Security Analysis and Auditing of IEC61850 Based Automated Substations

Upeka Premaratne, Jagath Samarabandu, *Member, IEEE*, Tarlochan Sidhu, *Fellow, IEEE*, Robert Beresh, *Senior Member, IEEE* and Jian-Cheng Tan, *Member, IEEE*.

***Abstract*—This paper proposes a scheme for auditing the security of an IEC61850 based network based upon a novel security metric for Intelligent Electronic Devices (IED's). A detailed security analysis on an IEC61850 automated substation is done initially with a focus on the possible goals of the attacker. This is followed by the development of a scheme to audit the security of such a network. Security metrics are considered since they provide a tangible means of quantifying the security of a network. The proposed auditing scheme is tested by using it to audit the security of an IEC61850 network. The results are then compared with two other metric schemes, the Mean Time to Compromise (MTTC) metric and VEA-bility metric which are used for auditing conventional computer networks. The input data for both metrics are obtained by using a network security tool to scan the IED's of the network. The impact of using high traffic generating network security tools on a time critical IEC61850 network is also investigated.**

***Index Terms*—Information security, security analysis, security auditing, security metrics, IEC61850, security tools, substation automation**

I. Introduction

IEC61850 is an Ethernet (IEEE 802.3) based communication standard proposed for control and automation of electric substations. It was developed jointly by the IEC (International Electrotechnical Commission) and IEEE with the aim of providing a flexible and interpretable communication system which could be easily integrated into the infrastructure of existing substations [1].

Electric substations are critical installations in the electric power grid and hence, a prime target for malicious activity. This paper focuses on a novel method to assess and audit the security of a IEC61850 based network.

This paper commences with a security analysis of electric substations (Section II). This is followed by an introduction to the proposed auditing scheme (Section III). Section IV introduces the novel metric for IED's. The impact of security tools on the network is investigated in Section V. Section VI details the results of the sample audit using the scheme.

II. 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 the perspective of an attacker.

U. Premaratne, J. Samarabandu and T. Sidhu are with the Department of Electrical and Computer Engineering, University of Western Ontario, London, Ontario, Canada, N6A 3K7 e-mail: upeka@ent.mrt.ac.lk, jagath@uwo.ca, sidhu@eng.uwo.ca.

B. Beresh and J. C. Tan are with Kinectrics Inc., Toronto, Ontario, Canada, M8Z 6C4 e-mail:{bob.beresh,jian-cheng.tan}@kinectrics.com

Manuscript received January 15, 2009. Submitted with revisions October 18, 2009 and accepted for publication on December 27, 2009.

A. 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 [2]. The enforceability of a security policy depends on the mechanisms used [3] which should be selected in a manner that they do not compromise the performance of the system [4], [5]. The report of the Power System Relaying Committee of the IEEE Power and Energy Society [6], [7] provides a comprehensive listing of security mechanisms applicable to IED's.

B. Attacker Perspective

The other method of security design involves looking at the problem through the perspective of the attacker [8]. 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 [9] and bait networks known as Honeypots [10]. In a Honeypot, a network is set up with the intent of luring and recording the behavior of real attackers.

C. Threat Identification

The next step would be to apply the analysis technique to the IEC61850 based system. In this context, two main attacker goals can be identified using the attacker perspective approach [8]. These are:

1) Disruption of the utility service (attack on availability).
2) Gaining access to confidential information for malicious purposes such as unfair competition, blackmail etc (attack on confidentiality).

Only two of the four types of attacks listed by Stallings [11], are listed. In for example, a financial institution, modification and fabrication would be likely goals of the attacker. However, 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 and shutdown a substation (goal of disrupting service) or obtain confidential information [12].

These two goals can then be analyzed in detail to identify the methods an attacker can use to achieve them. Such generic attacks along with their possible countermeasures can be identified using the approach of Ohta and Chikaraishi [13] as shown in Tables I and II.

TABLE I
ATTACKS ON CONFIDENTIALITY

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 II
DISRUPTION OF SERVICE

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

D. IEC61850 Security Mechanisms

The existing security mechanisms of IEC61850 are mentioned in IEC62351-4 and IEC62351-6 [14]. 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).
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.

In addition, the North American Electrical Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard for the protection of critical cyber assets, requires the incorporation of firewalls and anti-malware for compliance [15]. These security mechanisms are capable of countering a significant number of security threats listed in Tables I and II. However, a determined attacker is bound to innovate new methods over time to compromise these existing security mechanisms.

III. PROPOSED SECURITY AUDITING SCHEME

Security auditing is the process of assessing the security of a computer system and making recommendations to the client. The IEC61850 network to be audited consists of the IED's, switches, routers, firewall/gateway, HMI and servers. The proposed audit scheme consists of the following stages:

1) Preliminary survey of the network to identify its components, topologies etc.
2) Security assessment of the hosts of the network (e.g. IED's, gateway, HMI and servers) and other components (e.g. switches and routers).
3) Disclosing the results and recommendations to the client
4) Verification of implementation of recommendations

Out of these stages, the focus of this paper is on the security assessment of the hosts. This stage consists of:

1) A security tool assessment to uncover potential vulnerabilities of the entire network that may be visible to an attacker
2) An IED assessment to unravel the vulnerabilities of each IED and calculate the proposed IED metric from the results obtained

The scope of this auditing scheme is focused on the network infrastructure and can be integrated into organization wide security audits such as ISO/IEC27001 [16].

IV. NOVEL IED SECURITY METRIC

The main motivation behind research into obtaining metrics for network security is to provide a tangible means of measuring the security of a network [17]. Due to the technical difference between an IED and a standard computer, applying the Common Vulnerability Scoring System (CVSS) which is used by National Institute for Standards and Technology (NIST) [18] for threats can only be done for computer based nodes of an IEC61850 network such as database servers, engineering stations, HMI's and gateways. Hence, it is necessary to come up with an entirely new metric scheme for IED's. This new metric scheme is compared with security metrics developed for conventional computers. These include the Mean Time to

Compromise (MTTC), proposed by Leversage and Byres [19] and McQueen *et al.* [20] and the VEA-bility metric proposed by Tupper and Zincir-Heywood [21].

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.

A. 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. In addition, hidden security threats due to the use of insecure protocols (e.g. ftp, telnet) or security vulnerabilities in the operating systems can be identified by the scan done by the security tool. 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.
5) Stepping Stone (SS) - the IED can be logically used as a stepping stone to launch an attack on another target.

B. 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. These are determined by:

1) Scrutinizing the security features of the IED as specified by the manufacturer (e.g. encryption of data, use of secure protocols).
2) Examining the security mechanisms of the network infrastructure (e.g. MAC address restriction by the switches to counter a DoS or ARP sniffer attack).
3) In case the device has vulnerabilities in its software or operating system, check for available countermeasures in vulnerability repositories such as the Common Vulnerabilities and Exposures (CVE) database.

If a particular threat has the appropriate countermeasures it can be nulled (i.e. eliminated) from the threat list.

C. 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 relative risk or likeliness of the attack based upon the location of the attacker.

D. 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) Prior identification of all known threats to each individual IED (m threats).
2) Identification of the available countermeasures for each threat i (where $i = 1, 2, \ldots, m$). If a particular threat has one or more countermeasures, its countermeasure factor (c_i) is set to one. The value of c_i is set to 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 based upon their likelihood. The most likely type of attack is a remote attack launched from a distant location while the least likely is an attack involving physical manipulation of a device where there is a high risk of the attacker being detected.
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

To calculate the score for a particular threat (t_i) based upon its susceptibility (s_i) and countermeasure factor (c_i).

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

The score for the j^{th} IED with m_j threats would hence be:

$$E_j = \sum_{i=1}^{m_j} t_i \tag{2}$$

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

$$R = 10 - min(10, \sum_{j=1}^{n} E_j) \tag{3}$$

E. Compliance Threshold

Based on the final score (R) it is possible to define a compliance threshold. For example, the network can be considered secure if and only if the score for R *exceeds* 9. In such a case:

- A minor vulnerability where the attack needs to be executed by directly manipulating the IED or over the LAN would bring down the score to 9.9 or 9.8 respectively
- If the network has a serious vulnerability where an attack can be launched over the WAN, the score would become 9 so the network will be vulnerable and non-compliant
- If there are a small number of serious vulnerabilties or a large number of minor vulnerabilities, the score will tend towards 0 and indicate a highly insecure network

Due to this, normalization of the result according to the size of the network or considering the geographical spread is not needed.

V. Security Tool Traffic Analysis

The delivery time for certain packets of IEC61850 is critical. The proposed security auditing scheme relies heavily on data obtained from scans on the IED's using security tools. Therefore, 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.

A. Data Collection

Data is collected using Ethereal, an open source network analyzer available on both Windows and Linux platforms. While Ethereal is running, each security tool 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 and NMap 4.68. Both tools were tested on Windows and Linux platforms.

NMap 4.68 is a tool capable of identifying the operating system and list a limited amount 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 is that unlike its open source counterpart, the tests that are performed by the tool are not listed and its comprehensive assessment generates a large amount of traffic.

B. Data Analysis

The collected data is then analyzed using MATLAB. The instantaneous traffic rate in packets per second for each scan is first calculated. If the instantaneous traffic rate is greater than 100 packets/s then it is considered high and based on this, the time during which the generated traffic is high is obtained.. From this the average time during which the security tool generates high traffic can be obtained. Table III gives the traffic statistics for each tool for a particular host platform. According to it, Nessus which does a more comprehensive set of tests takes longer to assess a Windows machine than Linux machine. The same can be said of Nmap. Figures 1 and 2 show typical security tool traffic profiles for computers. The important factor to be considered is the time during which the tool generates high traffic. Table IV shows the summary of high loading for different tools and target machines, approximated to the nearest multiple of 5 for convenience. Further study on the impact of security tools is done via simulations.

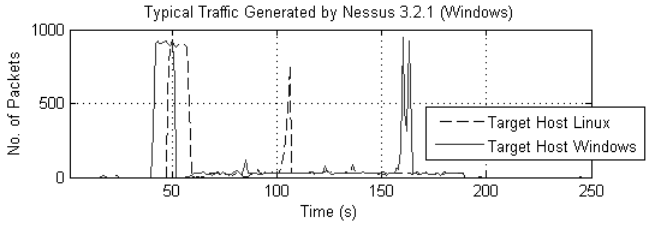

Fig. 1. Typical Traffic Generated by Nessus 3.2.1 (Windows)

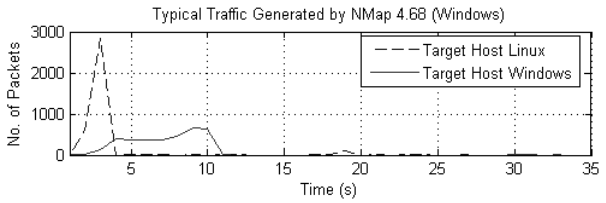

Fig. 2. Typical Traffic Generated by NMap 4.68 (Windows)

TABLE IV
Security Tool High Traffic Loading Time (Approximate)

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

C. Parallel Scans

Nessus 3.2.1 allows multiple hosts to be scanned in parallel. Figure 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 a single host (Tables III). For nearly 80% of the scan time (110s) the traffic is significantly greater than 100 packets/s.

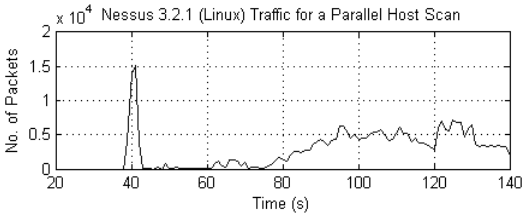

Fig. 3. Traffic Generated by Nessus 3.2.1 (Linux) for a Parallel Host Scan

TABLE III
SECURITY TOOL TRAFFIC STATISTICS

Target Host Platform	Tool (Platform)	Mean Traffic Rates (packets/s)			Mean Scan Time (s)	
		Mean	Maximum	High (%)	Total	High
Windows	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
Linux	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

D. Simulation

Simulation of the effect of the security tool is done using the open source simulator called Network Simulator 2.33 (NS 2.33). Using the simulation, the delay and drop rate of packets are analyzed and compared to the standards of IEC61850-5.

1) IED Model: NS-2 logically abstracts a network node (Figure 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 connect nodes together.

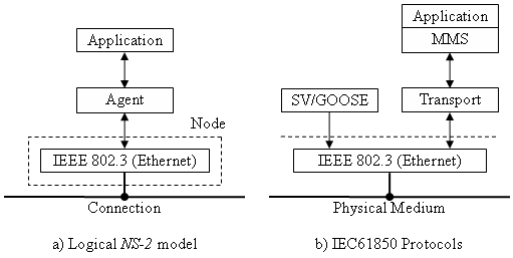

Fig. 4. NS-2 Logical Model

In order for two nodes to communicate, 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. 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.

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 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 6.

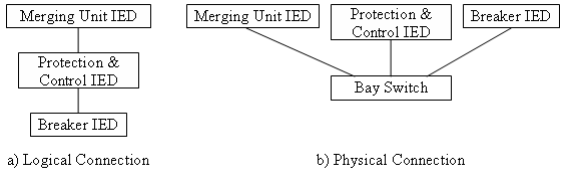

Fig. 5. Physical and Logical Connection of a Bay Network

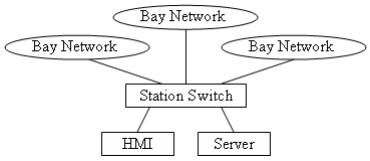

Fig. 6. Topology of Entire Substation Network

For the simulation, a substations consisting of two transformer bays and two to six transformer bays are used. Each MU is assumed to take 1920 raw data samples per second to achieve class P3 protection [22]. During 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 eeach way. A fault is simulated every 0.5s. In addition, each PC IED uploads a 2kb status report to the server every 2s.

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 IV). Due to constraints of simulation time and in order to generalize the situation, the burst duration is restricted to 10s 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.

4) Results: Tables V shows 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

The results clearly show that whenever the tool is in use there is a significant increase in the packet drop rate. The effect on packet delay does not appear to be significant. Despite that, the safety of the network is still affected because during the use of the security tool, a critical packet (e.g. GOOSE packet) can get dropped.

VI. Sample Audit

This section details a sample audit done on a IEC61850 network. The network contained the IED's given in Table VI. 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.

TABLE VI
Sample IEC61850 Network Devices

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

A. 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 VII) 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.

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 (Table III), the time during which the security tool loads the network with more then 100 packets is much less for either security tool. On average, for Nessus (Table VIII) it is just around 0.5s and for NMap (Table IX) it is around 0.15s.

B. MTTC Calculation

Table X shows the MTTC for the hosts of the network based upon individual vulnerabilities. The MTTC for the entire network is 1.8806 days. 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.

TABLE VII
Security Tool Scan Results - Open Ports

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)	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 VIII
Security Tool Traffic Statistics - Nessus 3.2.1

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

C. VEA-bility Calculation

The VEA-bility score of the network is obtained from the Common Vulnerabilities and Exposures (CVE)'s of the network. Table XI 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 is zero for all devices. The individual score is then multiplied by the number of devices to get the VEA-bility score of the entire network (Table XII). The final score of 3.333 indicates a highly insecure network.

TABLE V
NETWORK SIMULATION RESULTS

Scenario	2 Feeder Bays				4 Feeder Bays				6 Feeder Bays			
	Delay (ms)		Drop (%)		Delay (ms)		Drop (%)		Delay (ms)		Drop (%)	
	10Mb	100Mb	10Mb	100Mb	10Mb	100Mb	10Mb	100Mb	10Mb	100Mb	10Mb	100Mb
1	9.81	1.17	3.79	1.35	10.10	1.21	3.97	1.52	9.49	1.17	3.78	1.40
2	11.15	1.15	4.75	1.72	10.33	1.20	4.08	1.61	10.45	1.15	4.60	1.70
3	5.76	1.23	34.46	14.02	7.04	1.21	26.55	7.57	9.04	1.15	36.07	6.76
4	7.35	1.23	41.43	10.53	8.10	1.25	23.97	9.41	8.20	1.19	25.05	8.06
5	12.24	1.19	10.80	1.94	9.73	1.16	6.50	1.50	10.52	1.17	6.05	1.50
6	10.57	1.16	8.58	1.91	11.54	1.25	6.85	1.82	9.94	1.16	6.60	1.95
7	7.45	1.20	43.05	10.45	7.78	1.24	28.23	8.44	8.70	1.21	25.72	5.77
8	7.73	1.22	32.36	7.85	8.68	1.21	15.11	11.51	9.39	1.19	33.64	6.60

TABLE XII
SAMPLE NETWORK VEA-BILITY SCORE

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 IX
SECURITY TOOL TRAFFIC STATISTICS - NMAP 4.68

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 X
SAMPLE NETWORK HOST VULNERABILITIES

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 XI
SAMPLE NETWORK HOST VULNERABILITY CVSS SCORES

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

D. IED Assessment - GROUP1

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.

1) 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 [23], 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.

2) 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 these devices is trivial and the passwords are prompted. Since telnet transmits character by character, an automated brute force attack would be 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

TABLE XIII
COUNTERMEASURES FOR GROUP1 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
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

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 of the IED which can be found by consulting the manual.

3) Denial of Service Attacks: There are two possible scenarios of an attacker launching a DoS attack on these 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.

4) Countermeasures: Table XIII shows the countermeasures for the possible attacks on GROUP1 devices. 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.

E. IED Assessment - GROUP2

The devices 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.

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 [24]. 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 VI-D1.

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.

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.

TABLE XIV
COUNTERMEASURES FOR 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 Protocol Password Crack	LAN	MAC address restriction Physical protection
Unauthorized Access	LAN	Dual operator confirmation
ICMP DoS Protocol Password Crack	WAN	Blocking via Firewall Detection and reaction via IDS
Unauthorized Access	WAN	Dual operator confirmation

TABLE XV
COUNTERMEASURES FOR THE GROUP3 DEVICE

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 Protocol Password Crack	LAN	MAC address restriction Physical protection
ICMP DoS Protocol Password Crack	WAN	Blocking via Firewall Detection and reaction via IDS

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.

5) Countermeasures: Table XIV gives the countermeasures for the possible threats for all GROUP2 devices.

F. IED Assessment - GROUP3

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 (Section VI-D1) as the former two.
- Both http and ftp protocols are vulnerable to protocol password crack attacks.
- It is also vulnerable to a ICMP DoS attack.

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

G. 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

TABLE XVI
METRIC CALCULATION FOR GROUP1 DEVICES

Threat	Category	s	c	t
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 XVII
METRIC CALCULATION FOR GROUP2 DEVICES

Threat	Category	s	c	t
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 XVIII
METRIC CALCULATION FOR THE GROUP3 DEVICE

Threat	Category	s	c	t
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

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.

H. 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 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.

I. 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. 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.

J. IED Metric Calculation

In order to calculate the IED metric for the entire network, the score for each threat is evaluated using Equation 1 from the data of Tables XVI, XVII and XVIII. 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 using Equation 2 the total threat score (E_j) is calculated for each IED (Table XIX). The metric for the entire network can be obtained from Equation 3. It is calculated assuming that the network is only limited to a single LAN or interconnected to a WAN.

K. Audit Results

Table XX 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.

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

TABLE XIX
NETWORK METRIC CALCULATION

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 XX
NETWORK METRIC SCORES

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

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 obtained using Equation 3, indicates the poor security of the network based on vulnerabilities of the IED's themselves.

VII. CONCLUSIONS

Electric substations are prime targets for malicious attackers. Hence being able to assess the information security of electric substations is an essential need, especially with increased interconnection over insecure public networks. The novel metric scheme introduced in this paper shows promise when used to perform a security audit on a sample IEC61850 network.

In order to perform security audits, it is necessary to use network security tools. Tests on personal computers and simulations reveal that they have a high impact in terms of introduced traffic which result in high network traffic and high packet drop rates. However, the tests on IED's show that the times during which the tools introduce high volumes of traffic is substantially less than that of personal computers.

In general most IED's still use highly insecure protocols which 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. During the course of the research it was revealed that intrusion detection on a network and host level can be considered as a viable security countermeasure for IEC61850 networks. Future work would consist of investigating this further.

ACKNOWLEDGEMENTS

The authors would like to thank Harry Ou for his assistance during the sample audit and Kinectrics, 800 Kipling Avenue, Toronto, Ontario, Canada, M8Z 6C4 for funding for the research.

REFERENCES

[1] R. E. Mackiewicz, "Overview of IEC61850 and benefits," in *IEEE Power Engineering Society General Meeting, 2006*, June 18-22 2006, pp. 1–8.
[2] M. Bishop, "What is computer security?" *IEEE Security and Privacy*, vol. 1 (1), pp. 67–69, January/February 2003.
[3] F. B. Schneider, "Enforceable security policies," *ACM Transactions on Information and System Security*, vol. 3 (1), pp. 30–50, February 2000.
[4] 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.
[5] K. P. Yee, "Aligning security and usability," *IEEE Security and Privacy*, vol. 2 (5), pp. 48–55, September/October 2004.
[6] C1 Working Group Members of Power System Relaying Committee, "Cyber security issues for protective relays," in *IEEE Power Engineering Society General Meeting, 2007*, 2007, pp. 1–8.
[7] C1 Working Group Members of Power System Relaying Committee, "Cyber security issues for protective relays," Date Accessed:2008.12.04. [Online]. Available: http://www.pes-psrc.org/Reports/Cyber Security Issues for Protective Relays.pdf
[8] 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.
[9] 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.
[10] Honeynet Project, "Honeynet attack data," Date Accessed: 2008.06.30. [Online]. Available: http://www.honeynet.org
[11] W. Stallings, *Cryptography and Network Security Principles and Practice*. Upper Saddle River, NJ: Prentice Hall, 1998.
[12] U. Premaratne, J. Samarabandu, T. Sidhu, B. Beresh, and J. C. Tan, "Evidence theory based decision fusion for masquerade detection in IEC61850 automated substations," in *International Conference on Information and Automation for Sustainabilty*, 2008, pp. 194–199.
[13] T. Ohta and T. Chikaraishi, "Network security model," in *Proceedings of IEEE Singapore International Conference on Networks*, September 6-11 1993, pp. 507–511.
[14] IEC Technical Committee Number 57 (TC57), "IEC62351 Standard," International Electrotechnical Commission, Geneva, Switzerland, 2007.
[15] 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
[16] ISO/IEC Joint Technical Committee Number 1 (JTC1), "ISO/IEC27001 Standard," ISO/IEC, Geneva, Switzerland, 2005.
[17] 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
[18] CVSS Team, "Common vulnerability scoring system," Date Accessed: 2008.06.16. [Online]. Available: http://www.first.org/cvss/v1/guide.html
[19] 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.
[20] 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.
[21] 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.
[22] IEC Technical Committee Number 57 (TC57), "IEC61850 Standard," International Electrotechnical Commission, Geneva, Switzerland, 2003.
[23] 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
[24] 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.

Upeka Premaratne obtained his B.Sc.Eng. in Electronic and Telecommunication Engineering from the University of Moratuwa, Sri Lanka in 2005. He is currently reading for his M.E.Sc. in Electrical and Computer Engineering at the University of Western Ontario.

Jagath Samarabandu (M'92) currently serves as an Associate Professor at the Department of Electrical and Computer Engineering at the University of Western Ontario.

Tarlochan Sidhu (M'90, SM'94, F'04) currently is a Professor and the Chair of the Department of Electrical and Computer Engineering at the University of Western Ontario.

Robert Beresh (M'80, SM'02) is the Service Line Leader (Protection and Control) of Kinectrics, Inc.

Jian-Cheng Tan (M'96) is the Principal Engineer, Kinectrics Interoperability Testing Lab.