	0.107	214.307	0.229
Firewall	23.616	324	0.277	734.436	2.031
Database	76.687	642	0.131	178.546	0.234
Switch1	132.311	648	0.143	237.046	0.339
Switch2	135.608	648	0.143	230.916	0.330
Average	70.818	633.0	0.128	403.338	0.528

Table 6.3: Security Tool Traffic Statistics - Nessus 3.2.1

Tool	Traffic Rates (packets/s)			Scan Time (s)	
	Mean	Maximum	High (%)	Total	High
IED1	9.415	2003	0.039	269.418	0.106
IED2	11.876	2003	0.040	209.203	0.084
IED3	11.820	2003	0.040	209.519	0.084
IED4	11.825	2003	0.040	209.652	0.084
IED5	30.645	1368	0.129	75.024	0.097
IED6	30.494	1687	0.085	76.324	0.065
IED7	29.181	1622	0.083	82.020	0.068
Firewall	178.500	685	0.187	11.219	0.021
Database	24.431	1935	0.067	121.216	0.081
Switch1	9.408	1130	0.133	318.001	0.424
Switch2	9.219	987	0.102	317.560	0.324
Average	32.437	1584.2	0.086	172.651	0.131

Table 6.4: Security Tool Traffic Statistics - NMap 4.68

6.3.3 VEA-bility Calculation

The VEA-bility score of the network is obtained from the vulnerabilities of the network with CVE's. Table 6.6 gives the CVE's of devices in the network uncovered by *Nessus*. The individual scores of attackability, exploitability and vulnerability are then obtained for each device. Since the device has a firewall, the attackability score

Host	Open Ports	Vulnerabilities			MTTC (days)
		Low	Medium	High	
IED1	4	9	0	0	5.598569
IED2	4	9	0	0	5.598569
IED3	4	5	0	0	5.687029
IED4	4	5	0	0	5.687029
IED5	4	5	1	0	5.576716
IED6	4	5	1	0	5.576716
IED7	4	6	2	1	5.240864
Switch1	8	13	3	0	5.200654
Switch2	8	12	3	0	5.220711
Firewall	3	9	0	0	5.598569
Database	9	16	1	0	5.343082
Network MTTC					1.8806

Table 6.5: Sample Network Host Vulnerabilities

Device	CVE	Score		
		Base	Impact	Exploit
Switch	CVE-1999-0651	7.5	6.4	10
	CVE-2003-0001	5	2.9	10
Database Server	CVE-2005-1794	6.4	4.9	10

Table 6.6: Sample Network Host Vulnerability CVSS Scores

Device	Qty	Open Ports	Attackability	Exploitability	Vulnerability
Database	1	9	0.000	1.607	5.650
Switch1	5	8	0.000	1.429	10.000
Switch2	1	8	0.000	1.429	10.000
Network VEA-bility					3.3333

Table 6.7: Sample Network VEA-bility Score

is zero for all devices [39]. The individual score is then multiplied by the number of devices to get the VEA-bility score of the entire network (Table 6.7). The final score of 3.333 indicates a highly insecure network.

6.4 IED Assessment

6.4.1 IED Assessment - GROUP1 Devices

The devices of GROUP1 are used for line protection and control. The settings of either device can be set via the front panel, via RS232 or TCP/IP. The software provided by the manufacturer can be used as a GUI based HMI for it.

6.4.1.1 Relay Password Crack

Both devices have six access levels. Each access level requires a separate password. No minimum length for a password is specified, however the maximum length is 6 characters. Valid characters include numbers, upper case letters, lower case letters and two special characters. These are the hyphen (-) and the period (.). This gives a total of 64 characters (26+26+10+2), hence a total of $6.8719x10^{10}$ (64^6) combinations.

If a brute force password cracker were to attempt to crack one password, it would need nearly 8 days if it made 100000 attempts per second. Therefore, if properly monitored, a brute force attack is highly unlikely to go undetected. However, if a dictionary attack were to be launched, its chance of success would be higher if the employees fail to use strong passwords. A highly dangerous situation occurs if the factory default password is not changed and an attacker happens to find it out by consulting the manual of the device.

6.4.1.2 Packet Sniffing

This device uses both FTP and Telnet protocols. Both of these protocols have serious security vulnerabilities. In both protocols passwords and data are unencrypted, hence vulnerable to an eavesdropping attack. In this attack scenario, the attacker would be able to obtain the passwords for the FTP or Telnet protocol and launch an attack using this.

With the use of switches that match different Ethernet speeds and reduced use of network hubs, the risk of a direct packet sniffing attack is reduced. This is because multi speed switches do not simply send the packet to all ports unless it is a broadcast packet. This makes an eavesdropping attack difficult but not impossible. According to Spangler [46], the three possible methods of attack are:

1. ARP cache poisoning

2. CAM table flooding

3. Switch port stealing

Nevertheless, it should be remembered that in order to launch a packet sniffing attack, the attacker would have to either compromise a machine within the IEC61850 network or have physical access to the network infrastructure.

6.4.1.3 Protocol Password Crack

The FTP and Telnet protocols used by the relay can also be subjected to a password crack attack. Similar to the relay passwords, a brute force attempt may take too long and a dictionary attack may be more likely.

When Telnet is used, access to a GROUP1 device is trivial and the passwords for level 1 and level 2 access are prompted. Since Telnet transmits character by character, an automated brute force attack would be a non-trivial job for an attacker. Transmitting a single character at a time would also generate an abnormal amount of Telnet packets with a single character payload which can be detected by an IDS.

In the case of the FTP server, a brute force attack can be launched from a password cracker. For such an attack, the only thing the attacker needs to know is the user names for the FTP server. This can be found by referring to the manual of the IED.

6.4.1.4 Denial of Service Attacks

There are two possible scenarios of an attacker launching a DoS attack on GROUP1 devices. The first scenario is an attacker explicitly targeting one of the services of the device either FTP (port 21) or Telnet (port 23) by opening idle connections. In the second scenario, the attacker launches a generic DoS by overwhelming the device and network by generating unwanted traffic.

6.4.1.5 Countermeasures

Table 6.8 shows the countermeasures for the possible attacks on the GROUP1 device. When calculating the metric for this device, it is necessary to find out if at least one of the required countermeasures is implemented within the network.

Attack	Location	Countermeasures
Relay Password Crack	Node	Physical protection
Direct Packet Sniffing	LAN	Hub replacement Physical protection
ARP Packet Sniffing	LAN	MAC address restriction Static ARP tables ARP traffic analysis via IDS Physical protection
DoS (ICMP, FTP, Telnet) Protocol Password Crack	LAN	MAC address restriction Physical protection
DoS (ICMP, FTP, Telnet) Protocol Password Crack	WAN	Blocking via Firewall Detection and reaction via IDS

Table 6.8: Countermeasures for GROUP1 Devices

6.4.2 IED Assessment - GROUP2 Devices

The devices of this group are mainly protection relays. They can be accessed via the front panel, RS232 or TCP/IP. The manufacturer provides a software suite to manipulate the settings via a GUI based HMI.

6.4.2.1 Packet Sniffing

The software communicates with the relay via HTTP and Modbus protocols. The Modbus protocol is widely used in SCADA systems via TCP or RS232 and has no security mechanisms [47], [48]. Similarly, HTTP also has no security mechanisms and is used when information of the relay is viewed via a web browser. Thus, both of these protocols are vulnerable to a packet sniffing attack since all of the data they transfer are unencrypted. The attack scenarios are similar to those of Section 6.4.1.2.

6.4.2.2 Relay and Protocol Password Crack

Relays of this group use a 10 digit number as the password. Hence, a brute force password crack would require 10^{10} combinations. Such a crack would therefore take a significant amount of time, hence detectable. The main advantage of using only digits is that a dictionary attack is infeasible. Hence, it can be considered to be more secure than devices of GROUP1. In order to crack the password, the Modbus protocol has to be used.

Attack	Location	Countermeasures
Relay Password Crack	Node	Physical protection
Direct Packet Sniffing	LAN	Hub replacement Physical protection
ARP Packet Sniffing	LAN	MAC address restriction Static ARP tables ARP traffic analysis via IDS Physical protection
ICMP DoS	LAN	MAC address restriction Physical protection
Protocol Password Crack	LAN	MAC address restriction Physical protection
Unauthorized Access	LAN	Dual operator confirmation
ICMP DoS	WAN	Blocking via Firewall Detection and reaction via IDS
Protocol Password Crack	WAN	Blocking via Firewall Detection and reaction via IDS
Unauthorized Access	WAN	Dual operator confirmation

Table 6.9: Countermeasures for GROUP2 Devices

6.4.2.3 Denial of Service Attacks

Both Modbus and HTTP are protocols designed for handling multiple clients or slaves. Hence, launching a DoS attack is non-trivial, especially for HTTP since it is a stateless protocol. However, a DoS attack by overwhelming the client via fake traffic is highly realistic.

6.4.2.4 Generic Unauthorized Access

In order to counter the possibility of unauthorized access, these devices have a security feature known where a command or change of setting requires confirmation from both the user and the SCADA operator.

6.4.2.5 Countermeasures

Table 6.9 gives the countermeasures for the possible threats for all GROUP2 devices.

Attack	Location	Countermeasures
Relay Password Crack	Node	Physical protection
Direct Packet Sniffing	LAN	Hub replacement Physical protection
ARP Packet Sniffing	LAN	MAC address restriction Static ARP tables ARP traffic analysis via IDS Physical protection
ICMP DoS	LAN	MAC address restriction Physical protection
Protocol Password Crack	LAN	MAC address restriction Physical protection
ICMP DoS	WAN	Blocking via Firewall Detection and reaction via IDS
Protocol Password Crack	WAN	Blocking via Firewall Detection and reaction via IDS

Table 6.10: Countermeasures for the GROUP3 Device

6.4.3 IED Assessment - GROUP3 Devices

The IED7 is a differential protection relay which can be accessed by its front panel, RS323 or TCP/IP using the software suite provided by the manufacturer. The possible attacks on this device include:

- The software uses the HTTP and FTP protocols for communication, both are insecure and unencrypted. Therefore, this device is vulnerable to the same packet sniffing attack scenario as the former two.
- Both HTTP and FTP protocols are vulnerable to protocol password crack attacks. During an attack on HTTP, the attacker will have to send repeated POST requests. Such an attack would therefore be detectable by using an IDS to analyze payload of HTTP packets for the POST request.
- It is also vulnerable to a ICMP DoS attack.

Table 6.10 lists the countermeasures for possible attacks on the device.

6.4.4 Firewall

The gateway/firewall runs Windows XP and connects the IEC61850 network to external TCP/IP or DNP3 networks. This device runs the anti-malware software hence protects the network from such threats. It has both secure HTTPS and NERC CIP compliant VPN support for security. This device can be the target of a stepping stone attack where an outside attacker can execute arbitrary code on the machine in order to compromise the security of the network. However, during the security tool scan of the device no such vulnerabilities were uncovered.

6.4.5 Database Server

The database server runs Microsoft SQL Server on Windows XP. It has no explicit secure protocols such as SSH or HTTPS because of the security implemented by the MS SQL server itself. These services should however be properly enabled for optimum security. Similar to the Firewall, this device can also be used as a stepping stone by executing arbitrary code on it. Again, such vulnerabilities were not revealed during the security tool scan.

6.4.6 Switches

The network switches have a high number of security features implemented within them. These security features are implemented via secure protocols running on operating system within the switch. The security features can be categorized for switch management and network security.

The protocols Telnet, RSH, SSH, HTTP and HTTPS are used for switch management. Out of these, SSH and HTTPS are highly secure provided that a trusted third party handles the keys. In order to guarantee proper security, the remaining insecure protocols (Telnet, HTTP and RSH) have to be disabled.

This device allows MAC address based filtering, including associating single or multiple addresses to a single port. Such a security feature is vital in countering a number of possible threats such as general unauthorized access and ARP based packet sniffing.

Threat	Category	s_i	c_i	t_i
Relay Password Crack	UA	0.1	1	0
Direct Packet Sniffing	DI	0.2	1	0
ARP Packet Sniffing	DI	0.2	1	0
ICMP DoS (LAN)	KO	0.2	1	0
FTP DoS (LAN)	KO	0.2	1	0
Telnet DoS (LAN)	KO	0.2	1	0
Protocol Password Crack (LAN)	UA	0.2	1	0
ICMP DoS (WAN)	KO	1	0	1
FTP DoS (WAN)	KO	1	0	1
Telnet DoS (WAN)	KO	1	0	1
Protocol Password Crack (WAN)	UA	1	0	1

Table 6.11: Metric Calculation for GROUP1 Devices

Threat	Category	s_i	c_i	t_i
Relay Password Crack	UA	0.1	1	0
Direct Packet Sniffing	DI	0.2	1	0
ARP Packet Sniffing	DI	0.2	1	0
ICMP DoS	KO	0.2	1	0
Protocol Password Crack (LAN)	UA	0.2	1	0
Unauthorized Access (LAN)	UA	0.2	1	0
ICMP DoS (WAN)	KO	1	0	1
Protocol Password Crack (WAN)	UA	1	0	1
Unauthorized Access (WAN)	UA	1	1	0

Table 6.12: Metric Calculation for GROUP2 Devices

Threat	Category	s_i	c_i	t_i
Relay Password Crack	UA	0.1	1	0
Direct Packet Sniffing	DI	0.2	1	0
ARP Packet Sniffing	DI	0.2	1	0
ICMP DoS (LAN)	KO	0.2	1	0
Protocol Password Crack (LAN)	UA	0.2	1	0
ICMP DoS (WAN)	KO	1	0	1
Protocol Password Crack (WAN)	UA	1	0	1

Table 6.13: Metric Calculation for the GROUP3 Device

Device	Qty	E_j (LAN)	E_j (WAN)
IED1	1	0	2
IED2	2	0	2
IED3	6	0	2
IED4	2	0	2
IED5	1	0	4
IED6	3	0	4
IED7	2	0	2
Firewall	1	0	0
Database	1	0	0
Switch	6	0	0
	$\sum E_j$	0	42
	R	10	0

Table 6.14: Network Metric Calculation

6.4.7 IED Metric Calculation

In order to calculate the IED metric for the entire network, the score for each threat is evaluated. Tables 6.11, 6.12 and 6.13 give the susceptibility (s_i), countermeasure factor (c_i) and threat score (t_i) for each threat. Since most threats have the appropriate countermeasures, their respective threat scores are zero.

The only threats which have nonzero scores are the DoS attacks which can be launched from a remote location across a WAN. This is because, despite having a firewall which can block unwanted hosts, there is the possibility of an attacker using a legitimate host allowed by the firewall to launch the attack. Only an IDS would be able to detect such an attack.

Based on this, the metric for the entire network can be obtained (Table 6.14). It is calculated assuming that the network is only limited to a single LAN or interconnected to a WAN.

6.5 Conclusions

Table 6.15 compares the score of the network in terms of the three metric schemes used. All three metric schemes are consistent in terms of indicating the weak security of the network when it is connected to a WAN.

Metric	Network Score	Secure Score
MTTC	1.8806 (days)	5.8 (days)
VEA-bility	3.333	10
IED Metric (LAN)	10	10
IED Metric (WAN)	0	10

Table 6.15: Network Metric Scores

Should the network be limited to a single LAN, then the existing security measures would be sufficient to protect it from all foreseeable threats that can be launched from within the LAN. However, if the network is connected to a WAN it is highly insecure. This is because an attacker can trivially launch ICMP or protocol DoS attacks at almost all IED's and protocol passwords of most IED's can be easily be subjected to password crack attack. These attacks can only be effectively countered via an IDS which is not present on the network.

Another notable fact is that the VEA-bility metric indicates that the network is insecure based on the CVE's of the database server and network switches. Despite using highly insecure protocols, there are no host CVE's for the IED's themselves. However, the IED metric, indicates the poor security of the network based on vulnerabilities of the IED's themselves.

6.6 Recommendations

The following general recommendations are made for future IED development:

1. Phasing out insecure protocols such as FTP, Telnet, RSH and HTTP and replacing them with secure SSH and HTTPS. These secure protocols have been implemented at the embedded level such as dropbear (SSH).

2. The use of IEEE 802.1ae MACsec to guarantee security at the MAC level as a countermeasure against eavesdropping for both wired and future wireless extensions of IEC61850.

3. The development of suitable rule based and anomaly detecting intrusion detection for IEC61850 networks especially since wider interconnection over both wired and wireless insecure networks is likely to come.

Chapter 7 Simulated Attacks

7.1 Introduction

This chapter details the experiments done to investigate the vulnerabilities of the IEC61850 IED's via simulated attacks. The experiments were conducted at the Power System Protection Laboratory of the University of Western Ontario. It was also used to test the feasibility of some proposed countermeasures.

7.2 Methodology

Figure 7.1 shows the experimental setup for launching simulated attacks. The IED under test is connected to a switch along with a Windows host and Linux host. The Windows host is mainly used for changing the settings of the IED via the network or RS232 since most IED software is developed for the Windows platform. The Linux host is used for packet sniffing and intrusion detection. The connection to the IED is mirrored to the Linux host to allow packets to be monitored. Together, these units form the IED network. Henceforth it shall be referred to as the Network Monitor.

The IED is then accessed using two remote hosts connected to the main UWO network. Both Linux and Windows are used so that the Windows host is used for accessing the IED using its software to explore its vulnerabilities. The Linux host is mainly used for launching attacks. Both of these machines will be referred to as the Remote Windows and Remote Linux host respectively.

The experiments done consist of the following stages:

1. Simulated DoS attacks on the IED. The DoS attacks launched are,
   (a) ICMP DoS attack (Ping attack)
   (b) Service DoS attack (attack on the Telnet, FTP or HTTP server)
2. Password crack attack

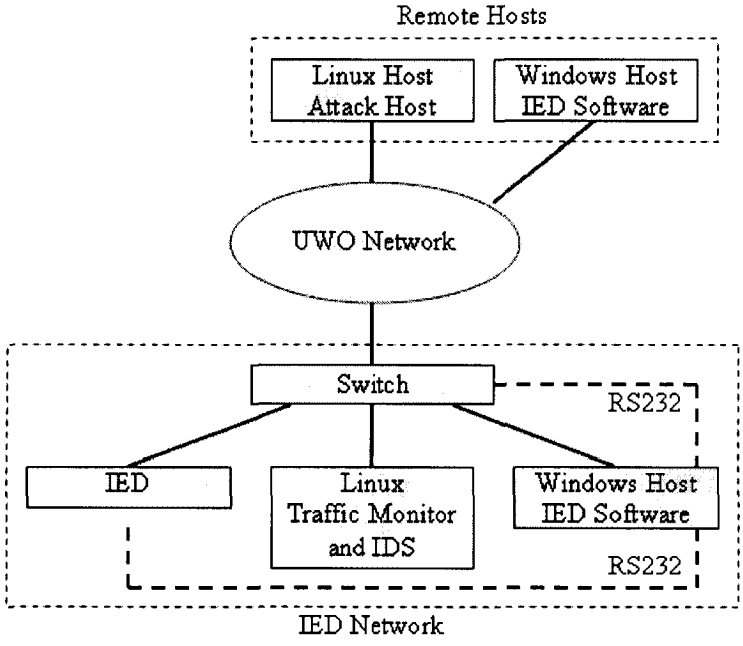


Figure 7.1: Experimental Setup for Simulated Attacks on IED's

7.3 Simulated Attack on an IED

7.3.1 DoS Attacks

The DoS attack is launched from the Remote Linux host. The basic method of testing is to run a DoS process and try to connect to the IED using its software from the Remote Windows host. The number of parallel connections is increased until the IED is overwhelmed. The Network Monitor is used to capture all traffic so that it can be analyzed and applied for intrusion detection.

7.3.1.1 Ping Attack

The ping attack is launched using the Linux ping command. While the remote host runs the Linux command, the Remote Windows host is used to connect to the device using the software. The interpacket delay (interval) and packet size are varied until the software can no longer connect to the relay. Table 7.1 shows the results of the experiment. The results indicate that a data rate of around 10Mbps is sufficient to achieve the goal of DoS with 5Mbps severely degrading performance.

Size (kB)	Interval (s)	Data Rate (Mbps)	Packet Loss	Comments
64	0.1	5.00	5%	Slow connection
64	0.01	50.00	99%	No connection
32	0.01	25.00	98%	No connection
24	0.01	18.75	97%	No connection
20	0.01	15.62	95%	No connection
18	0.01	14.06	94%	No connection
12	0.01	9.37	0%	Slow connection

Table 7.1: Ping Command Settings

7.3.1.2 Telnet Attack

The Telnet attack was trivially launched by using multiple shells to start parallel Telnet sessions. The IED was found out to be capable of handling only 3 parallel Telnet sessions.

7.3.1.3 FTP Attack

The same method for a Telnet DoS was used for FTP as well. The FTP server of the IED was found to be capable of handling only three parallel sessions. Hence, an attacker can trivially launch a DoS attack even when unauthenticated.

7.3.2 Password Crack Attack

The crack attempt is done using the open source tool *Hydra v5.4*. *Hydra* is an network security tool designed to check for weak passwords by attempting to login to a given protocol using a dictionary of passwords [49]. Unfortunately it can also be misused by an attacker to crack a password. Hydra is used with a standard dictionary of both uppercase and lowercase words.

7.3.2.1 FTP Crack

FTP transmits the entire password in a single packet. Hence, a high rate of login attempts can be maintained. Using a standard dictionary of both capital and simple letters, a weak password can be cracked within 10 minutes. Figure 7.2 is a typical report for such an attack. Details capable of identifying the IED have been withheld for security reasons.

```
[DATA] 1 tasks, 1 servers,
    126525 login tries (l:3/p:42175),
    ~126525 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 9360.00 tries/min,
    9360 tries in 00:01h,
    117165 todo in 00:13h
[STATUS] 9400.33 tries/min,
    28201 tries in 00:03h,
    98324 todo in 00:11h
[21][ftp] host: 172.18.227.36
    login: XXX   password: VVVVV
[STATUS] 9382.00 tries/min,
    65674 tries in 00:07h,
    60851 todo in 00:07h
[21][ftp] host: 172.18.227.36
    login: YYY   password: WWWW
```

Figure 7.2: Output of a Hydra v5.4 FTP Password Crack

Hydra requires the username of the device to be known. Since the limited resources of IED's usually only permit hardcoded usernames, an attacker with access to a manual can easily find the usernames and subsequently crack the passwords.

7.3.2.2 Telnet Crack Result

Hydra was incapable of cracking the Telnet protocol because unlike in FTP, the user is prompted for the password during the session. Analysis of the data of the traffic during the attempt reveals that Hydra cannot handle the messages during a password prompt. However, if the attacker succeeds in cracking the password for the usernames for FTP, it can be used straight away to gain access to the relay via Telnet.

7.4 Conclusions

The simulated attacks reveal that it is possible for a relatively less skilled attacker to compromise the information security of the test IED. In most cases, the attacks can be launched trivially using existing Linux commands with the appropriate modifications. The amount of code that needs to be written by the attacker is also relatively small

and simple, within the capability of a majority of potential attackers with modest programming skills. It is also possible to misuse open source security tools for this purpose such as OS fingerprinting and weak password detection.

The main reason for the high risk of compromise is the use of insecure protocols. In a way manufacturers are compelled to use such protocols to avoid heavy overheads [28]. Hence, it is necessary to implement better security mechanisms in future IED's to ensure that the IED will not be easily compromised. The possibility of using an IDS as an effective countermeasure for these attacks are discussed in Chapter 9.

Chapter 8 Temporal Risk Analysis

8.1 Introduction

This chapter looks into the temporal risk of IEC61850 automated substations. The risk and vulnerability of an IEC61850 network can also be analyzed on a temporal basis. This can be analyzed using statistical data obtained from known attacks and activity of IEC61850 networks. From this, the temporal risk of the network can be obtained.

8.2 Threat of Attack

8.2.1 Relationship with Human Alertness

Intuitively an attacker is most likely to attack a secure target during the ebb of human alertness. This is because during the ebb of human alertness, the defenders will be least alert to the impending attack. Anecdotal evidence such as pre-dawn military attacks can be found from history. However, there are no detailed analysis or statistics to back up such claims.

According to Van Dongen and Dinges [50], the human alertness is primarily governed by the circadian sleep rhythm. This in turn covaries with the circadian rhythm of core body temperature. Conroy *et al.* [51] developed a simplified model of the circadian rhythm of core body temperature using a cosine function (Figure 8.1).

8.2.2 Experimental Attack Statistics

Statistics of cyber attacks on actual systems are obtained from data collected by the Honeynet Project [22]. In a Honeynet, a network is deployed with monitoring and intrusion detection software with the intent of capturing attacker behavior. Nothing is done to explicitly attract attackers to the honeynet. Once an attacker intrudes

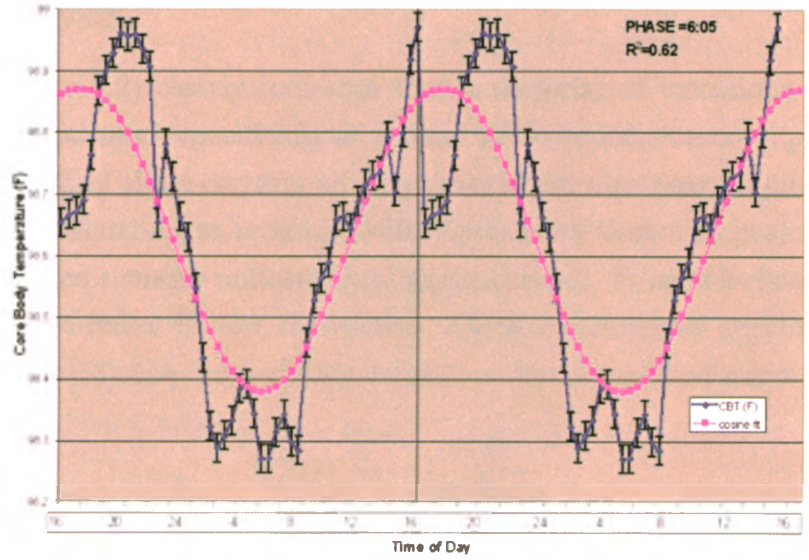


Figure 8.1: Mean Core Body Temperature Cosine Curve
Taken from Conroy *et al.* [51]

the network, all actions of the attacker are monitored and recorded. This allows the actions of real attackers to be studied.

The data was obtained from the reports generated by the open source intrusion detection program *Snort* [52]. When ever something suspicious takes place, the date and time of the activity is recorded. The duration of the collected data is from April 2000 to February 2001. Figure 8.2 shows the number of intrusion reports plot against the time during which the report was generated for the given period.

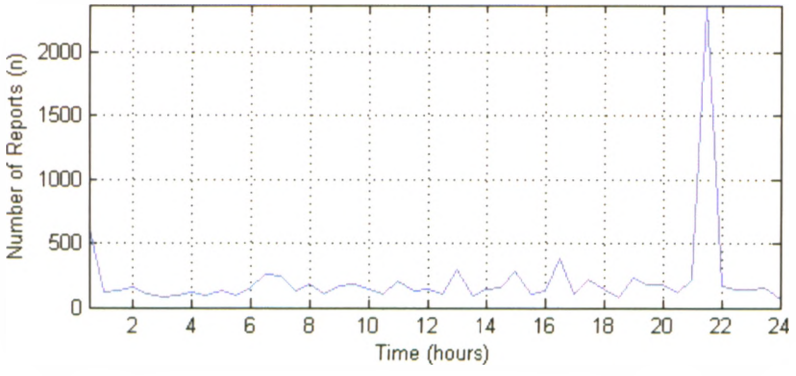


Figure 8.2: Number of Intrusion Reports vs. Time of Day

8.2.3 Analysis

The data (Figure 8.2) clearly indicates that a majority of intrusions (nearly 25%) take place at night more specifically at around 22:00 hours. A second peak occurs at 00:00 hours. Both of these correspond to a times of low alertness (Figure 8.1) but not the time of least alertness at around 06:00. Apart from these two peaks, the number of attacks reported remains uniform throughout the day. From this data it is possible to define a threat index (T) for the system. Using a conceptual approach similar to that of Hu *et al.* [53], the threat index is taken as the normalized curve of Figure 8.2.

$$T(t) = \frac{n(t)}{[n(t)]_{max}} \tag{8.1}$$

8.3 Power System Vulnerability

Power demand varies throughout the day due to changes in human activity. During a typical day, the power demand is high during midday with a noticeable peak during the night. After this it declines until it ebbs at around 04:00. Figure 8.3 shows the daily and average power demand curve for New South Wales, Australia during the month of March, 2008 [54].

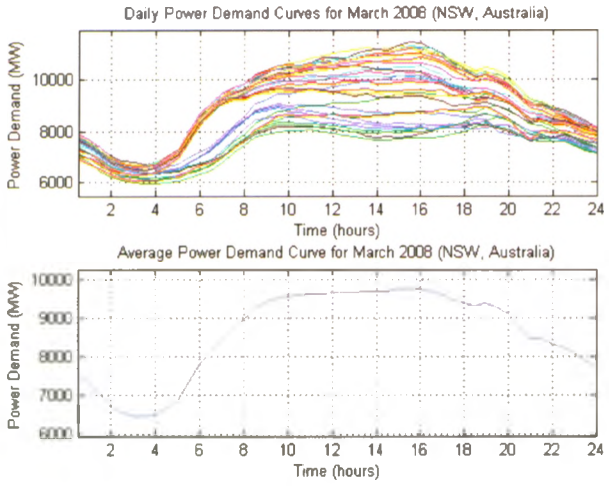


Figure 8.3: Daily and Average Power Demand Curve for New South Wales, Australia, March 2008
Taken from National Electricity Market, Australia Website [54]

A disruption in power would result in a loss to all consumers. Hence, the vulnerability of the power system can be considered proportional to the amount of power delivered. In order to inflict maximum damage to consumers, an attacker is most likely to target the system at a time of high power demand. Hence, the loss index (V) of the system can be taken as the normalized average power demand curve.

$$V(t) = \frac{P_{avg}(t)}{[P_{avg}(t)]_{max}} \tag{8.2}$$

8.4 Power System Temporal Risk Index

In order to obtain the temporal risk an approach similar to that proposed by Hu *et al.* [53] is used. The formula for the temporal risk index RI can be expressed as:

$$RI(t) = T(t)V(t) \tag{8.3}$$

Figure 8.4 shows the resulting risk index which is very much similar to that of the attack statistics (Figure 8.2). The implications of the temporal risk index include:

- The times during which more intensive security measures have to be activated.
- The times during which human monitors and cyber attack response teams should be most alert.

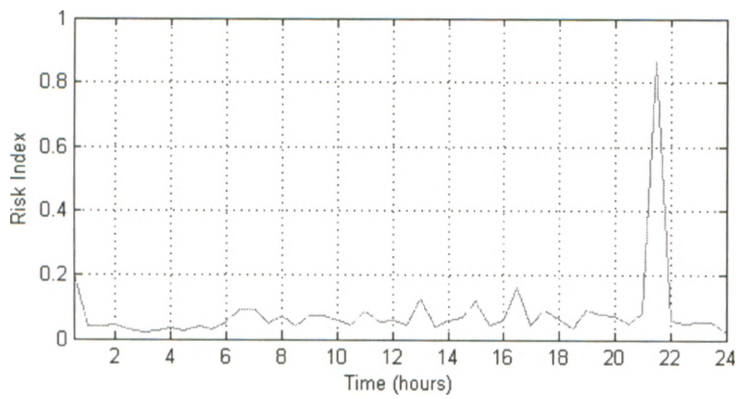


Figure 8.4: Temporal Risk Index for a Power System

Chapter 9 Intrusion Detection

9.1 Introduction

Intrusion Detection (ID) is the process of detecting a malicious intruder while attempting to or after entering a secure system. The basic framework for intrusion detection was given by Denning [55]. This chapter focusses on the issues related to intrusion detection encountered during the course of the research.

9.1.1 Motivation

During the study it was found out that numerous vulnerabilities of IED's can be effectively countered by intrusion detection. This was the main motivation to look into intrusion detection. In addition, it was decided to look into the need for intrusion detection in an IEC61850 network since it is not a mandatory security requirement like anti-malware or firewalls according to the NERC CIP requirements.

9.1.2 Basic Framework

The model proposed by Denning [55] focuses on intrusion detection by analysis of audit records of user activity and anomaly detection. Since this, numerous detection methods have been developed upon this framework from probabilistic methods [56], learning agents [57] to the use of artificial immune systems [58], [59]. A comprehensive analysis on different methods and technologies related to intrusion detection is given by McHugh [60].

9.1.3 Intrusion Detection Countermeasure

Experimentally, an Intrusion Detection System (IDS) was found to be the best countermeasure for the following attacks on an IEC61850 network:

1. ARP cache poisoning

2. CAM table flooding of switches using manipulated ARP packets
3. Switch port stealing using manipulated ARP packets
4. DoS attacks
5. Password crack attacks

The open source intrusion detection system *Snort* [52] was used for implementing the IEC61850 IDS.

9.2 ARP Traffic Monitor

The first experiment done related to intrusion detection was to determine a suitable countermeasure for ARP, cache poisoning, CAM table flooding and switch port stealing. For this purpose, it is necessary to monitor ARP traffic.

9.2.1 Data Collection

It was necessary to determine suitable bounds for normal ARP traffic in an average network. For this purpose, the ARP traffic of two subnets (129.100.227.xxx and 129.100.228.xxx) of the UWO network were captured for a period of 24 hours. Subsequently, the ARP traffic of one of the above networks with a host running an ARP sniffer was captured. The captured data is then analyzed and the results compared.

9.2.2 Normal ARP Traffic

Capturing of normal ARP traffic in a network is required to calibrate the IDS to detect abnormal amounts of ARP traffic generated during a CAM table flooding attack. Figure 9.1 shows the ARP traffic for each network for a 24 hour period. The histogram of the traffic (Figure 9.2) shows that usually less than 10 ARP packets are generated every second. This tallies with the data from an IEC61850 network (Figure 9.3) captured for a lesser duration (2000s) due to operational constraints. The statistics (Table 9.1) show that one average less than one ARP packet is generated per second for a computer network and around 1 for an IEC61850 network. Hence, if more than 100 ARP packets are generated on a regular basis, the situation can be deemed suspicious.

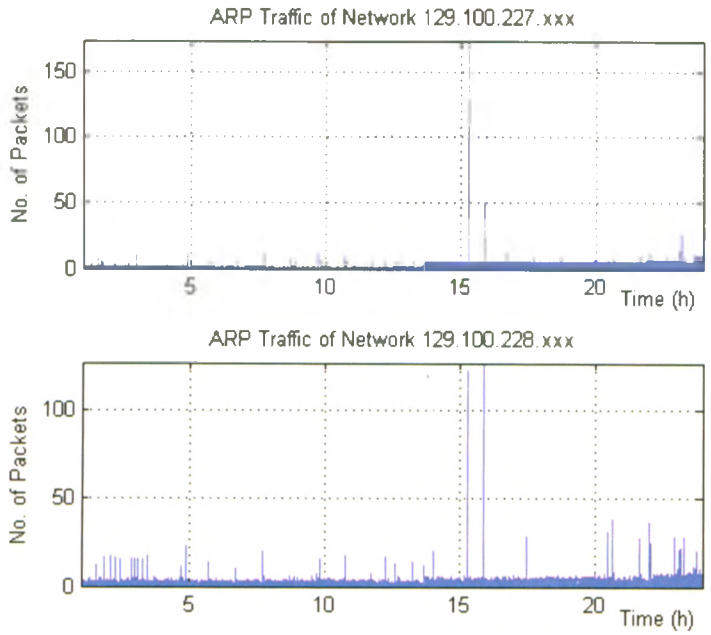


Figure 9.1: Normal ARP Traffic

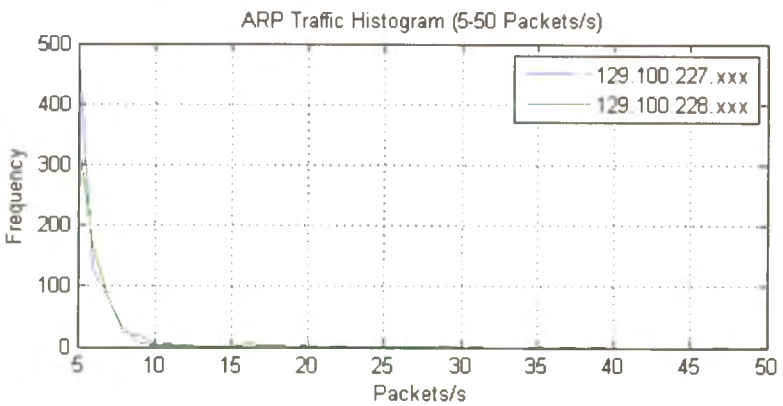


Figure 9.2: Normal ARP Traffic Histogram

Network	Traffic (Packets/s)	
	Mean	Maximum
129.100.227.xx	0.1793	174
129.100.228.xx	0.6289	127
IEC61850 (2000s only)	1.0191	6

Table 9.1: Normal ARP Traffic

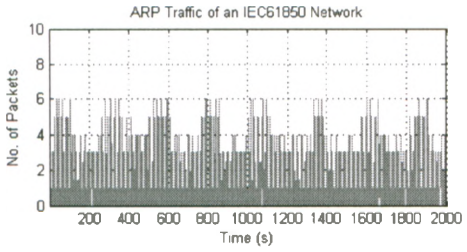


Figure 9.3: Normal ARP Traffic of an IEC61850 Network

9.2.3 ARP Sniffer Traffic

In the case of the ARP sniffer, the open source ARP sniffer *Seringe* was used [61]. This program does so by intercepting ARP requests and sending a forged reply with the MAC address of the host running the sniffer program. It was run on one of the hosts of the network with a packet sniffer running on another host. *Seringe* was run for nearly 1 hour on two hosts and compared with the histogram of the average ARP traffic generated during one hour by all hosts of the network under normal conditions. The results (Figure 9.4) indicate that the traffic generated by the host running the sniffer shows up abnormally with in excess of 1000 packets being generated compared to a normal value of less than 100.

Another indicator of the presence of a ARP sniffer can be found in the payload of the packet. A sniffer will produce ARP packets where the IP address of the Sender IP and Sender MAC address fields differ. This can be detected by analyzing the payload.

9.3 DoS Attacks

9.3.1 Data Collection

The data obtained during the simulated attacks on IED's (Section 7.3.1) is used for analysis. Based upon this, the necessary metrics are obtained for writing the IDS rules.

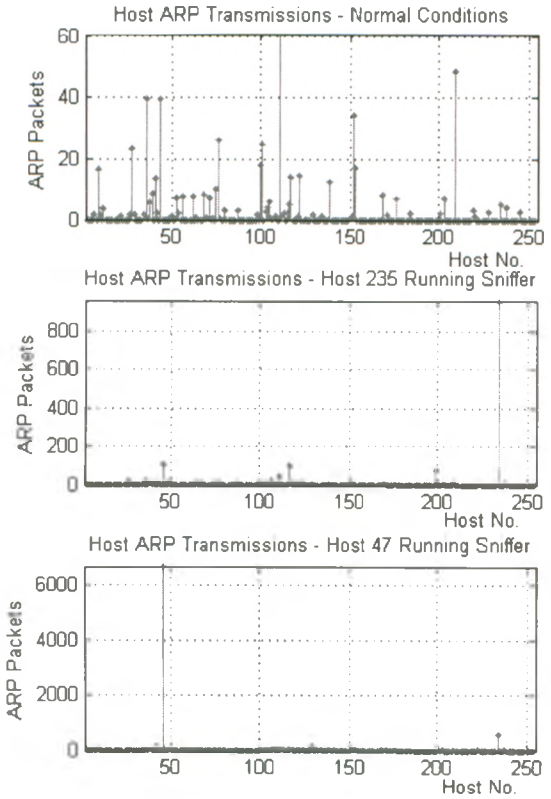


Figure 9.4: ARP Sniffer Traffic

9.3.2 Ping Attack

Overwhelming a host by a ping attack is a highly realistic possibility mainly because the ping command is commonly used as a network administration tool. Hence, it is necessary to differentiate between a genuine command and a malicious attack. For this, prominent features in the traffic have to be obtained for the IED.

Since the processing capabilities for the IED differ from a conventional host like a workstation or server, conventional IDS rules cannot be used. For analytic purposes, the incoming traffic from the remote host (i.e. the ping request sender) during a genuine command (Figure 9.5) and a dos attack (Figure 9.6) are used.

Table 9.2 shows the results of the analysis. The ping command with 12k of data is selected because it marks the threshold where performance of the device becomes

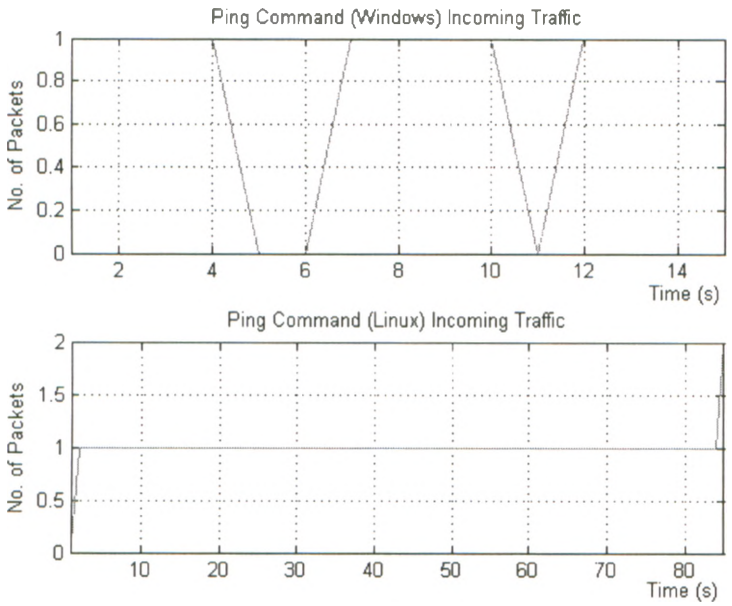


Figure 9.5: Ping Command Traffic

severely degraded (Table 7.1). The results show that all three features (packet size, arrival rate and interpacket delay) can be used as features to distinguish a genuine command from an attack.

Scenario	ICMP Packet Average Values		
	Size (Bytes)	Arrival Rate (Packets/s)	Separation (s)
Command (Windows)	74.0	0.8000	1.2433
Command (Linux)	98.0	1.0000	1.0000
DoS (12k)	1366.8	834.2	0.00120
DoS (18k)	1418.0	1140.2	0.00086
DoS (64k)	1489.5	3761.3	0.00025

Table 9.2: Ping Attack Results

In addition, when the size of the data of the ping exceeds the packet size, it is transmitted as a fragmented IP packet. This can also be detected via payload analysis.

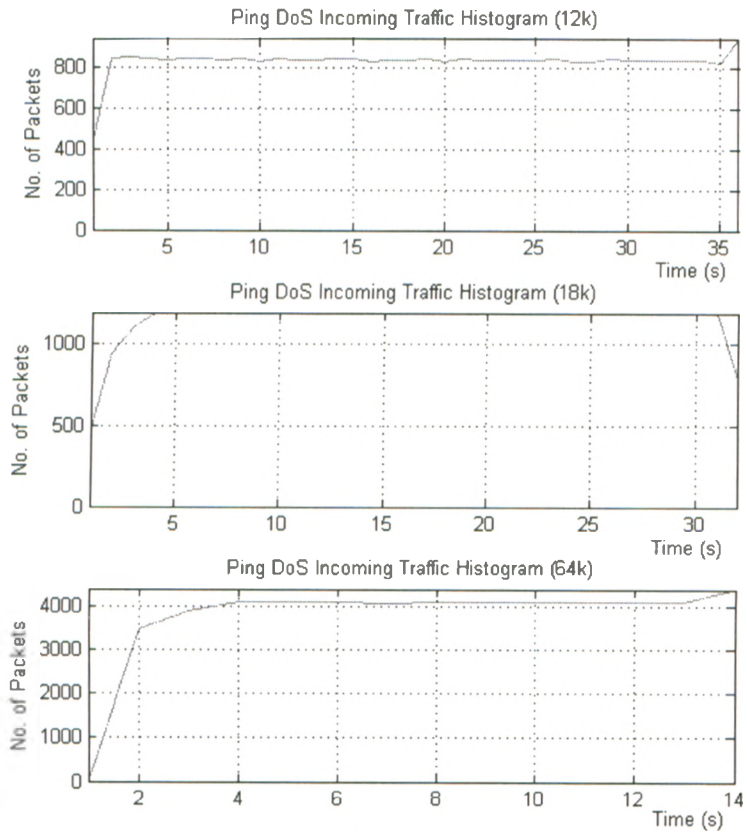


Figure 9.6: Ping DoS Traffic

9.3.3 Telnet and FTP Attack

Since only three parallel Telnet or FTP sessions are required to launch a trivial DoS attack, the IDS should be designed to recognize and react to the same host opening more than one connection in parallel. It is a reasonable assumption because in almost all cases, an authorized user using either the HMI software or command line interface of an IED would only require a single connection at a time.

9.4 Password Crack Attacks

9.4.1 FTP Password Crack

The FTP password crack attack using a dictionary produces an obvious, large amount of traffic. However, such a large amount of traffic can also be generated by a genuine user downloading a large file. Hence, the IDS will have to go deeper and perform payload analysis to find the repeating pattern of a login attempt.

9.4.2 Telnet Password Crack

Since Telnet prompts the user for the password, an attacker will have to develop code to handle the messages going back and forth during the login process. However, through payload analysis the IDS can detect the repeated request for a password along with the echoing of the asterisk.

9.5 System Development

The next stage is to develop the system. The open source network based intrusion detection system *Snort* was used for implementing the IEC61850 IDS.

9.5.1 Rule Development

From the data obtained through simulated attacks and experiments on ARP based packet sniffing, the following rules are derived.

1. More than n Telnet or FTP sessions started within a short period of time could indicate a DoS attack on the protocol
2. ARP packets with different IP's for the Sender IP and MAC address entries would indicate a packet sniffer attack
3. ARP traffic in excess of 100 packets per second is suspicious
4. ARP traffic in excess of 1000 packets per second is an indicator of an ARP sniffer
5. ICMP packets larger than 100 bytes indicate a Ping DoS

6. ICMP traffic in excess of 100 packets per second is an indicator of a Ping DoS
7. High frequency of the username being passed or '*' character being echoed via Telnet is a sign of a password crack attack
8. High number of attempts (> 5) of logins via FTP is an indicator of a FTP password crack attack
9. Fragmented ICMP packets will indicate a Ping DoS
10. HTTP packets with POST - HTTP password crack

The derived rules are then converted into rules of *Snort* syntax. ARP packet sniffing is handled by the ARP preprocessor of *Snort*.

The approach of *enumerating badness* allows the IDS to counter the known attacks effectively. However, in the event where an attacker develops a new type of attack, the IDS would be ineffective until the signature of the new attack is known. On the other hand a different approach known as *enumerated goodness* can also be employed. In this technique, genuine user activity is used to formulate the IDS rules and only activity that is deemed genuine is allowed. The shortcoming of this method is that exceptions in genuine user activity can always occur. It is impossible to anticipate all possible exceptions. Furthermore, the IDS would become highly inefficient with rules meant for exceptions that would very rarely occur.

9.5.2 IEC61850 IDS Connection

In the current situation of IEC61850 networks, there are two possible methods of including an IDS. The simplest and most effective method would be to include the IDS within the gateway (Figure 9.7). If this configuration is not feasible, it is possible to connect an IDS to a port mirroring the IEC61850 network connection to the gateway (Figure 9.8). This would effectively allow monitoring of all incoming traffic. This IDS is then tested on a network of IEC61850 IED's. The port mirrored IDS configuration is used as shown in Figure 9.9. Two remote hosts are used to test the system by launching simulated attacks and to generate genuine user traffic. Since the IDS is rule based and does not use any statistical or pattern recognition algorithm, a single test is sufficient to check if the attack can be detected. However, if the attacker

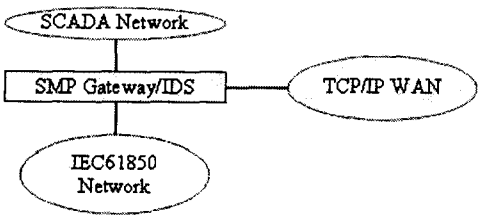


Figure 9.7: Gateway Based IDS

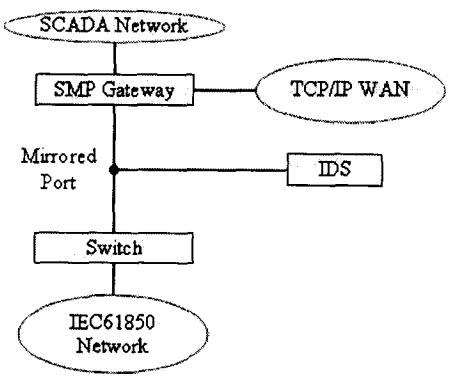


Figure 9.8: Port Mirrored IDS

changes the attack pattern sufficiently, the rule based detection scheme may fail. It also has the limitation of only being able to detect known attacks.

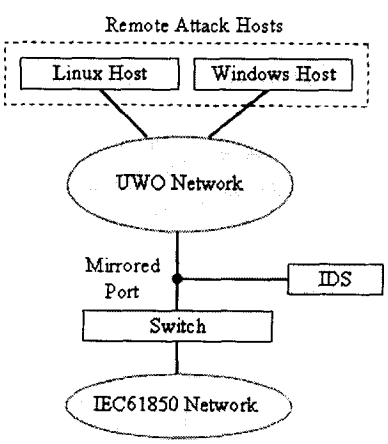


Figure 9.9: Experimental IDS Setup

9.5.3 Test Results

The IDS is tested for genuine scenarios (FTP session, Telnet session, HTTP browsing, ICMP pings and genuine ARP traffic) and malicious attacks (password crack attacks, DoS attacks and ARP packet sniffer attack). In the event of a malicious attack, *Snort* would issue an alert. The results (Table 9.3) show that the system is capable of detecting the malicious attacks and not respond to genuine user activity.

Scenario	Detection	
	Linux Host	Windows Host
FTP session	No	No
Telnet session	No	No
HTTP browse	No	No
ICMP ping	No	No
Normal ARP traffic	No	No
FTP DoS	Yes	Yes
Telnet DoS	Yes	Yes
ICMP flood	Yes	Not Applicable
FTP password crack	Yes	Not Applicable
Telnet password crack	Yes	Not Applicable
HTTP password crack	Yes	Not Applicable
ARP packet sniffer	Yes	Not Applicable

Table 9.3: IDS Scenario Detection

Chapter 10 Conclusions

10.1 IEC61850 Security

IEC61850 is a protocol developed with an emphasis on security. Its inherent security mechanisms are effective in guarding it against attacks on integrity, authenticity and confidentiality. In order to protect it from attacks on availability, additional security mechanisms such as firewalls and anti-malware are used. Currently, intrusion detection is not a mandatory component of an IEC61850 network. However, as the results show, it is an effective countermeasure since it can be actively adapted to counter newly innovated attacks by a determined attacker.

10.2 Security Auditing of IEC61850

This thesis also proposes a new scheme to audit the security of IEC61850 networks based on a novel metric to evaluate the security of IED's. This metric assesses the security based upon the possible threats to each individual IED.

When tested during a sample audit, it revealed that the network was secure as long as it is limited to a single LAN. In such a case the existing security measures would be sufficient to protect it from all foreseeable threats that can be launched from within the LAN. However, should it be interconnected via a WAN, it would become highly insecure. This fact is confirmed by simulated attacks where often trivial DoS attacks and password cracks can be launched on the IED's of the network.

This metric was also compared with two other metric schemes, namely the MTTC and the VEA-bility metric. Both metrics confirm the insecurity of the IEC61850 when connected to a WAN. However, it should be noted that the VEA-bility metric indicates that the network is insecure based on the CVE's of the database server and network switches. Despite using highly insecure protocols, there are no host CVE's for the IED's themselves. Analysis done on the MTTC reveal that it can be unrealistic. The IED metric on the other hand, indicates the poor security of the network when

interconnected based on vulnerabilities of the IED's themselves. Hence, it serves its purpose of providing a reliable audit of the security of the network.

10.3 Security Recommendations

10.3.1 Insecure Protocols

In general most IED's still use highly insecure protocols such as FTP, Telnet, Modbus and HTTP. Most of these insecure protocols have secure upgrades such as SSH (Telnet), SFTP (FTP) and HTTPS (HTTP). Countering threats to such insecure protocols would require specialized countermeasures. Such specialized countermeasures may turn out to be costly in the long run. Therefore, it would be necessary for IED manufacturers to collectively phase out such insecure protocols and keep in pace with the state of the art of network security.

10.3.2 IEEE 802.1ae MACsec

IEEE 802.1ae or MACsec is a scheme to provide encryption at the Medium Access Control (MAC) level. Currently traffic of IEEE 802.3 (Ethernet) or IEEE 802.11 (WiFi) has to be encrypted at a higher level to make it immune to eavesdropping. However, IEEE 802.1ae provides seamless encryption across different MAC protocols. Hence, inclusion of it to IED's would provide additional security for both wired and future wireless interfaces.

10.4 Future Work

Current IED's rely on simple but insecure protocols due to constraints in processing power and bandwidth. Therefore, future work should focus on a framework for IED design with a better emphasis on security. These next generation IED's could contain better access control techniques such as the use of private keys for authentication, to reduce the risk of password crack attacks, intelligent host based intrusion detection and intelligent anomaly detection.

References

[1] M. Bishop, "What is computer security?" *IEEE Security and Privacy*, vol. 1 (1), pp. 67–69, January/February 2003.

[2] S. Evans and J. Wallner, "Risk-based security engineering through the eyes of the adversary," in *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security*, 2005, pp. 158–165.

[3] R. E. Mackiewicz, "Overview of IEC61850 and benefits," in *IEEE Power Engineering Society General Meeting, 2006*, June 18-22 2006, pp. 1–8.

[4] IEC Technical Committee Number 57 (TC57), "IEC61850 Standard," International Electrotechnical Commission, Geneva, Switzerland, 2003.

[5] J. Holback, J. Rodriguez, C. Wester, D. Baigent, L. Frisk, S. Kunsman, and L. Hossenlopp, "Status on the first IEC61850 based protection and control, multi-vendor project in the United States," in *60th Annual Conference for Protective Relay Engineers, 2007*, 2007, pp. 283–306.

[6] V. M. Flores, D. Espinosa, J. Alzate, and D. Dolezilek, "Case study: Design and implementation of IEC61850 from multiple vendors at CFE La Venta II," in *60th Annual Conference for Protective Relay Engineers, 2007*, 2007, pp. 307–320.

[7] A. Prakash, M. S. Thomas, and A. Gautam, "Integration of IEDs using legacy and IEC61850 protocol," in *International Conference on Power Electronics, Drives and Energy Systems, 2006*, December 2006, pp. 1–5.

[8] Y. Yi, Y. J. Cao, Y. San, Y. Guan, B. Liu, and C. Guo, "An IEC61850 universal gateway based on metadata modeling," in *IEEE Power Engineering Society General Meeting, 2007*, 2007, pp. 1–5.

[9] T. S. Sidhu and Y. Yin, "Modelling and simulation of performance evaluation of IEC61850 based substation communication systems," *IEEE Transaction on Power Delivery*, vol. 22 (3), pp. 1482–1489, July 2007.

[10] G. Zhanjun, P. Zhencun, B. Peng, and W. Bin, "A new modeling approach to protective relaying and fault information systems," in *International Conference on Power System Technology, 2004*, November 21-24 2004, pp. 340–343 vol.1.

[11] L. Beil and M. Lian-shunl, "To realize the SCL configurator of IEC61850 based on relative model," in *International Conference on Power System Technology, 2006*, October 2006, pp. 1–7.

[12] Q. Chen, H. Ghenniwa, and W. Shen, "Web-services infrastructure for information integration in power systems," in *Power Engineering Society General Meeting, 2006*, June 18-22 2006, pp. 1–8.

[13] J. Hughes, "IntelliGrid architecture concepts and IEC61850," in *2005/2006 IEEE PES Transmission and Distribution Conference and Exhibition*, May 21-24 2006, pp. 401–404.

[14] L. Xu and S. Ma, "A distributed architecture for substation information integration," in *Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies*, April 6-9 2008, pp. 877–881.

[15] T. Sidhu and P. K. Gangadharan, "Control and automation of power system substations using IEC61850 communication," in *Proceedings of the 2005 IEEE Conference on Control Applications, Toronto, Canada*, August 28-31 2005, pp. 1331–1336.

[16] D. Dolezilek, "IEC 61850: what you need to know about functionality and practical implementation," Date Accessed: 2008.02.05. [Online]. Available: http://www.selinc.com/techpprs/SEL_Dolezilek_IEC61850_6170.pdf

[17] M. P. Pozzuoli, "Ethernet in substation automation applications - issues and requirements," Date Accessed: 2008.02.06. [Online]. Available: http://www.ruggedcom.com/pdfs/white_papers/ethernet_in_substation_automation_applications.pdf

[18] F. B. Schneider, "Enforceable security policies," *ACM Transactions on Information and System Security*, vol. 3 (1), pp. 30–50, February 2000.

[19] S. Hariri, Q. Guangzhi, T. Dharmagadda, M. Ramkishore, and C. Raghavendra, "Impact analysis of faults and attacks in large-scale networks," *IEEE Security and Privacy*, vol. 1 (5), pp. 49–54, September/October 2003.

[20] K. P. Yee, "Aligning security and usability," *IEEE Security and Privacy*, vol. 2 (5), pp. 48–55, September/October 2004.

[21] E. Jonsson and T. Olovsson, "A quantitative model of the security intrusion process based on attacker behavior," *IEEE Transactions on Software Engineering*, vol. 23 (4), pp. 235–245, April 1997.

[22] Honeynet Project, "Honeynet attack data," Date Accessed: 2008.06.30. [Online]. Available: http://www.honeynet.org

[23] L. Spitzner, "The honeynet project:trapping the hackers," *IEEE Security and Privacy*, vol. 1 (2), pp. 15–23, March/April 2003.

[24] K. W. Lie and J. M. Wing, "Game strategies in network security," *International Journal of Information Security*, vol. 4 (1-2), pp. 71–86, February 2005.

[25] T. Ohta and T. Chikaraishi, "Network security model," in *Proceedings of IEEE Singapore International Conference on Networks*, September 6-11 1993, pp. 507–511.

[26] G. N. Ericsson and A. Torkilseng, "Management of information security for an electric power utility - on security domains and use of ISO/IEC17799," *IEEE Transactions on Power Delivery*, vol. 20 (2), pp. 683–690, 2005.

[27] W. Stallings, *Cryptography and Network Security Principles and Practice.* Upper Saddle River, NJ: Prentice Hall, 1998.

[28] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, *Advances in Computer, Information, and Systems Sciences, and Engineering Proceedings of IETA 2005, TeNe 2005, EIAE 2005.* Springer Netherlands, 2006, ch. DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework, pp. 227–234.

[29] J. Pollet, "Developing a solid SCADA security strategy," in *2nd ISA/IEEE Sensors for Industry Conference, 2002*, 2002, pp. 148–156.

[30] T. Paukatong, "SCADA security: A new concerning issue of an in-house EGAT-SCADA," in *Asia and Pacific, 2005 IEEE/PES Transmission and Distribution Conference and Exhibition*, 2005, pp. 1–5.

[31] R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa, and S. Shenoi, *Critical Infrastructure Protection.* Springer Boston, 2007, ch. Security Strategies for SCADA Networks, pp. 117–131.

[32] IEC Technical Committee Number 57 (TC57), "IEC62351 Standard," International Electrotechnical Commission, Geneva, Switzerland, 2007.

[33] NERC, "NERC CIP Standards," Date Accessed: 2008.04.17. [Online]. Available: http://www.nerc.com/pub/sys/all_updl/\standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf

[34] National Institute of Standards and Technology, "Security metrics guide for informatioin technology," Date Accessed: 2008.06.21. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

[35] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup, "A weakest adversary security metric for network configuration security analysis," in *Proceedings of the ACM Workshop on Quality of Protection*, 2006, pp. 31–38.

[36] D. J. Leversage and E. J. Byres, "Estimating a system's mean time to compromise," *IEEE Security and Privacy*, vol. 6 (1), pp. 52–60, January-February 2008.

[37] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Time-to-compromise model for cyber risk reduction estimation," in *First Workshop on Quality of Protection, Quality of Protection: Security Measurements and Metrics.* Springer, 2005.

[38] CVSS Team, "Common vulnerability scoring system," Date Accessed: 2008.06.16. [Online]. Available: http://www.first.org/cvss/v1/guide.html

[39] M. Tupper and A. N. Zincir-Heywood, "VEA-bilty security metric: A network security analysis tool," in *The Third International Conference on Availability, Reliability and Security*, 2008, pp. 950–957.

[40] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security and Privacy*, vol. 4 (6), pp. 85–88, November-December 2006.

[41] R. Deraison, J. Beale, C. Van Der Walt, R. Temmingh, R. Alder, J. Alderson, A. Johnson, and G. A. Theall, *Nessus Network Auditing.* Syngress Publishing, 2004.

[42] C. Davis, M. Schiller, and K. Wheeler, *IT Auditing Using Controls to Protect Information Assets.* New York: McGraw-Hill, 2007.

[43] E. Johansson and P. Johnson, "Assessment of enterprise information security - the importance of prioritization," in *Proceedings of the 2005 Ninth IEEE International EDOC Enterprise Computing Conference (EDOC'05)*, 2005.

[44] J. Messer, *Secrets of Network Cartography: A Comprehensive Guide to nmap.* NetworkUptime.com, 2007.

[45] L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, P. Huang, s. McCanne, K. Varadhan, X. Ya, and Y. Haobo, "Advances in network simulation," *IEEE Computer*, vol. 33 (5), pp. 59–67, May 2000.

[46] R. Spangler, "Packet sniffing on layer 2 switched local area networks," Date Accessed: 2008.10.03. [Online]. Available: http://www.packetwatch.net/documents/papers/layer2sniffing.pdf

[47] G. Y. Liao, Y. J. Chen, W. C. Lu, and T. C. Cheng, "Toward authenticating the master in the modbus protocol," *IEEE Transactions on Power Delivery*, vol. 23 (4), pp. 2628–2629, October 2008.

[48] D. G. Peng, H. Zhang, L. Yang, and H. Li, "Design and realization of modbus protocol based on embedded linux system," in *International Conference on Embedded Software and Systems Symposia, 2008*, 2008, pp. 275–280.

[49] The Hackers Choice, "Hydra homepage," Date Accessed: 2008.10.20. [Online]. Available: http://freeworld.thc.org/thc-hydra/

[50] H. P. A. V. Dongen and D. F. Dinges, *Principles and Practice of Sleep Medicine*, 3rd ed. Philadelphia, Pennsylvania: W. B. Saunders, 2000, ch. Circadian Rhythms in Fatigue, Alertness and Performance, p. 391 to 399.

[51] D. A. Conroy, A. J. Spielman, and R. Q. Scott, "Daily rhythm of cerebral blood flow velocity," *Journal of Circadian Rhythms*, vol. 3 (3), 2005.

[52] B. Caswell, J. C. Foster, R. Russel, J. Beale, and J. Poslus, *Snort 2.0 Intrusion Detection*. Syngress Publishing, 2003.

[53] W. Hu, J. Li, and J. Shi, "A novel approach to cyperspace security situation based on the vulnerabilities analysis," in *Proceedings of the 6th World Congress on Intelligent Control and Automation, Dalian, China*, June 21-23 2006, pp. 4747–4751.

[54] National Electricity Market, Australia, "Power demand for NSW for March 2008," Date Accessed:2008.06.03. [Online]. Available: http://www.nemweb.com.au/mms.GRAPHS/data/DATA200803_NSW1.csv

[55] D. Denning, "An intrusion detection model," *IEEE Transactions on Software Engineering*, vol. SE-13 (2), pp. 222–232, February 1987.

[56] N. Ye, X. Li, Q. Chen, S. M. Emran, and M. Xu, "Probabilistic techniques for intrusion detection based on computer audit data," *IEEE Transactions on Systems, Man and Cybernetics-Part A: Systems and Humans*, vol. 31 (4), pp. 266–274, July 2001.

[57] Z. Yu, J. J. P. Tsai, and T. Weigert, "An automatically tuning intrusion detection system," *IEEE Transactions on Systems, Man and Cybernetics-Part B: Cybernetics*, vol. 37 (2), pp. 373–384, April 2007.

[58] D. Dasgupta and F. Gonzalez, "An immunity-based technique to characterize intrusions in computer networks," *IEEE Transactions on Evolutionary Computation*, vol. 6 (3), pp. 281–291, June 2002.

[59] P. K. Harmer, P. D. Williams, G. H. Gunsch, and G. B. Lamont, "An artificial immune system architecture for computer security applications," *IEEE Transactions on Evolutionary Computation*, vol. 6 (3), pp. 252–280, June 2002.

[60] J. McHugh, "Intrusion and intrusion detection," *International Journal of Information Security*, vol. 1 (14), pp. 14–35, July 2001.

[61] SecuriTeam, "Seringe - Statically Compiled ARP Poisoning Tool," Date Accessed: 2008.10.16. [Online]. Available: http://www.securiteam.com/tools/5QP0I2AC0I.html