SCHOOL OF COMPUTING AND INFORMATICS

NETWORK INTRUSION MONITORING AND REPORTING USING E-MAIL AND SMS (NIMRUES)

BY

KIHUHA, CYRUS KAMAU: P56/P/8344/2003

Supervisor

Andrew Mwaura Kahonge.

Submitted in partial fulfilment of the requirements of Masters of Science degree in Information Systems (IS)

March 2012

Declaration

This project is my original work and has not been presented for a degree in any other university

Student's Declaration

Signature......Kamau:.............................. Date ..16th April 2012:.........

Name: Kihuha Cyrus Kamau

Registration Number: **P56/P/8344/2003**

Supervisors Declaration

I confirm that the work reported in this project research was carried out by the candidate under my supervision as university supervisor. This research project has been submitted with my approval as university supervisor.

Signature .... Date ..27 | APR | 2012..........

Mr. Andrew Mwaura.

School of Computing and Informatics

Abstract

The fundamental problem with any security administrators today is its ability to cope with the rising amount of network intrusions. Network security is fast becoming an absolute necessity to protect the information contained on computer systems worldwide. With 40 per cent of the global economy driven by e-business, attacks on networks are becoming more frequent, more varied, and more costly.

The need for increased protection of information assets in storage, in transit, and during access has driven companies to look to vendors to provide products that ensure that their privacy is protected. The ever changing network use and operation along with the public concern for protection of sensitive information makes implementing an effective security plan a must. This includes many different pieces of software and hardware working together to provide the desired protection.

Network Intrusion Monitoring and Reporting Using Electronic mail and Short Message Service **(NIMRUES)**; an intrusion detection and monitoring system that involves capturing intrusion occurrences in Windows operating system security event log files. Once the intrusion is detected the message is captured and converted from Windows proprietary binary format to plain text format that is send to alert the security administrator through E-mail and SMS. Upon receiving this alert message the administrator will take necessary action(s) before serious negative impact is caused.

The developed **NIMRUES** prototype is based on XAMPP server which provides an integrated system of servers i.e. Mercury 32 mail server for sending E-mails, Apache web server for provision of web hosting; the web address http://localhost/nimrues.net provides an interface to access error information stored in My SQL database server by use of a web browser software. The retrieval of error messages in the back end (database) is facilitated by use of php scripting which the XAMPP server is able to parse. Java Eclipse has been used integrate SMSLib tools to send errors messages to the security administrators phone before been written to the database.

Dedication

I would like to dedicate this work to my wife Caroline who has kept me going despite difficult and tiring moments, my colleague and friend Ephantus whose wisdom and guidance have been immeasurable. This research will be applicable in several upcoming projects within the IBEA research group team.

Acknowledgement

First I give thanks to the almighty God for enabling me to finish this course and project successfully. I wish to express my sincere appreciation for the effort and dedication shown by my supervisor Mr. Andrew Mwaura, for his support, valuable advice and assistance to carry out and complete this project

The contribution of Mr. Ephantus Kinyajui and my colleagues at Kimathi University College is greatly acknowledged. Finally, thanks for the love from my dear wife, Caroline without her support; I would not have completed this research.

Table of Contents

Declaration ii
Abstract iii
Dedication iv
Acknowledgement v
Table of Contents vi
List of Figures ix
List of Diagrams x
List of abbreviated words xi

1 INTRODUCTION 1
1.0 Introduction 1
1.1 Importance of network management systems 3
1.2 Pre and Post network intrusion monitoring application/tools. 5
1.2.1 Firewalls 5
1.2.2 Intrusion Detection Systems (IDS) 6
1.2.3 Log files 10
1.3 Problem statement 12
1.4 Objectives 14
1.5 Research Questions 14
1.6 Project Justification 14

2 LITERATURE REVIEW 16
2.0 Introduction 16
2.1 Network Intrusion 17
2.2 Network Monitoring and Reporting 20
2.2.1 MonitorMagic 21
2.2.2 Net Peeker 21
2.2.3 Fireplotter 22
2.3 Generic log Adapter (GLA) 22
2.4 Short Message Service (SMS) applications and tools: 24
2.4.1 Ozeki NG - SMS System 25
2.4.2 Zozoc SMS 26
2.4.3 Mig33 27
2.5 Electronic mail applications and tools: 27
2.5.1 Thunderbird 28
2.5.2 Eudora 28
2.5.3 Lotus Notes 28

3 METHODOLOGY 30
3.0 Overview: 30
3.1 Conceptual Model 30
3.1.1 Design of the Conceptual Model 31
3.1.1.1 Client side 31
3.1.1.2 Server side 32
3.2 Research Methodology 33
3.2.1 Observation 33
3.2.2 Documents Review 35
3.3 System development methodology 37

3.3.1 The Analysis using Data Flow Diagrams 37
3.3.2 Logical Data Modelling 40
3.3.3 Flow of program Logic 42

4 RESULTS 43
4.0 Introduction 43
4.1 Log parsers implementation 43
4.1.1 Phases in log parsing: 44
4.1.2 GLA adapter conversion to XML (Extract). 47
4.2 Mobile interface implementation 48
4.2.1 Installing and Configuring the SMSLib 3.5 48
4.2.2 OutboundNotification Class 50
4.2.3 SendMessage Class (Extract) 50
4.2.4 Send SMS using Huawei Modem gateway 52
4.3 Web interface implementation 52
4.3.1 Login.php 52
4.3.2 index.html 53
4.3.3 Show.php 53
4.3.4 Contacts.php 54
4.3.5 System users.php 54
4.4 Electronic mail (E-mail) interface implementation 55
4.4.1 Microsoft outlook express (Local mail server) 55
4.4.2 Gmail and Yahoo mail (external mail Server) 55
4.5 Testing 57
4.6 Resources 57
4.7 Project schedule 58

5 DISCUSSIONS AND CONCLUSIONS 59
5.0 Introduction 59
5.1 Discussions 59
5.2 Assumptions 60
5.3 Limitations 60
5.4 Recommendations 61
5.5 Impact of Future Technologies 62
5.5.1 IP Version-6 62
5.5.2 Encryption 62
5.5.3 Wireless Technologies 62
5.6 Conclusions 63

6 REFERENCES AND BIBLIOGRAPHY 64

APPENDIX 1: DARPA 1999 EVALUATION 70
APPENDIX 2: MICROSOFT SECURITY TOOLS 71
APPENDIX 3: SECURENET PRO OVERVIEW 72
APPENDIX 4: CISCO PRODUCT LINE 74

List of Tables

Table 1: Top Management Errors that Lead to Computer Security Vulnerabilities........................2

Table 2: SANS list of Top Twenty Computer Vulnerabilities in October 2001...........................18

Table 3: Error logs Extract table..41

Table 4: Administrators information...41

Table 5: User Login account...41

Table 6: Counter...41

Table 7: Project Schedule..58

List of Figures

Figure 1: Component of a typical network management system..3

Figure 2: A LAN protected by a firewall with package filtering & proxy server...........................6

Figure 3: Technologies to implement in forensics an d post analysis of intrusion........................17

Figure 4: Ozeki NG - SMS modem connectivity for SMS messaging...26

Figure 5: Conceptual Model Design...31

Figure 6: Current System Level O DFD (Context Diagram)...37

Figure 7: Current System Level 1 DFD...38

Figure 8: New system Level O DFD...38

Figure 9: New system Level 1 DFD..39

Figure 10: New system Level 2 DFD..39

Figure 11: New system Level 3 DFD..40

Figure 12: System Flowchart..42

Figure 13: Adapter configuration file for windows log parser..46

Figure 14: Text error log file generated by the Windows log parser...47

List of Diagrams

Diagram 1: Detecting the GSM modem connection..51

Diagram 2: Successful sending of messages by the GSM modem..52

Diagram 3: Login.php...52

Diagram 4: Index.html..53

Diagram 5: Log events..53

Diagram 6: Administrator details form..54

Diagram 7: Registered system users...54

Diagram 8: Outlook express mails received from nimrues.net mail server...................................55

Diagram 9: Nimrues.net mail server relays mails to Google mail client......................................56

Diagram 10: Nimrues.net mail server relays mails to Yahoo mail client......................................56

List of abbreviated words

CBE-common base event

SMS-short message service

MIB-management information base

ATM-asynchronous transfer mode

NNTP-network news transfer protocol

URL- universal resource locator

GLA-generic log adapter

HCI-human computer interaction

ICS-Internet connection sharing

NETBIOS-Network basic input system

HTML-Hypertext Mark-up Language

PHP-Hypertext Pre-processor

IIS-Internet Information Server

IPS-Intrusion Prevention System

NFS- Notes Storage Format

GUI- Graphical User Interface

DFD-Data Flow Diagram

CCTA-Central Computer and telecommunication Agency

ERD-Entity Relationship Diagram

SQL-Structured Query Language

IDMEF - Intrusion Detection Message Exchange Format

MIT-Massachusetts Institute of Technology

AITI-Africa Information Technology Initiative

IDS-Intrusion detection system

SNMP-simple network management protocol

OpenSSL-Open secure sockets layer.

IETF- Internet Engineering Task Force.

WI-FI - Wireless Fidelity

AOL - America on Line

IBM - International Business Machines

IMAP - Internet Mail Applications Protocol

IDXP- Internet Detection Exchange Protocol

GPRS - General Packet Radio Service

VPN - Virtual Private Network

DNS -Domain Name System

XAMPP - Xml, Apache, MySQL, Php and Perl

FBI - Federal Bureau of Investigations

IDIOT- Intrusion Detection In Our Time

CGI - Common Gateway Interface

RDS - Remote Data Services

SSH - Secure Shell

TCP - Transmission Control Protocol

GPL - General Public Licence

ASCII - American Standard Code for Information Interchange

W3C - World Wide Web Consortium

LTA - Log and Trace Analyzer

NAT - Network Address Translation

WEP- Wired Equivalency Privacy

UDP - User Datagram Protocol

POP3 - Post Office Protocol 3

IMAP -Internet Message Access Protocol

DLL- Dynamic Linking Library

EAP - Extendible Authentication Protocol

ISA - Internet Security and Acceleration

AIX- Advanced Interactive and eXecutive

ASA- Adaptive Security Algorithms

ISAPI - Internet Server Application Programming Interface

RPC - Remote Procedure call

GSM - Global System for Mobiles

ICMP - Internet Control Message Protocol

Chapter 1

1 INTRODUCTION

1.0 Introduction

Most security issues focus on the connection of the corporate network to the Internet and related issues such as viruses transmitted via electronic mail and intrusion from hackers. The issue for evaluation here is the monitoring and reporting network and security threats from the outside and inside of the corporate enterprise. There are many issues for security that are still pertinent even if a company has no Internet connection (*See Appendix 1*). Network security and intrusion threats to the business today are real and require distinct attention [1].

This area of intrusion and reporting risk does not get as much attention as the typical perimeter security situation thought of when dealing with network security. When a person looks at corporate business enterprise network security the first obvious issue is firewalls. But this is only truly for perimeter protection. Shirley notes this in Network Computing magazine that "although the majority of corporate losses originate from abuse, most organizations have kept their focus on the perimeter" [2]. The reality of intrusion threats to security is not as apparent but does have impact.

A tutorial from Network Magazine depicts the internal threat quite well. "Intentional threats are also potentially damaging. Employees and outsiders pose intentional threats. Outsiders—terrorists, criminals, industrial spies, and crackers—pose the more newsworthy threats, but insiders have the decided advantage of being familiar with the network. Disgruntled employees may try to steal information, but they may also seek revenge by discrediting an employee or sabotaging a project. Employees may sell proprietary information or illegally transfer funds. Employees and outsiders may team up to penetrate the system's security and gain access to sensitive information [3]. "

In a white paper from Network General, a network security software manufacturer, the issue of network intrusion threats does show the real story. The information from Network General reveals that "recent studies estimate that 50% to 80% of intrusions originate from the inside. More disturbing is the fact that these internal attacks are the most damaging [4]."

These statistics are supported by the Federal Bureau of Investigation (FBI). Knowles noted in CIO magazine that "computer security problems involve someone inside the corporation about 90 percent of the time; FBI estimates peg the figure at 85 percent [5]." There is additional data to show that this internal threat does exist but often times a company does not report its security breaches.

A survey conducted by the System Administration, Networking, and Security (SANS) Institute shows some items that are related to this issue of internal security [6]. The survey shows the 7 Top Management Errors that Lead to Computer Security Vulnerabilities [7]. This list depicts several items affect security matters, specifically items number two, four, and five.

Number Seven:	Pretend the problem will go away if they ignore it.
Number Six:	Authorize reactive, short-term fixes so problems re-emerge rapidly
Number Five:	Fail to realize how much money their information and organizational reputations are worth.
Number Four:	Rely primarily on a firewall.
Number Three:	Fail to deal with the operational aspects of security: make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed
Number Two:	Fail to understand the relationship of information security to the business problem -- they understand physical security but do not see the consequences of poor information security.
Number One:	Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.

Table 1: Top Management Errors that Lead to Computer Security Vulnerabilities.

The damage that is caused by network intrusion can be severe and can result in a loss of revenue. Loss of corporate data or transfer of company files can have a more distinct affect on the business than a physical disaster. System downtime as a result of an intrusion can have an adverse result on the enterprise and end users.

The cost of internal network intrusion threat is tangible. Radcliff noted an excellent cost impact in an article on InfoWorld Electric [8]. "Omega Engineering learned firsthand the dangers of the disgruntled employee after a timed virus, known as a logic bomb, wiped out all of its research, development, and production programs in one fell swoop. (The tape backup also was destroyed.) In January, charges were filed against 31-year-old Timothy Lloyd, an Omega programmer, for placing the bomb on the network, which detonated 10 days after his termination. Omega's costs will likely exceed $10 million as engineers and designers rewrite designs and recode programs."

1.1 Importance of network management systems

A conventional network management system consists of two classes of components: managers and element agents [9]. The Figure 1 below depicts a simple case scenario.

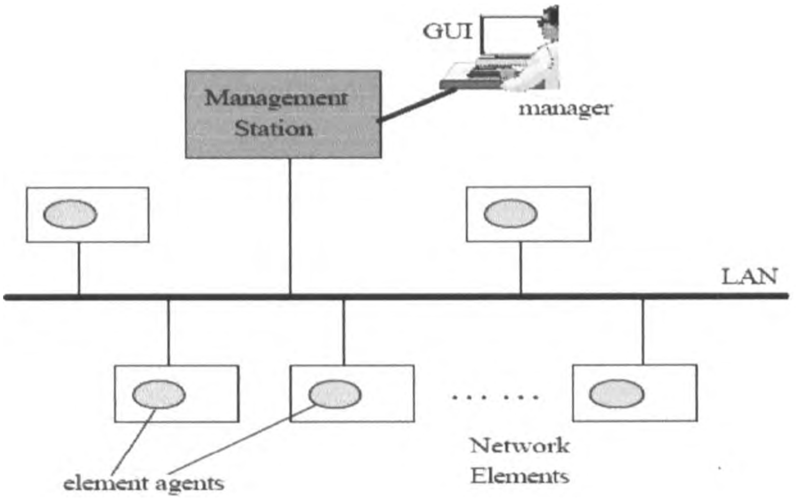


Figure 1: Components of typical Network Management Systems

In network management systems applications in the central management station assume the manager role, and execute with a GUI for human managers to perform certain monitoring functions. Element agents are server processes running in each involved manageable network entity. These agents collect device data from the network elements; it then stores it in the

Management Information Bases (MIBs), and support a management protocol, e.g., Simple Network Management Protocol (SNMP)[10]. Manager applications retrieve data from element agents by sending corresponding requests over the management protocol.

Current network monitoring/management systems favour a centralized framework where most of the monitoring intelligence and computation burdens are allocated to the manager applications executing at the central station. This results to several barriers to effective network monitoring, especially for emerging high-speed networks.

Given the centralized allocation of management responsibilities, all the monitoring interactions within the system and processes have to go through the management station which becomes the bottleneck and single point of failure.

This leads to a system that hardly scales up to large and complex networks. Since manager applications can only interact with the network elements through low-level general-purpose interfaces, any non-trivial monitoring task requires huge volume of "raw" SNMP variables being transferred to the management station, which is known as the micro-management problem. Micro-management results in high communication overheads and significant operation delays if the managed network is wireless or satellite-based.

In modern computing environments large networks are inherently distributed. This has in turn resulted to the need to share information and resources within and across computing enterprises. We therefore need a mechanism to enable the components brought together by the large networks to communicate coherently and to inter operate. Dealing with large distributed networks is a challenging endeavour. Many application programming interfaces and packages currently in existence have greatly eased the complexity of developing applications that can work with mobile technologies.

Such has been the growth of e-mail and SMS that it has been recognized that it has a potential beyond that of a means of casual communication between parties. The service is now seen as employable in situations where standard communications is not only costly, but unpractical and time consuming. E-mail and SMS are now seen as a cost-effective means of communication in areas of the information age society.

1.2 Pre and Post network intrusion monitoring application/tools.

Network Intrusions can be simply broken down into three areas: Before the Attack, During the Attack and After the Attack. It is very easy to break it down this way, but very hard to and other security research groups contend that anywhere from 50%-75% of all intrusions take place from inside your corporate "trusted" network. Additionally, if intrusions are performed for the purpose of gathering information or resource usage, rather than denial of service or defamatory purposes, the attacker will do everything in his or her power to ensure that their presence is difficult to detect. This makes it even harder to detect and trace what is happening within your network environment.

1.2.1 Firewalls

A firewall is commonly used as a pre-intrusion monitoring tool that acts as a barrier between an internal local area network (LAN) and the "outside world" – the LAN's connection to the Internet or another internetwork. However, Microsoft's ISA Server is a good example of this: While its predecessor, Microsoft Proxy Server, was not considered to be a full-fledged firewall. Another type of intermediary is a proxy server [11]. It's important for IT professionals to understand the difference between the two.

Firewall job is to use filtering to prevent unauthorized data from entering the network and restricting the data that can be sent out [12]. Just as a physical firewall in a building or vehicle is designed to stop a fire from spreading from one area to another, a network firewall is designed to keep data in or out of a network this prevents intrusion from unknown source within the public network.

The most common filtering methods are:

i). Packet filtering, which works primarily at the network layer

ii). Circuit filtering, which works at the transport layer

iii). Application filtering, which works at the application layer

Packet filters examine the information in the IP packet headers of messages and make the decision as to whether the data is allowed in (or out) based on that information. Thus packet filtering allows you to designate specific IP addresses (or host or domain names) that will be specifically blocked or specifically allowed. Filters can also process information at the transport layer (TCP and UDP port numbers). Specific ports can be blocked or left open. Because particular services use specific ports (for example, POP 3 incoming email uses port 110), this allows you to prevent specific types of data from entering the network (in this case, incoming POP3 email). There are two types of filtering, static and dynamic. With dynamic filtering, the necessary ports are opened up only when a communication is actually taking place, rather than staying open all the time. As soon as the communication ends, the port is closed.

These back doors initiate connections to an attacker that, from the firewall's perspective, seem to be coming from "inside" and are therefore allowed [13]. The reality is that back doors can allow attackers to take over control of an internal system and create considerable damage.

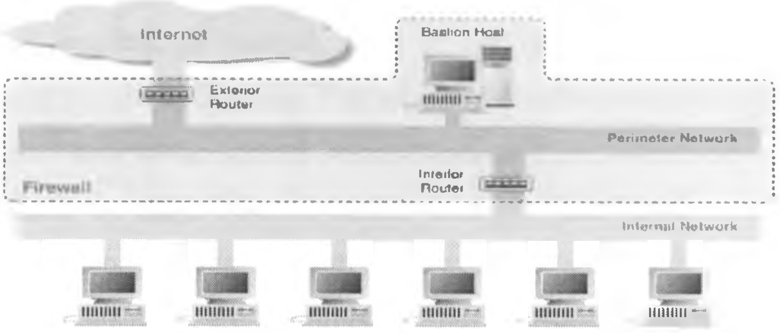


Figure 2: A LAN protected by a firewall with package filtering and proxy server

Basically, a firewall is a barrier to keep destructive forces away from your property and limits access to your computer by outside sources, and examines packets of information sent to your computer over the Internet. In fact, that's why it's called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next.

1.2.2 Intrusion Detection Systems (IDS)

An intrusion detection system (IDS) is also used as a pre-intrusion detection system that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system [14]. The importance of the IDS has grown significantly as the industry recognizes that 90 per cent of attacks in recent years have exploited application vulnerabilities. IDS, on the other hand, can expose these application layer attacks.

But detection alone is insufficient—it is also important to terminate the attack upon detection. Hence, the trend is to evolve the IDS into an Intrusion Prevention System (IPS), which takes detection to the next level and stops the detected attacks, including application attacks. In addition to the IDS/IPS, application content security arsenal in an enterprise may also include antivirus, anti-spam and content filtering devices [15].

There are three categories of intrusion detection systems, they are:-

1) *Misuse detection vs. Anomaly detection:* in misuse detection, the IDS analyses the information it gathers and compares it to large databases of attack signatures. IDS look for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.
2) *Network-based vs. Host-based systems:* in a network-based system, or NIDS, the individual packets flowing through a network are analysed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.
3) *Passive system vs. Reactive system:* in a passive system, the IDS detect a potential security breach, log the information and signal an alert. In a reactive system, the IDS respond to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

Though they both relate to network security, IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening [16]. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An ID evaluates suspected intrusion once it has taken place and signals an alarm. An ID also watches for attacks that originate from within a system. The following are the different methods used to provide firewall protection, and several of them are often used in combination depending on the configuration level.

a) *Stateful Inspection*

A technology incorporated in a firewall system that ensures that all inbound packets are the result of an outbound request. It's also called "stateful packet inspection" (SPI), it was designed to prevent harmful or unrequested packets from entering the computer. All incoming packets from that URL must pass the stateful inspection to be accepted.

b) *Network Address Translation (NAT)*

(Network Address Translation) An IETF standard that allows an organization to present itself to the Internet with far fewer IP addresses than there are nodes on its internal network [17]. The NAT technology, which is implemented in a router, firewall or PC, converts private IP addresses. When packets come back from the Internet, NAT uses the tables to perform the reverse conversion to the IP address of the client machine. NAT is also provided with Windows Internet Connection Sharing.

c) *Packet Filter*

Blocks traffic based on a specific Web address (IP address) or type of application (e-mail, ftp, Web, etc.), which is specified by port number. [18] Packet filtering is typically done in a router, which is known as a "screening router." Or bastion host. Bastion hosts are used for services such as Web site hosting, mail, DNS lookups and FTP transfer and are located on the public side of a perimeter net.

d) *Proxy Server*

A computer system or router that breaks the connection between sender and receiver, it functions as a relay between client and server, proxy servers help prevent an attacker from invading a private network and are one of several tools used to build a firewall [19]. The word proxy means "to act on behalf of another," and a proxy server acts on behalf of the user. All requests from clients to the Internet go to the proxy server first. The proxy evaluates the request, and if allowed, re-establishes it on the outbound side to the Internet. Likewise, responses from the Internet go to the proxy server to be evaluated. The proxy then relays the message to the client. Both client and server think they are communicating with one another, but, in fact, are dealing only with the proxy.

The best firewall software tool should be inexpensive and easy to install and use, should also offer clearly explained configuration options and also hide ports to make your system invisible to scans, It must also protect your system from all attacks, the tool in use should also be able to track all potential and actual threats and immediately alert you when serious attacks occur, In addition it should also ensure that no unauthorized entry occurs to your system.

Examples of common software tools include:-

i). Windows firewall.

A software component of Microsoft Windows that provides firewall services and packet filtering functions (*See Appendix 2*). It was first included in Windows XP and Windows Server 2003 [20]. It is also known as Internet Connection Firewall. Every type of network connection, whether it is wired, wireless, VPN, or even FireWire, has the firewall enabled by default. A number of additions were made to group policy, so that Windows system administrators could configure the Windows firewall product on a company-wide level configurations requirement. Windows firewall cannot block outbound connections: it is only capable of blocking inbound ones.

ii). PC Tools Firewall.

This is a powerful free personal firewall for Windows' based system that protects your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network. By monitoring applications that connect to the PC tools firewall can stop Trojans, backdoors, key loggers and other malware from damaging your computer and stealing your private information.

PC Tools Firewall is advanced technology designed especially for people, not just experts. Powerful prevention against attacks and known exploits is activated by default while experienced users can optionally create their own advanced packet filtering rules, including IPv6 support, to customize the network defences. Its backed by regular Smart Updates, real-time protection and comprehensive network shielding to ensure your PC remains safe and hacker free.

PC Tools firewall features include hiding your system from Internet hackers, fine-grained control over inbound and outbound traffic, Easy to use, designed for novice and expert users, Optional password protection for rules and settings.

iii). ZoneAlarm Firewall.

Considered an excellent tool for replacing the default Windows firewall with a stronger option that includes better outbound protection, anti-phishing guards, and behavioural detection network. Multiple new features include quieter outbound protection, behavioral detection from the Internet security suite, automatic Wi-Fi security setting activation.

1.2.3 Log files

Log files are post-intrusion detection application that records activities of interest that have occurred in a computer system. It stores messages generated by an application, system, and security of an operating system. These messages are used to track the operations performed [21]. An application is said to "log" information to the log file (hence the name "log file"). Log files are generated automatically by some applications as they work and are typically (but not always) text editable files [22]. Text editable (and therefore human readable) log files are typically generated to provide a record of what went on and are not normally used again by the application that generated them. For example, Web servers maintain log files listing every request made to the server [23]. Log files are usually plain text (ASCII) files and often have a .log extension. In Backup, a file that contains a record of the date the tapes were created and the names of files and directories successfully backed up and restored. The Performance Logs and Alerts service also creates log files.

Internet Information Services (IIS) 6.0 offers a number of ways to record the activity of your Web sites, File Transfer Protocol (FTP) sites, Network News Transfer Protocol (NNTP) service, and Simple Mail Transfer Protocol (SMTP) service and allows you to choose the log file format that works best for your environment [24]. IIS logging is designed to be more detailed than the event logging or performance monitoring features of the Windows operating systems. IIS log files can include information such as who has visited your site, what was viewed, and when the information was last viewed. You can monitor attempts to access your sites, virtual folders, or files and determine whether attempts were made to read or write to your files. IIS log file formats allow you to record events independently for any site or virtual folder. The challenge in reading log files is in the formats that they have been written in. Some contain easily parse able text lines while others are binary files with proprietary data formats.

Examples of files that are in plain text formats are:

i). NCSA

The NCSA log formats are based on NCSA httpd, and are widely accepted as a standard among HTTP server vendors [25]. NCSA common log format only contains basic HTTP access information.
The fields in NCSA common log file formats are:

host rfc931 username date: time request status code bytes

NCSA combined log format is an extension of NCSA common log file plus three optional fields: the referral field, the user_ agent field, and the cookie field.
Referrer (http://www.ibm.com in the example)
The URL which links the user to your site.

User_agent: ("Mozilla/4.05 [en] (WinNT; I)" for the example)
The web browser and platform used by the visitor to your site.

Cookies: (USERID= ckamau; IMPID=197929" for the example).

ii). W3C Extended Log Format

This log format is the one used by Microsoft IIS 4.0 and 4.5[26]. A log file in this format contains a sequence of lines containing ASCII characters. Each line may either be a directive (if it starts with #) or an entry. Entries consists of columns separated by white space.

iii). SUNTM ONE Web Server (iPlanet)

A log file in one web server (iplanet) consists of a sequence of lines containing ASCII characters. Just like in W3C formats a line may either be a directive or an entry [27].

Examples of files in binary formats are;

i). Unix wtmp file

The Unix wtmp file captures login and logout activity on a Unix box [28]. This file is important since it can be used to track a user's connection habits. All operating system programmes that read and write data to the wtmp file get the file definition from a C include file which is normally located at:-

/usr/include/utmp.h

ii). Windows Event log file.

The Windows Event Log is an important source for application status information [29]. When properly integrated with the Windows operating system, applications can report their errors to the Event log by recording an event entry into the Application log. Furthermore, details on failing operating system components and hardware can be found in the System log. On Windows 2000 or newer server operating systems, the Active Directory has its own directory and replication log. On Windows NT/2000 login and logout activity, operating system messages, security events etc are captured by the event logs [30]. The event log service doesn't log plain text files, but binary log files. One needs to make calls to the Windows Event Log API to read event logs. Therefore the format is highly proprietary.

This project therefore focuses on these proprietary formats and there conversion process to plain text format by use of the generis log adapter. However, most log files in UNIX are produced by UNIX syslog service. The UNIX syslog service generates log files in plain text formats.

1.3 Problem statement

Security administrators continually monitor systems such as servers for any events that might require their intervention. For systems security reasons, one thing that is commonly monitored on servers is network intrusion and operating system event log files. The network intrusion detection is important in order to detect security threats that arise from log in successes as a result of illegal attempts to gain entry or due to cracked passwords by use of brute force, user account lock outs, failed unauthorised attempts to access secure files and security log tampering identifying and preventing such attacks is important. In the case of log files they should be monitored since this is where applications and/or operating systems record events are recorded when they happen and this could be of interest to the security administrators.

Having to monitor this for far a collection of servers can be an enormous challenge especially when the organisation consists of many servers spread all over a distributed environment or multiple offices in a geographically dispersed area for an organisation. Some errors that occur in servers may require execution of routine steps in order to rectify possible failures or faults in critical systems situation. This can be solved by automating some of the system processes or actions by automatically running a script to correct anomalies and simultaneously activating a communication mechanism to notify the security administrator of the failure and/or success of these processes.

In majority of the vendor tools available in the market can to some extent perform these functions; however they generate too many messages that are not useful the security administrators and this becomes cumbersome to look for events of interest. In the arising situations the security administrator may miss out important and critical events hidden in the numerous messages generated in the event log files. The manual method of checking of log files is tedious and pro-active requiring the security administrator to physically examine logs. This approach is impractical especially when dealing with large-scale distributed networks.

As much as it's desirable, it is important to have a system in place to help the security administrators in pursuit of this task. The developed system has the ability to present the data and information in a way that the security administrators are alerted about critical and time sensitive system events in real time mode. In addition it allows for extensibility and growth (Open system) which is a plus for system developers and builders in that it allows developers to add and/or change components without having to change the whole design a process commonly referred to as system innovation and redesign. The design also enables the security administrators to monitor and analyse any, or at the least the most important firewall intrusion messages that would be necessary in addition alert the security administrators of any possible and potential threat to the network and systems at large.

The intrusion detection and the event log messages are relayed on a real time basis. The security administrators are subscribed for online alerts to those messages that are of interest, importance and urgency to the functional operation and security of the entire system. Information and data is first pre-processed and filtered from binary to text files before been sent to the security administrators.

. A mechanism using java eclipse has been put into place for string searching in the generated regular expression in order to filter content that will be sent to the administrators. The security administrators have set and configured different events priorities in the server which allows servers to alert them in ways that clearly indicate the importance, urgency and severity of the events.

1.4 Objectives

This project has three main objectives, namely:-

1. Identify the challenges faced by security administrators while monitoring Windows security event log files.
2. Design a system that monitors network intrusion occurrences within the Windows operating system.
3. Develop a system that will report the occurrence of Windows security log events on a real time basis.

1.5 Research Questions

1. What are the challenges faced by security administrators in monitoring Windows security event log files?
2. What design strategies can security administrators implement in detecting network intrusion in Windows security event log files?
3. What implementation and deployment tools can security administrators develop in detecting and reporting network intrusion for Windows security event log files?

1.6 Project Justification

Security administrators are usually dogged with challenges of monitoring firewalls installed in network servers, routers, domains and gateways and for events that could compromise security and integrity of data and information. Without a well-developed system in place for this function to aid them in this area some tasks and events will go unnoticed.

Most of the available solutions with vendors are rigid and focus on particular aspects of the network. Strategies and policies of reporting intrusions and security attacks that could compromise data and information in an organisation are missing in most of them, while others are lacking systems with appropriate configuration rules and ability to allow security administrators to subscribe and to receive only those events that are of interest to their work.

Majority of vendor available tools in the market allow log messages to be routed over the network which results in congestion and wastage of network bandwidth or cannot be customised and/or do not provide interfaces for extensibility for future innovations or technological changes which creates a vacuum and need develop one.

Chapter 2

2 LITERATURE REVIEW

2.0 Introduction

Intrusion attempts and attacks from the Internet are a reality. Last year a statement by representatives of a number of security companies and U.S. universities, all involved in research on computer security, highlighted several worldwide trends in the Internet and factors leading to attacks against Web sites and corporate networks. The main reasons are the availability of attack tools in the open source environment and the production of insecure software applications leading to the installation of large numbers of systems with weak security. Because servers with weak security and hardly any protection are connected to the Internet, they can be compromised and made agents or handlers in large-scale hacker attacks against corporate servers and networks. The average level of the technical competence of system administrators in companies has decreased. At the same time, the number of 'directly connected homes, schools, libraries and other venues without trained system administration and security staff has increased, allowing hackers to set up their Distributed Denial of Service clusters of masters and Trojan horse agents largely undisturbed. Because of lack of support from the international law, the hacker is often not at risk of getting caught [31].

However, the fact that a company has security policies in place and a firewall installed to protect the network from attacks from the Internet is no guarantee for security. Intrusion, Inc. claims in their white paper that 'The majority of damaging attacks on the enterprise [...] comply with the enterprise security policy. These attacks succeed by simply exploiting loopholes in the current security policy' Therefore the network and the computers exposed to the Internet need to be constantly monitored by using an Intrusion Detection System [32].

Literature review is divided into the following sections:

1. Network Intrusion.
2. Network Monitoring and Reporting
3. Generic Log Adapter (GLA)
4. Short Message Service (SMS) applications and tools.
5. Electronic Mail (e-mail) applications and tools

2.1 Network Intrusion

Most corporations start by employing a number of security measures such as firewalls and network-based intrusion detection systems (IDS). There are also tools to help 'During an Attack' such as host-based intrusion detection. Finally, companies will use a myriad of tools to help with forensics and post analysis of intrusions. The figure below, it outlines where certain technologies can help in the three phases of an attack.

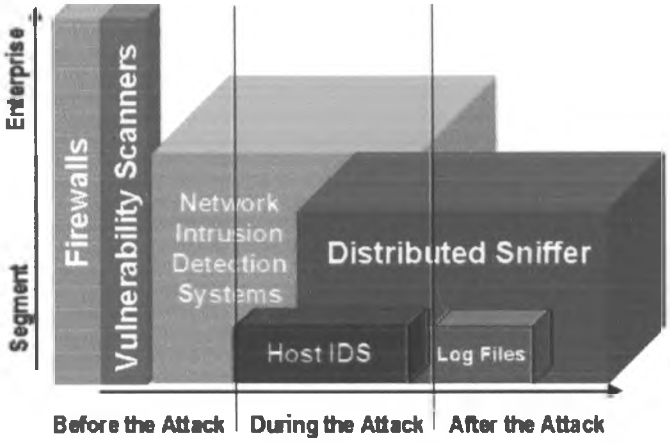


Figure 3: Technologies to implement in forensics and post analysis of intrusion.

The SANS Institute in conjunction with the FBI has published the Top Twenty Computer Vulnerabilities in October of 2001[33]. (see table below) a list of tool categories that will help with detection and visibility of the most popular network intrusions (SANS list) and what companies use each for their networks.

Type of Attack	Firewall	Network IDS	Host IDS	Vulnerability Assessment
Default installs of operating systems and applications				X
Accounts with No Passwords or Weak Passwords				X
Non-existent or Incomplete Backups				
Large number of open ports	X	X		X
Non-existent or incomplete logging				
Vulnerable CGI Programs		X		X
Unicode Vulnerability (Web Server Folder Traversal)		X	X	X

ISAPI Extension Buffer Overflows				
IIS RDS exploit (Microsoft Remote Data Services)				
NETBIOS – unprotected Windows networking shares				X
Information leakage via null session connections				
Weak hashing in SAM (LM hash)				
Buffer Overflows in RPC Services		X		X
Sendmail Vulnerabilities				X
Bind Weaknesses				X
R Commands (Rlogon, rsh, rcp)	X	X	X	X
LPD (remote print protocol daemon)	X			X
Sadmind and mountd				X
Default SNMP Strings				X
Not filtering packets for correct incoming and outgoing addresses	X			

Table 2: SANS list of Top Twenty Computer Vulnerabilities in October 2001.

i) Before the Attack

Most companies work very hard to take pro-active steps to prevent network intrusions, but they still happen and they still cause a lot of damage. However, if an adversary spends enough investigatory time and has the appropriate technical knowledge, they could get in if they are willing to work hard enough. As previously stated most network intrusions happen from inside the trusted network, completely bypassing the firewall. Most companies utilize a network based intrusion detection system, which is a distributed probe that monitors internal network segments and looks for unauthorized traffic or requests. "Intrusion detection" is a type of network security that, as the name implies, detects, identifies and isolates attempts to "intrude" or make inappropriate, unauthorized use of computers [34]. Attacks originate either via an external network connection or from within the confines of the organization that is targeted for attack [35]. Targeted systems are usually server or workstation systems; however attackers may also focus on network devices such as hubs, routers and switches.

A network intrusion detection system (NIDS) helps identify the fact that attacks may be occurring [36]. It is designed to detect, monitor, and log potential security breaches. Current network IDS products use a predominantly passive approach to collecting data via protocol analysis garnered by watching traffic on the network. Each one monitors the traffic on specific network segments. It gets copies of its segment's traffic to inspect by "listening in promiscuous mode" and having its network interface card bring in a copy of every packet it sees. It examines these packets, and attempts to determine whether they represent an intrusion attempt by comparing it to a list of known attack signatures. It does this by determining if the contents of the packet contain the signature of a known attack method, that is, whether it contains a string of characters that matches a specified pattern, or otherwise fits rules that define known attack methods.

While a network intrusion detection system is beneficial and recommended, it is not fool proof and you should not be lulled into a false sense of security (*See Appendix 3*). There are known published techniques on ways of bypassing NIDS systems (Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, which many experienced hackers both internal and external can take advantage of [37]. Furthermore, there are no NIDS products that are flexible enough to fully address the high speeds and vastly distributed nature of modern topologies present in most large networks today.

ii) During an Attack

When someone is trying to attack or penetrate your network, it is commonly understood that they are trying the following: accessing data that is not for public consumption, trying to change or deface company information (websites, files, etc.), illegally using your server memory for their own storage, and attempting to flood a particular device rendering it unusable to the authorized users thereby creating a denial of service attack [38].

There are many tools to help network administrators determine if their company is under attack. Host based intrusion detection systems are a great tool to deploy to critical servers to help identify when you are under attack [39]. They sit on hosts that a company would like to protect and will send off alerts if an unauthorized user try to access something that is restricted. That helps protect against accessing data or changing critical information on particular servers that are not for public consumption. The main shortfall with host based intrusion detection is the limited platform coverage.

Another common attack that can cause serious downtime is a Denial of Service attack. This attack looks to send a tremendous amount of traffic via bogus server requests to your critical servers [40]. Your machine becomes overburdened and will be unable to respond to normal requests. This is a very common attack to websites or key file servers. If your machine is compromised, your machine's resources can be used in a Denial of Service attack for another target unbeknownst to you. This results in numerous companies wasting a tremendous amount of man-hours searching and identifying malicious code.

iii) After the Attack

Attacks on your network will happen. The question is whether you will know about it, and after analysis, be able to understand what happened and how to fix it so that it does not happen again. If an attack on your network occurs, it is essential to do everything possible to ensure that it can be detected, and the traffic can be captured and analysed. In the April 2001 edition of Secure Computing, the complexity of this issue is detailed [41].

"Once a crime occurs, analysing the evidence, closing any holes that have been opened and perhaps even moving forward with civil or criminal litigation is a complex process - one that demands more than just a once-over by an IT administrator [42]." After you identify that you are under attack or have been attacked, you cannot go back and collect the necessary raw network traffic to piece together what happened. The only avenue at this point is to access log files of the critical machines hit in the attack, provided you had the highest detailed logging turned on [43]. Even with this information, you could still be missing critical data. It is like trying to complete a jigsaw puzzle without knowing the number of pieces available and how many you are missing. You may not be able to understand what the picture even looks like.

The ability to filter on a specific device or traffic pattern will help to quickly identify important data to begin tracing what the intruder attempted or accomplished [44].

2.2 Network Monitoring and Reporting

The monitoring and reporting mechanism aimed at monitoring network intrusion detection and reporting. This section will highlight a few tools. Tools are employed in different aspects of a computing set up. Network monitoring tools are for example, used to identify problems, quantify expected performance and to set against expected levels of service in a computer network. Most monitoring tools are employed to monitor specific aspects and behavioural activities of both systems and networks. For this main reason is evidently enough to explain why most systems and network administrators usually employ more than one monitoring tool. In order to get a fuller picture of a computing set up Examples of tools used in monitoring networks are:-

2.2.1 MonitorMagic

The MonitorMagic is an event log monitor is used to check the occurrence of certain events generated on a computer. MonitorMagic uses an event log monitor for each event log a systems and /or network administrator would want to evaluate the events from [45]. A Systems and network administrator can monitor all event logs of a computer, a selection of event logs, or a single event log.

MonitorMagic can access both local and remote Windows Event logs and scan its contents. Every event entry has its own source, ID, severity and description, which can be used to detect possible incidents. MonitorMagic can be triggered to alert on every event property or attribute and take action when necessary. Example: The tool can be used to monitor the security event logs on all your critical Windows 2003 servers. When a failed security audit event occurs then the MonitorMagic event log manager can send the systems and/or network administrator an email with the description of the event.

2.2.2 Net Peeker

A common distributed network traffic monitoring tool. Net peeker displays real time network traffic speed for each and every computer and all active network application on any computer in network. In addition it display application properties and loaded modules. Support "Internet Connection Sharing (ICS)", and can monitor network usage of ICS clients without installing agents on the clients. The net peeker can monitor NETBIOS file transfer, which is a local network shared file copying. It uses "WHOIS" service to get detail information on remote IP address and domain names. Other additional features of net peeker are integrated system firewall and application firewall on all computers.

Net Peeker can also generate log data and information for each session, this includes start/stop time, application, remote address/port, total transferred bytes and average speed. This enables it to generate network traffic statistics report and display the period which network usage for each application and each remote IP and Compact log information storage for each agent. In order to save disk space it implements a support archive on the fly, to archive log files from remote agents saved in .ZIP format and further load archived log files without uncompressing the archive a great advantage is that the loaded archives can be exported in text format.

2.2.3 Fireplotter

FirePlotter is a real-time session monitor that monitors your firewall. It simply shows you the traffic that is flowing through your internet connection moment to moment and in real-time. FirePlotter can also be described as a firewall visualization tool, or a bandwidth analyzer or a connection monitor that has been adopted by Cisco ASA/PIX firewall *(see appendix 4)* or FortiGate firewall systems and technologies. One of its main advantages is that it can replay all the session data it collects to either confirm or reject the occurrence of a past intrusion detection.

The benefits associated with FirePlotter include: bandwidth efficiently monitoring which reduces costs, increasing productivity, reducing liability and can deliver critical insight into firewall activity processes. It can also aids security administrators to discover hacker attacks, virus attacks and security breaches. It can also help to detect inappropriate internet usage by employees, bandwidth utilization, protocol and web usage. A major plus as monitoring tool property is that it is embedded with a “What tool” which is used to find out who or what is using my bandwidth.

2.3 Generic log Adapter (GLA)

The Generic Log Adapter allows you to process application log files and transform their contents into the Common Base Event format [46]. The Common Base Event specification prescribes a common format for logging, management, problem determination, and autonomic computing. It provides a consistent format that facilitates intercommunication between tools that support these goals. Common Base Event objects allow you to develop a common prescriptive event in a consistent format so that tools can be developed to support these goals.

In order to take advantage of tools such as the Log and Trace Analyser that support Common Base Event objects, your application log files need to conform to the Common Base Event format. To produce application log records that conform, you can do one of the following:

i) Change the application that generates the log file to create Common Base Event records directly.

ii) Write a transform that converts application log files to Common Base Event records.

The first approach is impractical unless the application is currently being developed. This approach does not solve the problem of integrating existing application logs with the Common Base Event format.

The second approach is more practical. However, it leaves you with the tedious task of writing the transform [47]. Typically, this is accomplished by either writing some custom code in either a third-generation programming language or a script that can be used by established scripting tools such as Perl. Once the transform is created, you must test the transform and integrate the transform solution into the tools that use Common Base Event objects.

The Generic Log Adapter simplifies the adoption of the Common Base Event format. The Adapter Configuration Editor and the runtime are components provided by the Generic Log Adapter that will help you create and test transforms quickly [48]. The editor allows you to write the transforms using Java or script fragments using regular expressions (such as Perl) to describe the mapping of log file content to Common Base Event attributes. You can also test your script fragments as you write the regular expression scripts in the editor. The runtime takes as inputs the rules that you have written and your log file and produces Common Base Event objects as outputs.

2.4 Short Message Service (SMS) applications and tools:

In the evolving and emerging world of technologies that involves the use Electronic mail (E-mail) and Short Message Service (SMS) the technology driven software prototypes is becoming a globally recognized ability to send and receive images, video and alphanumerical messages to and from a cellular devices or computer terminals. The SMS technology was developed along with the European standard for digital communications. Global System for Mobiles (GSM), the first application that involved the use short message is believed to have been sent in December 1992 from a Personal and Computer (PC) to a mobile phone on the Vodaphone GSM network in the UK (GSM Association) [49]. Messages are limited to 140 octets or 160 characters of the GSM default alphabet and, according to Rao, Chang and Lin, have the advantage that: "GSM SMS provides a connectionless transfer of messages with low-capacity and low-time performance [50]". According to a new report from Business Monitor International, mobile phone penetration in Kenya and Tanzania will surpass the 100% mark by the year 2013 [51]. The report also predicts a higher than 90% penetration for Uganda at the end of the same period.

The report, entitled [52] "East and Southern Africa Telecommunications Report Q1 2009" upwardly adjusted their forecast from previous versions due to the huge uptake of cellular telephony in these countries over the last survey period. However, the report revised its mobile subscriber forecast downwards for Angola, Mozambique and Sudan, citing lack of competition in the mobile service provider markets in these countries. Botswana and Mauritius, which already has high mobile penetration rates, were expected to show slow growth in the mobile sector.

Indeed messages require data rates as low as 2.4 kb/s, and can be transported even by older cellular networks. Messages therefore are delivered virtually anywhere in the world, within seconds of being sent. Use of mobile phones in E-mails and SMS's have established themselves as essential revenue components of the mobile communications industry, and have been put to use in many forms and innovative schemes. Indeed Vodafone, the UK's largest mobile carrier report that SMS now accounts for up to 9 percent of revenues and 20 percent of profits.

The SMS service was first used as an alert mechanism for voicemail messages received on mobile phones, but has since been popularized by teenagers as a cheaper alternative to actual mobile calls. Since its early years the popularity of SMS has spiralled upwards at an exceptional rate, and subsequently has been adapted to a diverse variety of uses [53]. These include both business and leisure. SMS can be a cost-effective way of contacting groups such as employees, students, or subscribers. Likewise it may be used for advertising, or providing information updates to sport or entertainment followers.

The network intrusion monitoring systems that use workstations and mobile devices will primarily involve a platform that supports E-mail and Short Message Service (SMS) [54]. The messages can comprise of alphanumeric combination. Message lengths vary according to network provider, usually between 100 and 256 characters. For SMS messages can be delivered at any time, regardless of whether data or voice calls are in progress. In Kenya, SMS messaging has been popular with the young teenagers for some time and is slowly gaining popularity with all age groups.

“Text messaging is continuing to rise in popularity and diversity", comments Mike Short, Chairman of the Mobile Data Association [55]. "As well as person to person text messaging we are seeing interactive text as a popular communication tool.

2.4.1 Ozeki NG - SMS System

For commercial systems that can send and receive fewer than 15 000 SMS messages per day, its advisable to use a suitable GSM device (phone or modem) attached to your computer with a phone-to-PC data cable. The GSM device has to be equipped with a SIM card that charges (preferably) low rates for SMS messages.

With this setup you can use a computer program such as Ozeki NG - SMS Gateway to send and receive SMS messages. In this case, the software uses the attached device to communicate with the GSM network. If a message is sent out by the gateway running on the computer, it is first sent to the attached GSM device. Then the GSM device transmits it to the SMS Center (SMSC) of the GSM service provider, using a wireless link (Figure 4).

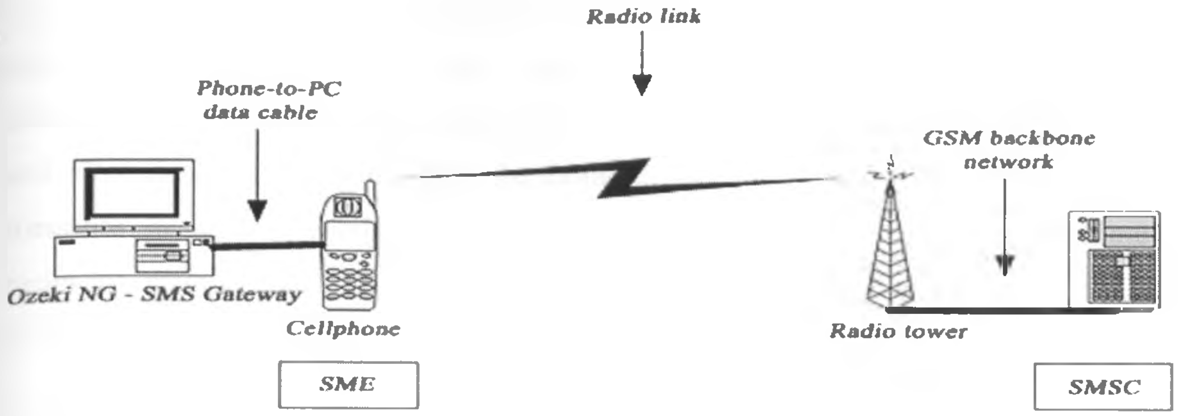


Figure 4: Ozeki NG - SMS modem connectivity for SMS messaging

When a message is received, the GSM device stores the message in its memory or on the SIM card, and sends a notification to Ozeki NG - SMS Gateway. When the program receives this notification, it retrieves (reads) the message from the respective memory cell, and then deletes the message from the device to make room for the next incoming message.

The advantage of using a cellular modem is that you do not need Internet connection for SMS messaging. Sending an SMS message using a cellphone takes about 5-6 seconds. Receiving takes about the same time. Good software, such as Ozeki NG - SMS Gateway allows you to attach more than one device to your PC and to use them simultaneously to increase capacity. The best option to connect a phone to the PC is to use a standard RS232 serial cable. USB cables, InfraRed and BlueTooth connections are not as reliable.

2.4.2 Zozoc SMS

Zozoc is a simple to use mobile Application developed with the aim of reducing your SMS costs. Zozoc leverages the internet connection of your mobile (GPRS/Wi-Fi) to send and receive SMS, so you don't have to pay your operator hefty SMS costs or log onto websites on your PC.Zozoc 'Smart' versions for Symbian and Windows mobile versions are always on, seamlessly integrated with the default phone's inbox and phonebook. Send and receive messages directly from your inbox with an ability to add contacts from your existing phonebook.

In addition it has enhanced Pop-up delivery reports for all In and Out SMSe, Application shortcut in applications folder, Auto Start on Phone boot up option, New Improved User Interface, Work Offline Mode, Enhanced messaging Functionality with T9 and copy paste and more. Improvements made on the front to save messages to draft, sending pending messages in outbox, sending messages to contacts from phonebook, adding multiple recipients manually and Overall improved account management features and application performance

Special features:

- **Over 140 countries supported:**

  Now communicate freely with your contacts around the globe since it works in over 140 countries . No need to pay your carrier hefty international SMS charges.
- **No character Limits:**

  Now write as much as you want – No half limits to your message lengths. 80 or 500 characters, we will deliver your message without failing.

2.4.3 Mig33

Mig33 is the world's largest "mobile-first" community. It is the place where millions go on their phones, to stay in touch with friends, make new friends, share photos, and more. Exciting chat/sms messenger application supporting many features, it has a vibrant mobile community that enables users to connect with friends, meet new people, exchange emoticon expressions and send virtual gifts. It also connects members to other instant messengers like Yahoo Messenger, Google Talk, MSN Messenger and AOL. The service is available to any mobile phone user and is optimized to work with more than 2,000 handsets that include most Nokia, Sony Ericsson and Blackberry handsets.

It has great value rates for making phone calls and sending SMS, especially to international countries. You can call and text to over 100 countries.

2.5 Electronic mail applications and tools:

Email clients are programs intended to access remote mail servers and retrieve mail from them. Email clients allow also composing and sending email messages. Email client is a perfect solution for dial-up connection, since the messages can be viewed without an Internet connection. But there are much more email clients that are worth mentioning. Web based email clients gained great popularity among the Internet users.

The main disadvantage of the web-based mail is that is the lack of offline capability. Such popular email programs as Outlook Express, Mulberry, or Eudora are commonly used by the majority of users. Depending on your flexibility you can install and configure an email client that works fine with your applications.

2.5.1 Thunderbird

Thunderbird is a powerful email program intended to help Internet users better manage their inbox. Thunderbird offers a great number of handy ways of displaying, managing and organizing and your folders. The folders can be displayed by recently viewed, favorites, or folders with unread messages. Besides, it allows you to tag messages with marks such as "Done" or "To Do" as well as create your own tags that are specific to your needs. Thunderbird works on Windows 95 and higher and XP, on Mac OS X, OS/2, Linux, and Solaris.

2.5.2 Eudora

Eudora is an email program that uses the POP as well as IMAP protocols. This email application runs on both the Mac and PC. A freeware package, Eudora Light, is also available. It allows to easily import mails, addresses and attachments from Outlook to Eudora, making switching to Eudora easier than ever. Eudora does not allow anything to run from the email messages, stopping Trojans and viruses. Eudora warns users about potentially dangerous content in emails.

2.5.3 Lotus Notes

Lotus Notes is the client side of a client–server, collaborative application originally created by Lotus Development Corp. in 1989. In 1995 Lotus was acquired by IBM and became known as the Lotus Development division of IBM and is now part of the IBM Software

Group. IBM describes the software as an "integrated desktop client option for accessing business e-mail, calendars and applications on [an] IBM Lotus Domino server" Prior to release 4.5, the term Lotus Notes referred to both the client and server applications.

The Lotus Notes framework provides applications with functionality to access, store & present information through a user-interface, enforce security and replicate (that is, allow many different servers to contain the same information and have many users work with that data). Although Lotus Notes may access relational databases (usually through an additional server called a Lotus Enterprise Integration server) Notes' standard storage mechanism is a document database format, the Notes Storage Format or NSF.

As Lotus Notes is an application runtime environment, email and calendaring is an application within Lotus Notes, albeit one that IBM provides with the product, but one that can be changed or completely replaced by a Domino application developer.

Applications for Lotus Notes are developed in a variety of development languages including a Visual Basic-like language called Lotus Script, and Java. Applications may be developed to run within the Lotus Notes application runtime environment and/or through a web server for use in a web browser, although the application interface would need to be developed separately for each. IBM is attempting to resolve this with a new development solution called xPages, where the application is consistently displayed using web-technologies but this is still an immature technology.

Chapter 3

3 METHODOLOGY

3.0 Overview:

The fact finding techniques and the requirements determination played a critical part in the in the selection of the system requirements determination. This process helps in determining the best and most appropriate method that can be applied for this project case scenario

3.1 Conceptual Model

The conceptual model for the network intrusion monitoring and reporting has been developed using GLA Windows event generated messages which relayed by use of Mercury mail and SMSLib Short Message Service (SMS). This proposed project is concerned with the role of network security intrusion reporting by implementing an intrusion mechanism that involves network monitoring and reporting. The project will involve the design, development and implementation of java, SMSLib, and XAMPP web based solution prototype.

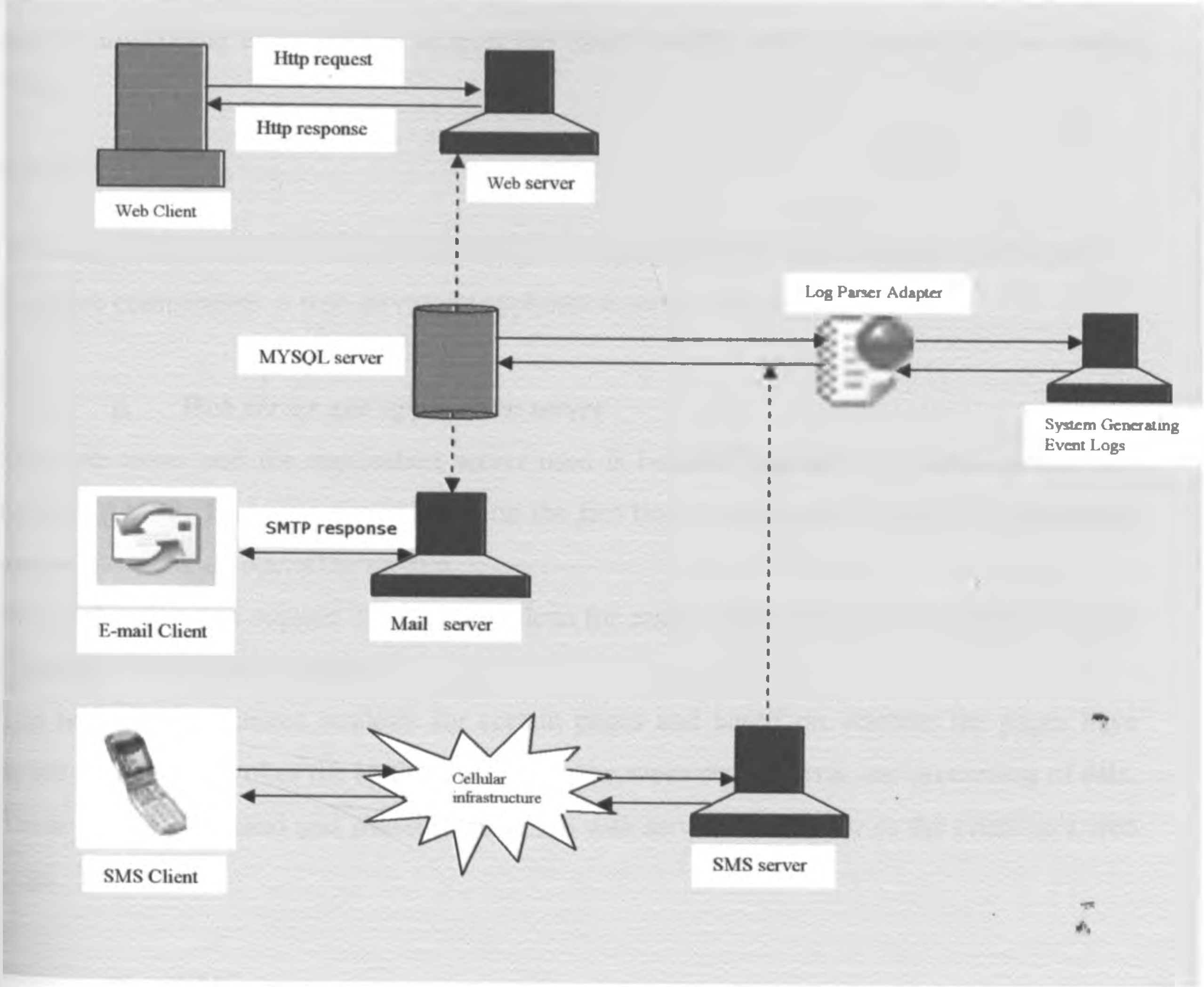
Available tools in the market today fall victim of lack of support to heterogeneous interoperable tools. However some software tools today are integrated to support multiple platforms an example of such tool is the XAMPP which is a utility pack for servers that includes Apache, MySQL, PHP and Perl. It's an open-code, multi-platform pack. Setting up a web server on Apache that connects to MySQL databases and interprets dynamic pages in PHP and Perl is not an easy task; it requires a high number of configurations and you need to compile the packs separately, this include modules for PHP, MySQL and Perl support, among other more technical complications. It is an open-code utility that lets you set up a web server easily and in a few steps.

However, the pack makes the job much easier. In addition it includes security and management modules like OpenSSL and phpMyAdmin to manage MySQL databases. In summary XAMPP is an extremely useful pack for web developers. In this project it will be used to create a local web server with the address http://localhost/nimrues.net for end user display of the results of the parsed data. However, this local web server can be accessible to everyone over the Internet if hosted on a public domain.

3.1.1 Design of the Conceptual Model

The system conceptual model can be split into three modules parts; the client side; the server side and the database or SQL server. Each part is captured in the figure 5 below.

Figure 5: Conceptual model design.



3.1.1.1 Client side

The system is accessed through two clients, the web client, the SMS client.

i). Web client

This can be any web browser that supports JavaScript; for instance Mozilla Fire fox and internet explorer. Any computer that has one of this client software can be used to run the web based module which consists of web pages written in HTML and JavaScript and php.

ii). SMS client

This can be any MPSP whose network supports SMS. Any mobile phone with access to such a network can be used. The cloud is used to represent the cellular infrastructure which is central to any system.

The SMS may in some cases such as payment require specific format but the system does not require any coding to be done to support this client module since its responsible for sending SMS.

3.1.1.2 Server side

This section will contain the application logic that processes the request made via clients. It has three components: a web server, an application server and an SMS server.

i). Web server and application server

The web server and the application server used is bundled together in an open source tool called XAMPP. This choice was based on the fact that it works well with both Linux based and windows based operating system.

This web server has support for PHP functions for easier interaction with the MySQL server (Database Management system).

The web server receives requests for certain pages and based on whether the pages have dynamic content invokes the application server for necessary retrieval and processing of data. These data is processed and passed over to the web server for transfer to the client in a web page.

ii). SMS server

The MIT AITI SMS server is modified to service the SMS clients. It does so by communicating with the SQL server for information retrieval and data storage.

The server has a module that handles requests from the mobile phone client; the modem in use is the HUAWEI E173 model.

Methodology applied has been implemented in two ways:

3.2 Research Methodology

With respect to requirements analysis, the following methods were used in collecting facts about the system for the purpose of analysis:

3.2.1 Observation

Observation is way of gathering data by watching behaviour, events, or noting physical characteristics in their natural setting. Observations can be overt (everyone knows they are being observed) or covert (no one knows they are being observed and the observer is concealed) [56]. The benefit of covert observation is that people are more likely to behave naturally if they do not know they are being observed. However, you will typically need to conduct overt observations because of ethical problems related to concealing your observation. Observation of the system, network and security administrators work environment which provided details on how they collect information about network monitoring.

The observations were conducted through the use of a guided structured protocol . The protocol involved the use of a request form for capturing narrative describing events that occurred to the system as observed by security administrators. The use of the protocol regarding this project helped to ensure that the observation process of gathering the pertinent information and, with appropriate application of the necessary skills, using the same criteria in the evaluation processes.

The protocol use went beyond recording of computer users and security administrator's behaviours, activities or events, i.e., use of identified materials, and provide an overall context for the data. The protocol prompted me to:-

i) **Describe the setting** of program delivery, i.e., where the observation took place and what the physical setting was like;
ii) **Identify the people** who participated in those activities, i.e., characteristics of those who were present;

iii) **Describe the content of the intervention,** i.e., actual activities and messages that were delivered;

iv) **Document the interactions** between security administrators and system users;

v) **Describe and assess** the quality of the delivery of the intervention; and

vi) **Be alert to** unanticipated events that might require refocusing one or more evaluation procedures involved in monitoring and reporting of security error occurrences.

The following information was gathered during the observation process:

a) The **setting:** - The physical environment within which the security administrators conducted their network and system monitoring duties. The server room observation noted several points of interest one of which is that this is a physical location and the administrators were always mobile due to the nature of their functions which is an inhabitant for effective and efficient service delivery.

b) The **human, social environment** - The ways in which all actors (staff, participants, others) interacted and behaved towards each other. The presence of a help desk did not assist much as most of the system error events that occur require the direct and sometimes immediate presence of the security administrators to solve the issues at hand

c) **Error occurrence reporting mechanism** - What goes on in the work life of the security administrator? What do various actors (staff, participants, others) actually do? How error occurrences either in servers or clients reach the technical team? Users call the extension line either for the administrators or the help desk. Due to their high mobility to serve clients technical issues the calls may not reach them for help thus easier to reach them by SMS notification.

d) The **technical language of reporting failure occurrences** - Different organizations and agencies have their own ICT technical language or jargon to describe the problems they deal with in their computing environments. Capturing the precise technical terms of all participants is an important way to record how staff and users understand their experiences.

e) **Non-verbal communication** - Nonverbal cues about what is happening in the network monitoring and reporting activities on the way all users report failures occurrences, express their opinions, physically space themselves during discussions, and arrange themselves in their physical setting.

f) **Notable non-occurrences** – Determined what was not occurring although the expectation is that it should be occurring as planned in the network monitoring and reporting processes, or noting the absence of some particular activity/factor that is noteworthy and would serve as added information in the observation of both administrators and their behaviours/activities.

This provided an understanding of how error messages are generated by the Windows operating system and how the generated messages are reported to administrator for action.

3.2.2 Documents Review

Study of the documents used in the current system. This provided an understanding of how the system stores generated log files and how the security administrators this information and the available interfaces for data processing.

Existing records often provide insights into a setting and/or group of people that cannot be observed or noted in another way. This information can be found in document form. Lincoln and Guba defined a document as "any written or recorded material" prepared for the purposes of the evaluation or at the request of the inquirer [57]. Documents review in this project has been divided into two major categories: public records and personal documents:-

a) Public records:

Materials created and kept for the purpose of "attesting to an event or providing an accounting" [57]. Public records can be collected from outside (external) or within (internal) the setting in which the evaluation is taking place. The following records were useful in this data gathering process of this project.

Application, system and security error log reports generated by windows operating system, which were helpful in determining what common failure occurrences not only prominent but also iterative which ultimately led to graceful system faults. This assisted me greatly in gathering information about a collection of multiple correlative clusters of system behaviours and relevant trends. This error log files were helpful in gaining better understanding in the modelling process of the project objectives on understanding the challenges faced by security administrators and making comparisons between computer users and their needs.

The existing documentation contained descriptions of operating system and network configuration processes. These documents were particularly useful in describing institutional characteristics, such as backgrounds and security administration policies and procedures, and in identifying computing and ICT application and tools usage strengths and weaknesses. They played a crucial role in understanding the institution's resources, values, processes, priorities, and concerns. Furthermore, they provided a record or history not subject to recall bias.

b) Personal documents:

Documents that provide first-hand accounts of events and experiences these "documents of life" include diaries, portfolios, photographs, artwork, schedules, scrapbooks, poetry, letters to the paper, etc. Personal documents helped me understand how the security administrator's sees the world and how they interact with the system during the monitoring and reporting of failures occurring in the system. From a personal perspective, unlike other sources of qualitative data, collecting data from personal documents provided a virtual platform which is relatively invisible to, and requires minimal cooperation from the security administrators and other users of the system with the setting being studied from [58].

The usefulness of existing sources varied this was based on whether they were accessible and accurate. In this monitoring and evaluating project, documents availed provided me with useful information about the culture of the ICT department under study and security administrators involved in the project, which in turn can assisted in the development of evaluation questions on the monitoring and reporting processes. Information gathered and extracted from the documents was also used to generate critical information gaps and/or to identify events to be observed. Furthermore, existing records were useful for making comparisons (e.g., comparing all administrators to security administrators, project proposal to project implementation, or documentation of institutional policies and program descriptions prior to and following implementation of monitoring and reporting project interventions and activities).

In the current system, as mentioned in problem definition, the security administrator has to rely on third party tools which that need to execute process that are resource and memory intensive while others that are available in the market are commercial and do not support mobile technology.

3.3 System development methodology

The Structured Systems Analysis and Design Method (SSADM) were used as the development methodology for this project. SSADM is a waterfall based method used in the analysis and design of information systems. It was developed by the Central Computer and Telecommunications Agency (CCTA) in United Kingdom. The most important techniques of SSADM that were used in this project are:

3.3.1 The Analysis using Data Flow Diagrams

This stage employs data flow modelling in analysing the current system. It involves identifying, modelling and documenting how data moves around the network monitoring and reporting system.

In it; processes - which are activities that transform data from one form to another-, data stores-which are the holding areas for data-, external entities –which send data into the network monitoring system or receive data from the databases or files, and data flows-which identify the route by which data flows-are examined. The end results of this technique are the Data Flow Diagrams (DFDs) shown below:

Current System DFD

Figure 6: Current System Level O DFD (Context Diagram)

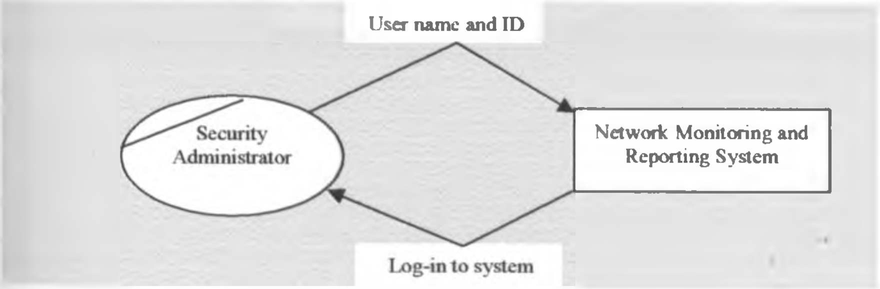
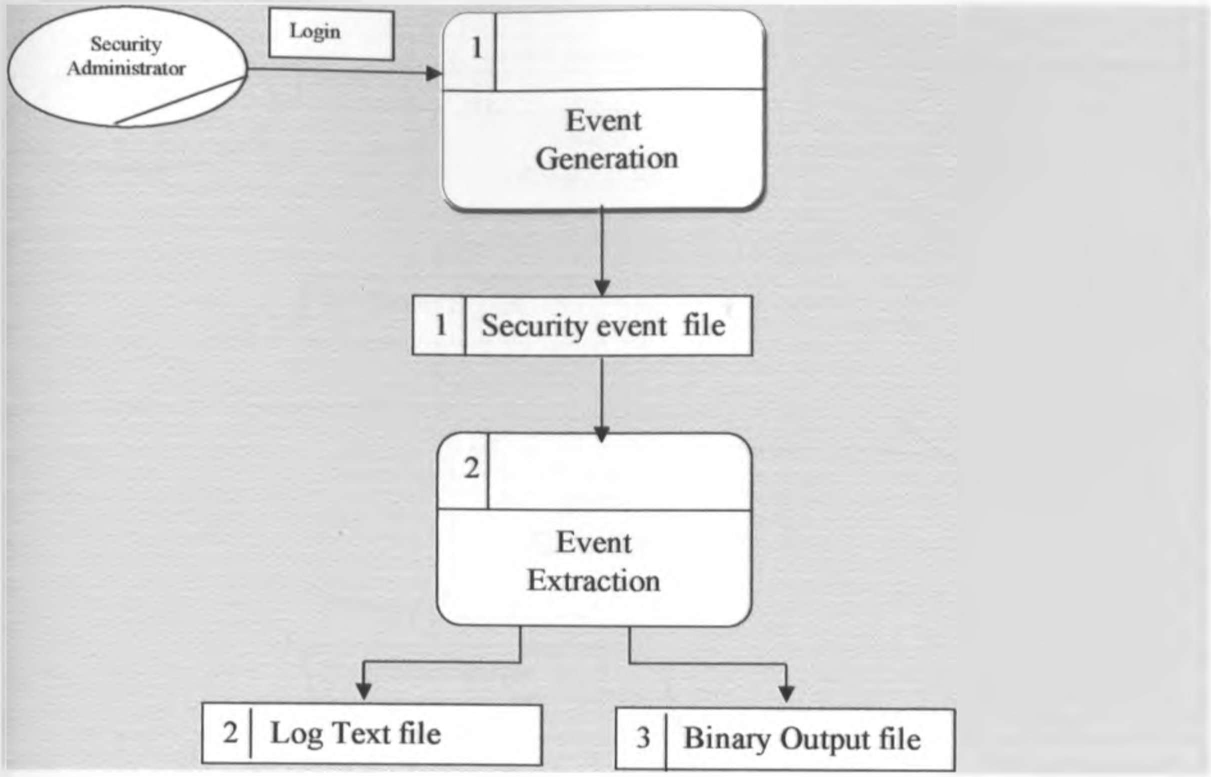


Figure 7: Current System Level 1 DFD



New system DFD

One of the major differences between the current and the new system captured by the DFD is the ability of the system to report to the security administrator using Eletronic mail or short messaging service.

Figure 8: New system Level O DFD

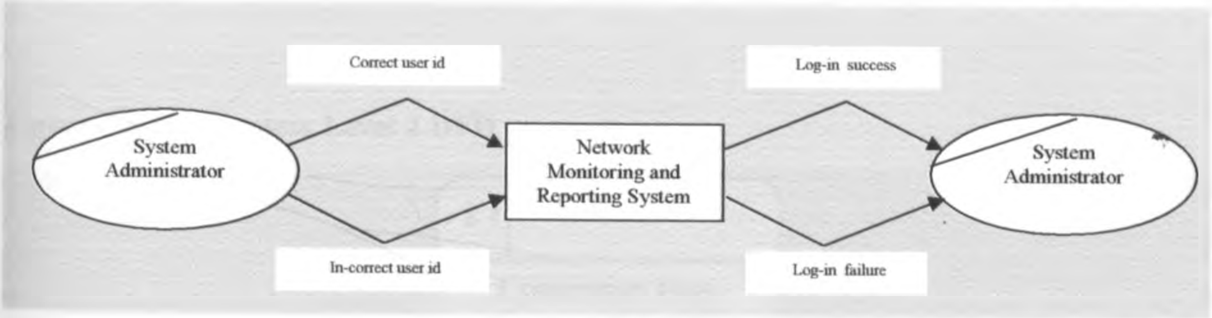


Figure 9: New system Level 1 DFD

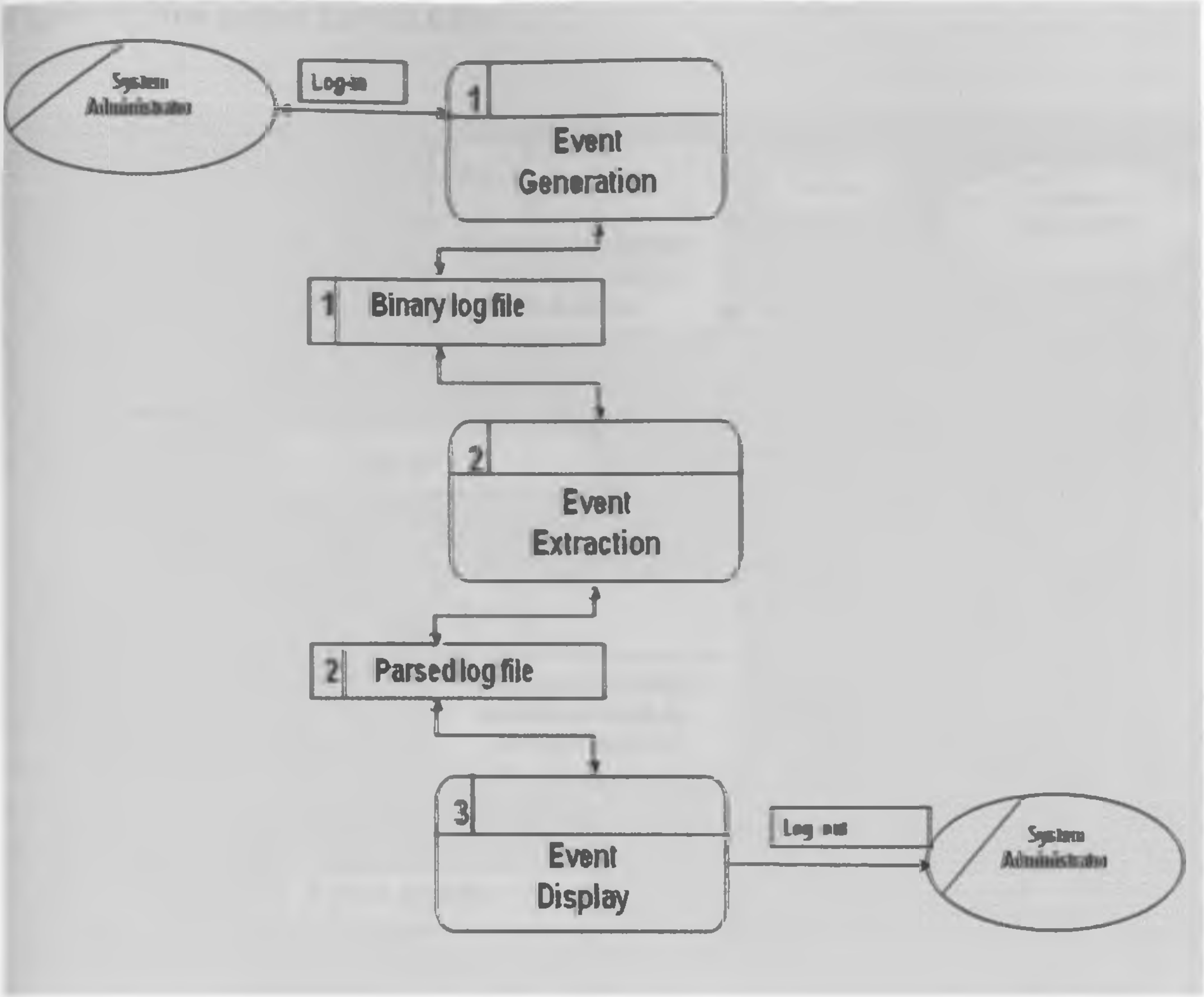


Figure 10: New system Level 2 DFD

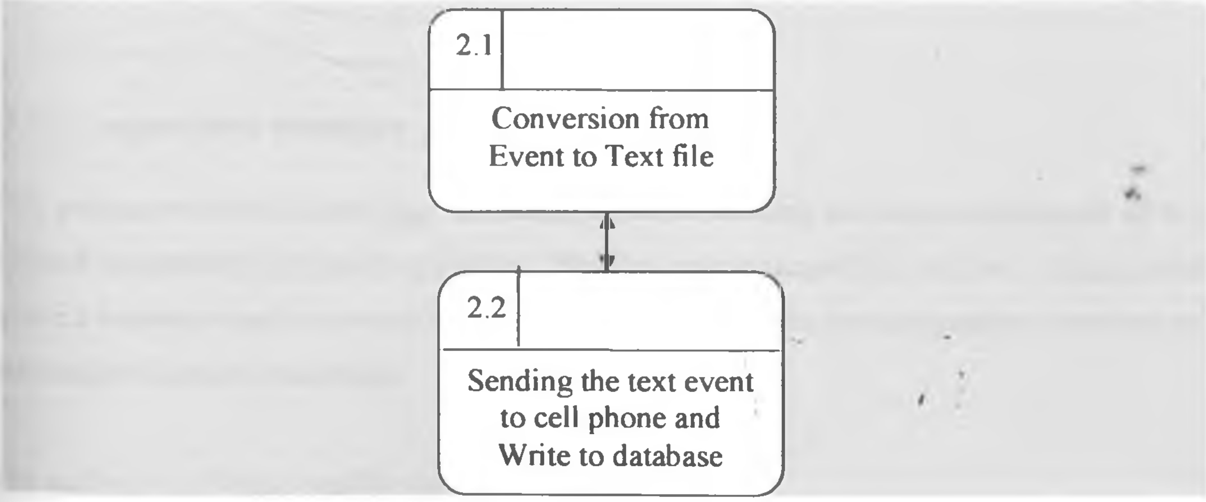
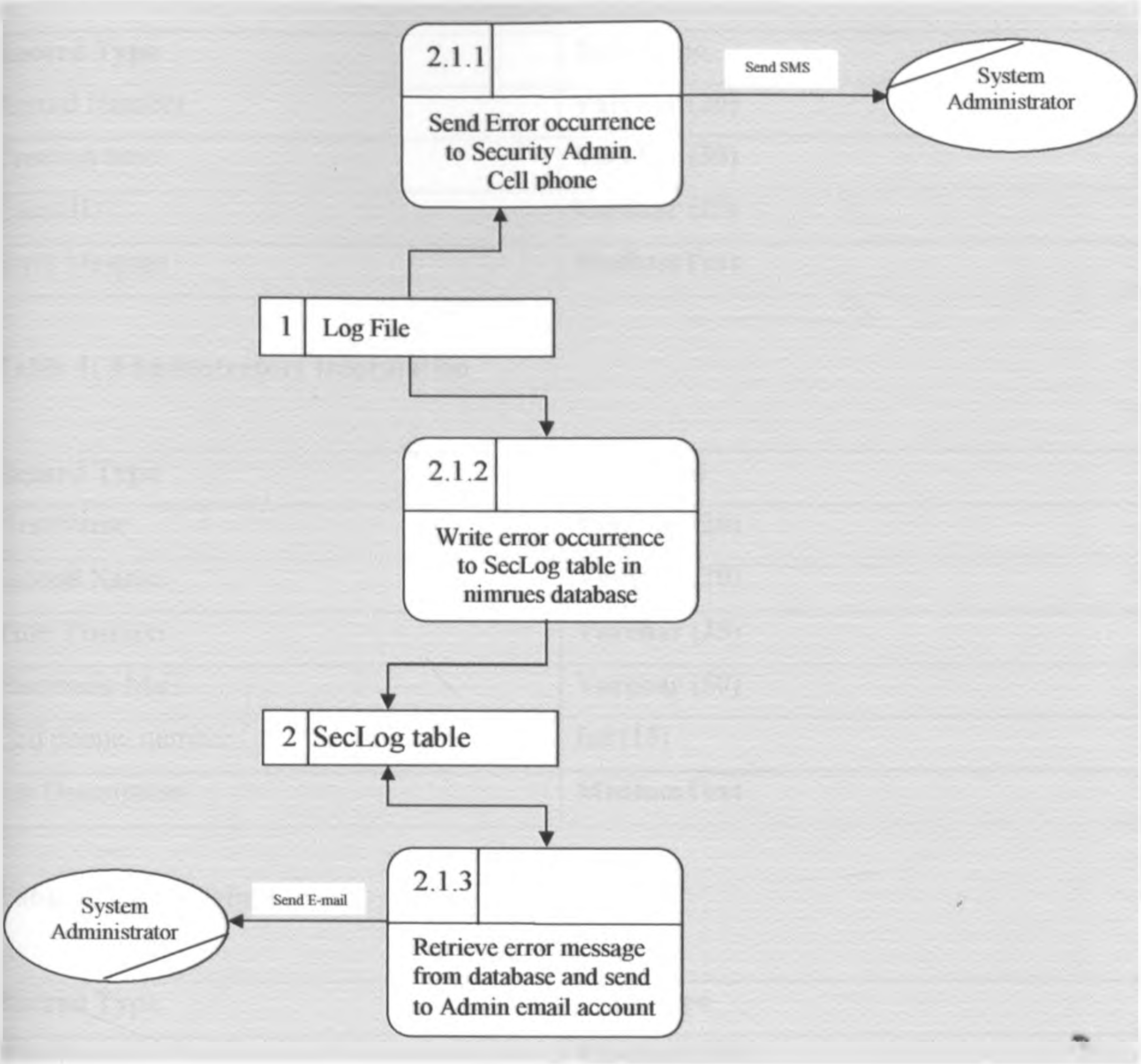


Figure 11: New system Level 3 DFD


2.1.1
Send Error occurrence to Security Admin. Cell phone
Send SMS
System Administrator
1
Log File
2.1.2
Write error occurrence to SecLog table in nimrues database
2
SecLog table
2.1.3
Retrieve error message from database and send to Admin email account
Send E-mail
System Administrator

3.3.2 Logical Data Modelling

This process involved identifying, modelling and documenting the data requirements of the network monitoring and reporting system. The data was separated into entities - things about which a business needs to record information and since entities are independent there are no associations between the entities.

The end result of which was the entities as shown below:

Table 3: Error Log Extract Table

Record Type	Data Type
Record Number	**Varchar (20)**
Creation time	**Varchar (30)**
Event ID	**Varchar (15)**
Error Message	**MediumText**

Table 4: Administrators Information

Record Type	Data Type
First Name	**Varchar (20)**
Second Name	**Varchar (20)**
Title/ Position	**Varchar (25)**
Electronic Mail	**Varchar (50)**
Cell phone number	**Int (15)**
Job Description	**MediumText**

Table 5: User Login Account

Record Type	Data Type
User Name	**Varchar (20)**
Password	**Password MD5 (30)**

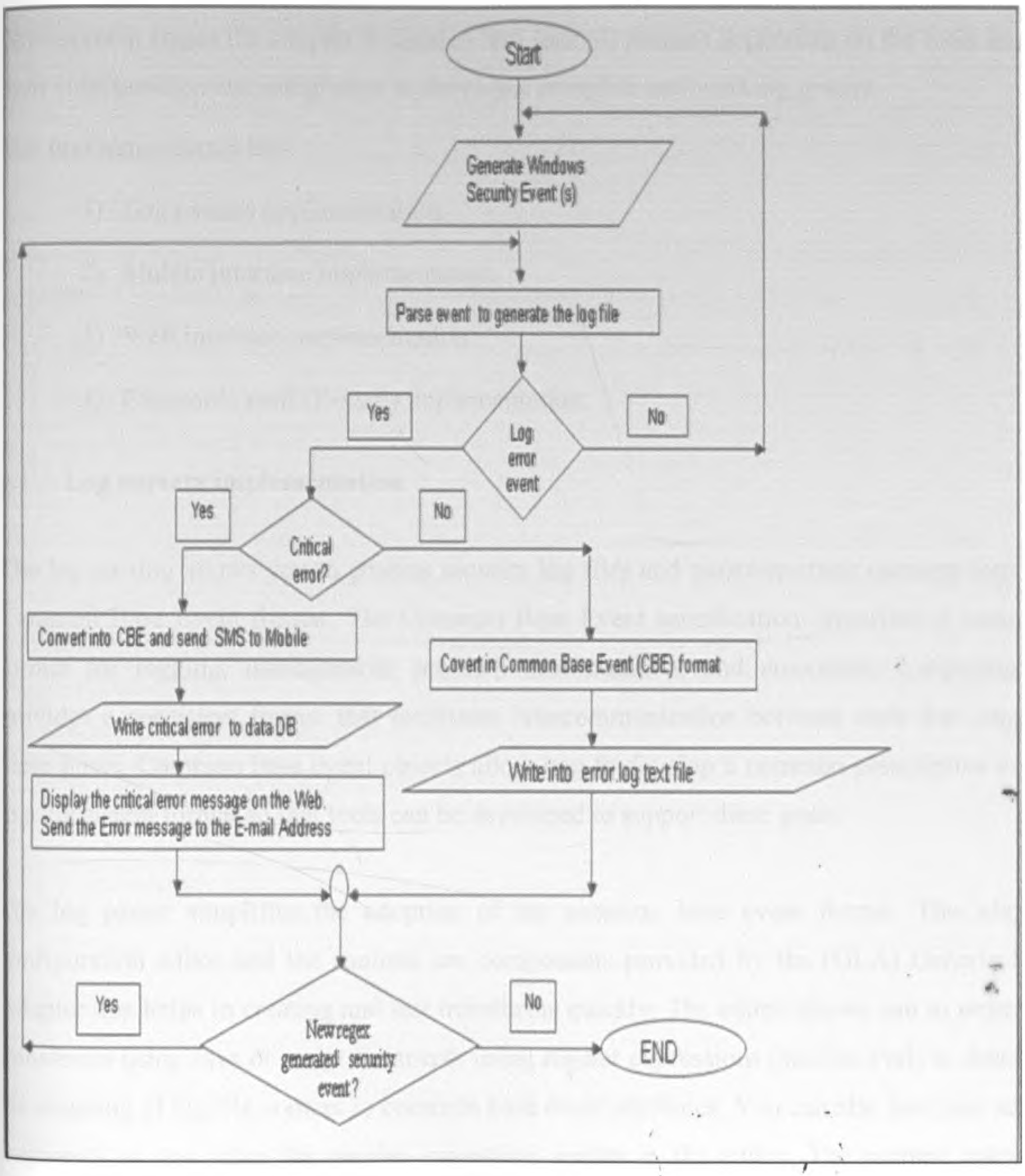
Table 6: Counter

Record Type	Data Type
Count	**Int (10)**

3.3.3 Flow of program Logic

Below is a graphical representation of the flow of control within the network intrusion monitoring and reporting using E-mail and SMS (NIMRUES) system.

Figure 12: System Flowchart


Start
Generate Windows Security Event (s)
Parse event to generate the log file
Yes
No
Log error event
Yes
No
Critical error?
Convert into CBE and send SMS to Mobile
Covert in Common Base Event (CBE) format
Write critical error to data DB
Write into error.log text file
Display the critical error message on the Web.
Send the Error message to the E-mail Address
Yes
No
New regex generated security event?
END

Chapter 4

4 RESULTS

4.0 Introduction

The development and implementation process is core in fulfilling the objectives of this project and answering the research questions. Due to the multiple tools needed in the development stages the chapter is divided into four (4) phrases depending on the tools in use, their configuration and integration to develop a complete and working system.

The four main phases are:

1) Log parsers implementation.
2) Mobile interface implementation.
3) Web Interface implementation.
4) Electronic mail (E-mail) implementation.

4.1 Log parsers implementation

The log parsing allows you to process security log files and transform their contents into the Common Base Event format. The Common Base Event specification prescribes a common format for logging, management, problem determination, and autonomic computing. It provides a consistent format that facilitates intercommunication between tools that support these goals. Common base event objects allow you to develop a common prescriptive event in a consistent format so that tools can be developed to support these goals.

The log parser simplifies the adoption of the common base event format. The adapter configuration editor and the runtime are components provided by the (GLA) Generic Log Adapter that helps in creating and test transforms quickly. The editor allows you to write the transforms using Java or script fragments using regular expressions (such as Perl) to describe the mapping of log file content to common base event attributes. You can also test your script fragments as you write the regular expression scripts in the editor. The runtime takes as inputs the rules that you have written and your log file and produces Common Base Event objects as outputs.

4.1.1 Phases in log parsing:

i) Context

The context describes the ordered grouping of components as they are chained together for log file processing. Each log file has a separate context, and multiple contexts can be defined in a single configuration.

The adapter provides one context: org.eclipse.hyades.logging.adapter.impl.BasicContext - a context which runs each of the components in a single thread.

ii) Sensor

The sensor provides the mechanism to read the content for processing. The Generic Log Adapter provides the following sensors:

SingleFileSensor: A sensor that reads files from a local storage medium.Executable Class: org.eclipse.hyades.logging.adapter.sensors.SingleOSFileSensor

StaticParserSensor: A sensor that integrates transforms that are performed by Java based implementations. It directly invokes the Java parser and exports the Common Base Event objects that the Java parser produces.

Executable Class: org.eclipse.hyades.logging.adapter.config.sensors.StaticParserSensor

AdapterCBESensor: A sensor that monitors the adapter's execution. It is used internally by Generic Log Adpater to log messages from the Generic Log Adapter itself. All internal logging within the

adapter is sent to this sensor. Executable

Class:org.eclipse.hyades.logging.adapter.internal.util.-AdapterSensor

iii) Extractor

The extractor takes a collection of input lines provided by the sensor and separates them into message boundaries. The Generic Log Adapter provides the following extractors:

org.eclipse.hyades.logging.adapter.extractors.RegularExpressionExtractor

This extractor uses regular expressions to describe the delimitation of the log file into messages.

org.eclipse.hyades.logging.adapter.extractors.SimpleExtractor.

This extractor uses simple string comparisons to describe the delimitation of the log file into messages. This extractor, a high-performance alternative to the regular expression extractor, should be used with log files that contain unchanging message delimiters.

iv) Parser

The parser takes the messages that have been delimited by the extractor and builds a set of mappings of string values to a data structure. In the case of the adapter the data structure is Common Base Event 1.0.1. It provides the following parser class:org.eclipse.hyades.logging. adapter.parsers.Parser

This parser uses regular expressions to parse values to build Common Base Event objects. The java.util.regex library is used for processing regular expressions. The parser has two phases of execution:
The global processing phase, entails a set of global regular expressions is executed against the message provided by the extractor. The attribute processing phase, involves specific sets of substitution rules are executed to determine the value to be assigned to each attribute in the data structure (Common Base Event 1.0.1).

The two phases of execution allow the message to be tokenized into a series of attribute values during the global processing phase. The attribute values can then be referred to by attribute name or index during the attribute processing phase.

v) Formatter

The formatter takes the mappings of attributes to their values provided by the parser and builds the correct Java object instance. The adapter runtime contains a single formatter that creates Common Base Event objects conforming to the Common Base Event version

vi) Outputter

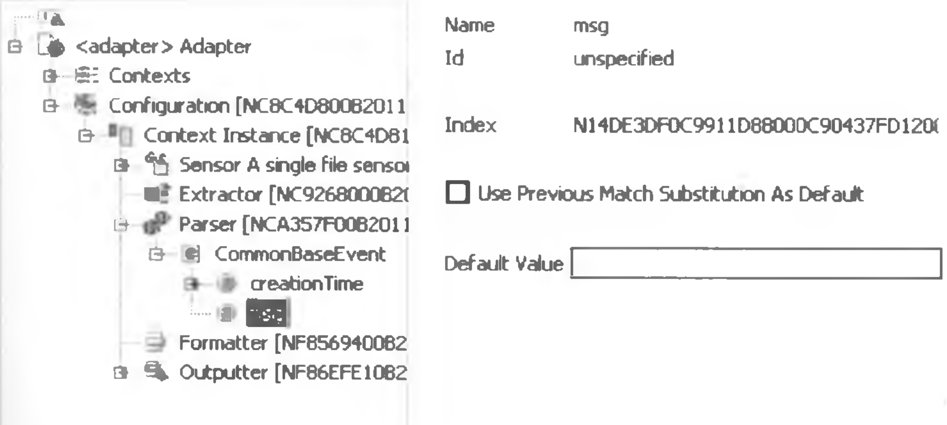
The outputter externalizes the resulting Common Base Event records provided by the formatter. Outputters provide, or wrap, the mechanism for storing the final outputs of the context. The Hyades Generic Log Adapter provides the following outputters:
org.eclipse.hyades.logging.adapter.outputters.CBEFileOutputter: receives Common Base Event instances and writes the externalized records to a file.

org.eclipse.hyades.logging.adapter.outputters.CBEStdoutOutputter: receives Common Base Event instances and writes the externalized records to standard output.

org.eclipse.hyades.logging.adapter.outputters.CBELogOutputter: This outputter receives Common Base Event records, creates a logging agent and writes the externalized records to the logging agent. The CBELogOutputter should only be included in adapter configuration files that will be used outside of eclipse. The user can specify the logging agent name as an Outputter proprerty in the adapter configuration file and must manually attach and start monitoring the agent within Log and Trace Analyzer in order to see the data in the Log View.

org.eclipse.hyades.logging.adapter.outputters.StaticParserOutputter: This outputter receives Common Base Event instances and writes the externalized records to a logging agent. The StaticParserOutputter should only be included in adapter files that will be used to import logs into the Log and Trace Analyzer. It should only be used for parsers that are extensions of the org.eclipse.hyades.logging.parsers.logParser extension point.

The diagram below represents a common adapter configuration file.



Name msg

Id unspecified

Index N14DE3DF0C9911D88000C90437FD120(

□ Use Previous Match Substitution As Default

Default Value

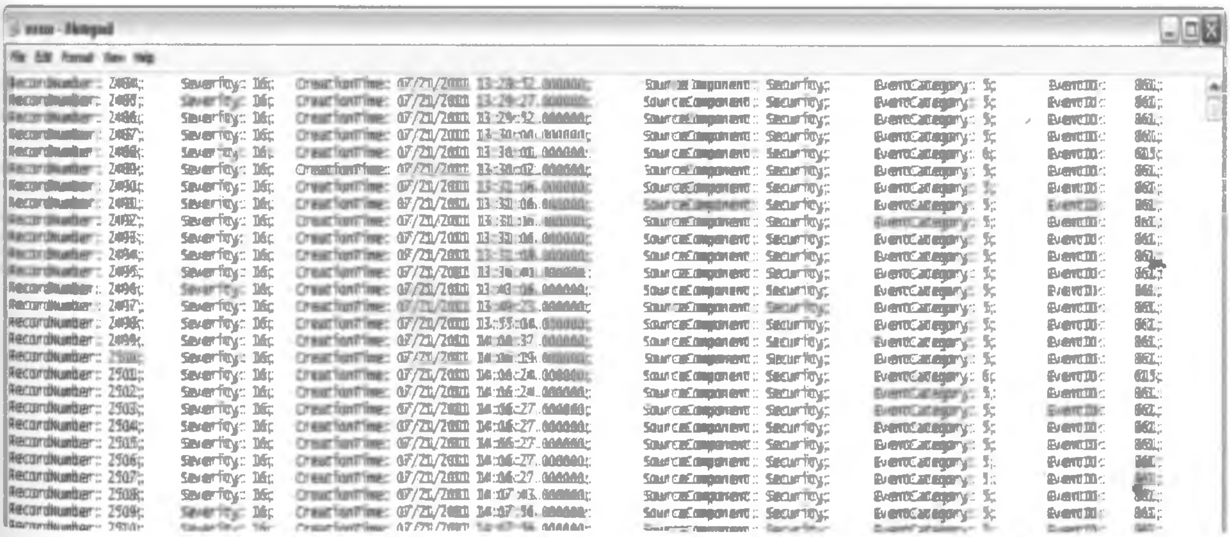
Figure 13: Adapter configuration file for Windows log parser

The log adapter you created is run externally from by a batch file in the Windows environment (shell script in exists for Linux environments). The java eclipse code is used to run the runregex_example adapter file, to run the Generic Log Adapter on a system, Hyades must be installed on that system. Below is the extract of the XML version of the executed Adapter file when opened in Dreamweaver 8 program.

4.1.2 GLA adapter conversion to XML (Extract).

```
<?xml version="1.0" encoding="UTF-8"?>
<adapter:Adapter xmlns:adapter="http://www.eclipse.org/hyades/schema/Adapter.xsd"
xmlns:cc="http://www.eclipse.org/hyades/schema/ComponentConfiguration.xsd"
xmlns:ex="http://www.eclipse.org/hyades/schema/Extractor.xsd"
xmlns:fmt="http://www.eclipse.org/hyades/schema/Formatter.xsd"
xmlns:hga="http://www.eclipse.org/hyades/schema/Context.xsd"
xmlns:op="http://www.eclipse.org/hyades/schema/Outputter.xsd"
xmlns:parser="http://www.eclipse.org/hyades/schema/Parser.xsd"
xmlns:pu="http://www.eclipse.org/hyades/schema/ProcessUnit.xsd"
xmlns:sensor="http://www.eclipse.org/hyades/schema/Sensor.xsd">
  <hga:Contexts>
```

Once the file has been executed as a batch file it creates an error log file named "Error.log" which is in text file format and an out file named "Example.out" in binary format. This two files are as result of converting Windows Security binary file into a text file. A sample on the out error file is as given below.



```
RecordNumber:: 2484;   Severity:: 16;   CreationTime:: 07/21/2011 13:28:52.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2485;   Severity:: 16;   CreationTime:: 07/21/2011 13:29:27.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2486;   Severity:: 16;   CreationTime:: 07/21/2011 13:29:52.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2487;   Severity:: 16;   CreationTime:: 07/21/2011 13:30:04.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2488;   Severity:: 16;   CreationTime:: 07/21/2011 13:30:01.000000;   SourceComponent:: Security;   EventCategory:: 6;   EventID:: 615;
RecordNumber:: 2489;   Severity:: 16;   CreationTime:: 07/21/2011 13:30:02.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2490;   Severity:: 16;   CreationTime:: 07/21/2011 13:31:06.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2491;   Severity:: 16;   CreationTime:: 07/21/2011 13:31:06.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2492;   Severity:: 16;   CreationTime:: 07/21/2011 13:31:16.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2493;   Severity:: 16;   CreationTime:: 07/21/2011 13:31:06.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2494;   Severity:: 16;   CreationTime:: 07/21/2011 13:31:18.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2495;   Severity:: 16;   CreationTime:: 07/21/2011 13:36:41.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2496;   Severity:: 16;   CreationTime:: 07/21/2011 13:43:06.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2497;   Severity:: 16;   CreationTime:: 07/21/2011 13:49:25.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2498;   Severity:: 16;   CreationTime:: 07/21/2011 13:53:04.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 862;
RecordNumber:: 2499;   Severity:: 16;   CreationTime:: 07/21/2011 14:00:37.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2500;   Severity:: 16;   CreationTime:: 07/21/2011 14:00:29.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2501;   Severity:: 16;   CreationTime:: 07/21/2011 14:06:24.000000;   SourceComponent:: Security;   EventCategory:: 6;   EventID:: 615;
RecordNumber:: 2502;   Severity:: 16;   CreationTime:: 07/21/2011 14:06:24.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2503;   Severity:: 16;   CreationTime:: 07/21/2011 14:06:27.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 862;
RecordNumber:: 2504;   Severity:: 16;   CreationTime:: 07/21/2011 14:06:27.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 862;
RecordNumber:: 2505;   Severity:: 16;   CreationTime:: 07/21/2011 14:06:27.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2506;   Severity:: 16;   CreationTime:: 07/21/2011 14:06:27.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2507;   Severity:: 16;   CreationTime:: 07/21/2011 14:06:27.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2508;   Severity:: 16;   CreationTime:: 07/21/2011 14:07:43.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2509;   Severity:: 16;   CreationTime:: 07/21/2011 14:07:56.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
RecordNumber:: 2510;   Severity:: 16;   CreationTime:: 07/21/2011 14:07:56.000000;   SourceComponent:: Security;   EventCategory:: 5;   EventID:: 861;
```

Figure 14: Error log file generated in text format by the Windows Security log parser

4.2 Mobile interface implementation

The mobile implementation phase has been developed using Java programming language, the Java Eclipse software platform for the text editor, Java 2 Standard development Kit (J2SDK) and Java Runtime Environment (JRE) version 1.6.22 for both which are used for interpreting and compiling the code during execution.

A collection of other jar files have been added to facilitate the connection of the SMS gateway. More details about the development, configuration and execution have been described below.

4.2.1 Installing and Configuring the SMSLib 3.5

This part of the project involves installing and setup of the sms gateway with SMSLib, I used SMSLib, because it's support the sending of sms to Java and J2ME applications, using the push registry. Below is the explanation on how to setup SMSLib in Windows using java eclipse.

The installation is divided into two parts: i.e. the pre-requisites then installation and configuration process.

a) Pre-requisites

To use SMSLib, the following components should have already be pre- installed:

- SUN JDK 1.6 or newer.
- Java Communications Library.
- Apache ANT for building the sources.
- Apache log4j.
- Apache Jakarta Commons – NET.
- JSMPP Library

Starting from SMSLib v3.4, the installation procedure has slightly changed. Some SMSServer components that required extra dependencies have been pulled out of the main source tree. This has been done in order to reduce the required third party libraries & dependency files for those wanting to use the core library. The core SMSLib/SMSServer source files can now be compiled with only two dependencies: the Simple logging facade for Java and the Apache Commons/NET for the IP modem driver.

All other add-on SMSServer components are moved in the folder /misc/SMSServer /Interfaces/, organized by development status. Installation instructions for these specific components are given in the relevant SMSServer documentation pages.

Java Communications Library: Meant for use for Win32 systems and the SUN Java Comm v2 is the most available and stable package in the market.

Java Comm Installation: The installation procedure for both the old Java Comm v2 and the new Java Comm v3 is identical.

b) Installation and Configuration process

To perform the installation and configuration process then, the first step involves unzipping the downloaded archive file (http://www.doitmyway.net/2010/05/14/smslib-installer-netjava/) in a temporary place and performs the following copies to their respective folders:

File comm.jar, commons-net-2.0.jar, jsmpp-2.1.0.jar, log4j-1.2.16.jar, slf4j-simple-1.6.1.jar and slf4j-api-1.6.1.jar are placed under C:/Program Files/Java/jdk1.6.0/jre/lib/ext/

File javax.comm.properties should go under C:/Program Files/Java/jdk1.6.0/jre/lib

Library files (i.e. win32com.dll) for windows32 should go under C:/Program Files/Java/jdk1.6.0/bin/

If you have a separate JRE directory from the one of JDK, do the same copies for the JREDIR directory!

Since the SMSLib is been used for only two functions, reading and sending the error message then the java files below are implemented.

4.2.2 OutboundNotification Class

```
package org.aiti.sms;
import org.smslib.IOutboundMessageNotification;
import org.smslib.OutboundMessage;
public class OutboundNotification implements IOutboundMessageNotification {
        public void process(String gatewayId, OutboundMessage msg) {
                System.out.println("Outbound handler called from Gateway: " + gatewayId);
                System.out.println(msg);
        }
}
```

4.2.3 SendMessage Class (Extract)

```
// SendMessage.java - Sample application.
//
// This application shows you the basic procedure for sending messages.
// You will find how to send synchronous and asynchronous messages.
//
// For asynchronous dispatch, the example application sets a callback
// notification, to see what's happened with messages.


package org.aiti.sms;

//import org.smslib.IOutboundMessageNotification;
import org.smslib.Library;
*import org.smslib.OutboundMessage;
import org.smslib.Service;
import org.smslib.modem.SerialModemGateway;

import java.io.*;
import java.sql.*;
import java.util.*;

public class SendMessage extends OutboundNotification
{
        public void doIt() throws Exception
        {
                Service srv;
                OutboundMessage msg;
                OutboundNotification outboundNotification = new OutboundNotification();
                System.out.println("Example: Send message from a serial gsm modem.");
                System.out.println(Library.getLibraryDescription());
                System.out.println("Version: " + Library.getLibraryVersion());
```

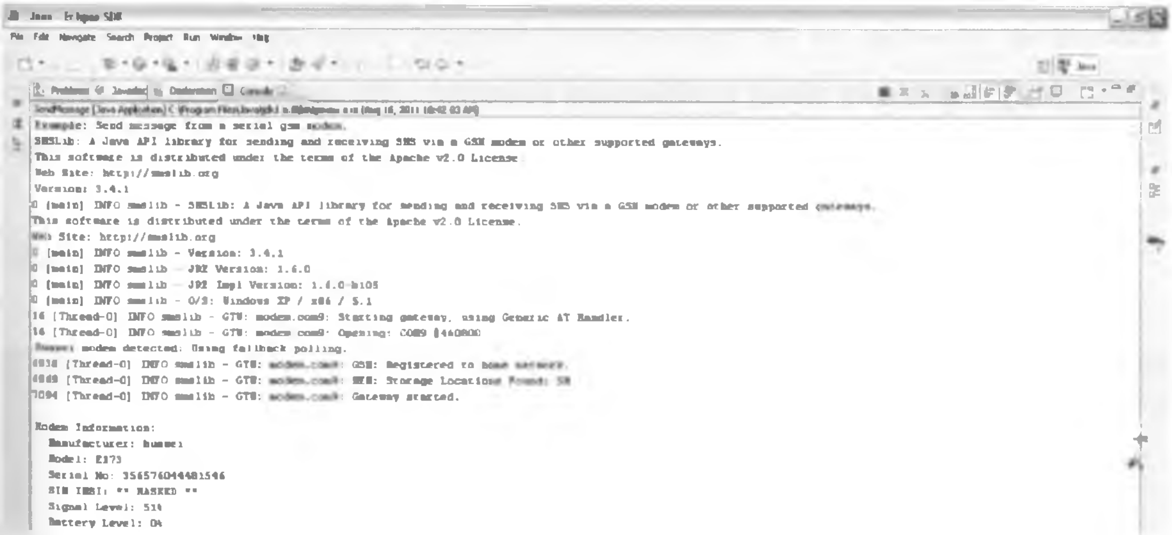
```
			srv = new Service();
			SerialModemGateway gateway = new SerialModemGateway("modem.com9",
"COM9", 460800, "Huawei", "E173");
			//SerialModemGateway gateway = new SerialModemGateway("modem.com",
"COM23", 921600, "ZTE", "MF637U");
			gateway.setInbound(false);
			gateway.setOutbound(true);

			srv.startService();
			System.out.println();
			System.out.println("Modem Information:");
			System.out.println("  Manufacturer: " + gateway.getManufacturer());
			System.out.println("  Model: " + gateway.getModel());
			System.out.println("  Serial No: " + gateway.getSerialNo());
			System.out.println("  SIM IMSI: " + gateway.getImsi());
			System.out.println("  Signal Level: " + gateway.getSignalLevel() + "%");
			System.out.println("  Battery Level: " + gateway.getBatteryLevel() + "%");
			System.out.println();

			//Database connectivity
			 Class.forName("com.mysql.jdbc.Driver");

			 while(true)
			 {
```

Once the two classes are executed, the Java Eclipse detects the presence of the huawei E173 modem and with the available API libraries. The diagram below shows the detection.


Java - Eclipse SDK
File Edit Navigate Search Project Run Window Help
Problems Javadoc Declaration Console
SendMessage [Java Application] C:\Program Files\Java\jdk... (Aug 16, 2011 10:42:03 AM)

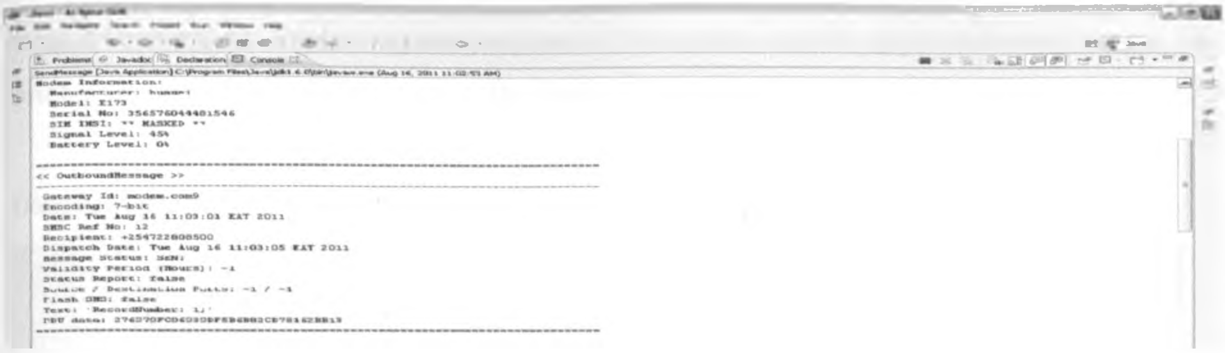
```
Example: Send message from a serial gsm modem.
SMSLib: A Java API library for sending and receiving SMS via a GSM modem or other supported gateways.
This software is distributed under the terms of the Apache v2.0 License.
Web Site: http://smslib.org
Version: 3.4.1
0 [main] INFO smslib - SMSLib: A Java API library for sending and receiving SMS via a GSM modem or other supported gateways.
This software is distributed under the terms of the Apache v2.0 License.
Web Site: http://smslib.org
0 [main] INFO smslib - Version: 3.4.1
0 [main] INFO smslib - JRE Version: 1.6.0
0 [main] INFO smslib - JRE Impl Version: 1.6.0-b105
0 [main] INFO smslib - O/S: Windows XP / x86 / 5.1
16 [Thread-0] INFO smslib - GTW: modem.com9: Starting gateway, using Generic AT Handler.
16 [Thread-0] INFO smslib - GTW: modem.com9: Opening: COM9 @460800
Huawei: modem detected: Using fallback polling.
4938 [Thread-0] INFO smslib - GTW: modem.com9: GSM: Registered to home network.
4969 [Thread-0] INFO smslib - GTW: modem.com9: MEM: Storage Locations Found: SM
7094 [Thread-0] INFO smslib - GTW: modem.com9: Gateway started.

Modem Information:
  Manufacturer: huawei
  Model: E173
  Serial No: 356576044481546
  SIM IMSI: ** MASKED **
  Signal Level: 51%
  Battery Level: 0%
```

Diagram 1: Detecting the GSM modem connection.

4.2.4 Send SMS using Huawei Modem gateway

If the modem is detected correctly by the java API, the message is sent to the mobile phone number given in the send message class in the Java Eclipse SDK program.



```
SendMessage [Java Application] C:\Program Files\Java\jdk1.6.0\bin\javaw.exe (Aug 16, 2011 11:02:53 AM)
Modem Information:
  Manufacturer: huawei
  Model: E173
  Serial No: 356576044401546
  SIM IMSI: ** MASKED **
  Signal Level: 45%
  Battery Level: 0%

-----------------------------------------------------------------------------------
<< OutboundMessage >>
-----------------------------------------------------------------------------------
 Gateway Id: modem.com9
 Encoding: 7-bit
 Date: Tue Aug 16 11:03:01 EAT 2011
 SMSC Ref No: 12
 Recipient: +254722808500
 Dispatch Date: Tue Aug 16 11:03:05 EAT 2011
 Message Status: SENT
 Validity Period (Hours): -1
 Status Report: false
 Source / Destination Ports: -1 / -1
 Flash SMS: false
 Text: 'RecordNumber: 1;'
 PDU data: 276270FCD6039DFEB4B82CB78162BB13
-----------------------------------------------------------------------------------
```

Diagram 2: Successful sending of messages by the GSM modem

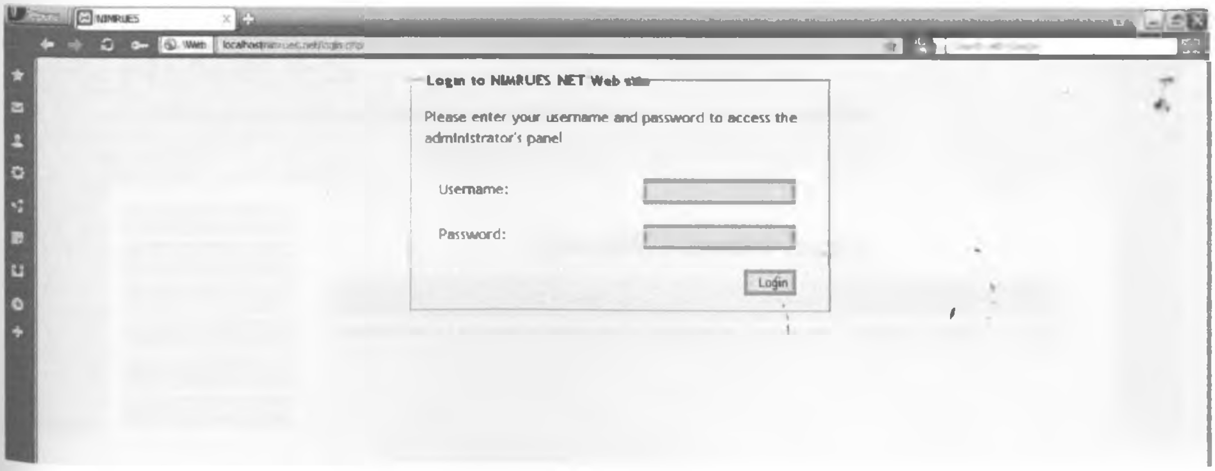
4.3 Web interface implementation

The client side of web interface is implemented using HTML and the server side using PHP. The screen capture of the system login to properties and the php code is shown below.

4.3.1 Login.php

This ensures that a registered user is allowed to log-in into the systems. Secure session management is maintained to ensure that user password are not cached by the browser and once the system user logs off it becomes impossible to access the index page without login again with user names and encrypted passwords been stored in the database.

Diagram 3: Login.php



Login to NIMRUES NET Web site

Please enter your username and password to access the administrator's panel

Username:

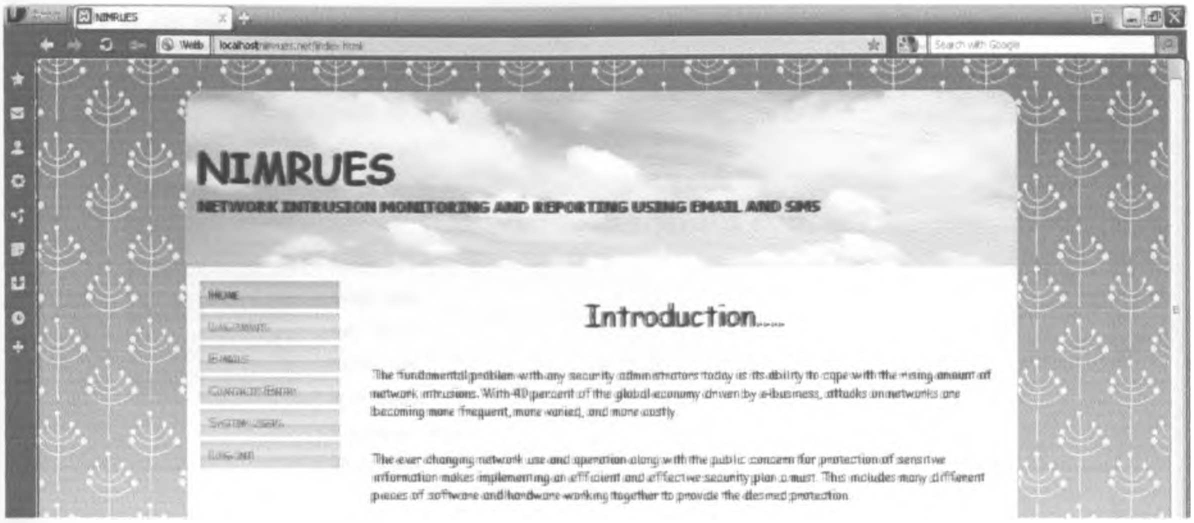
Password:

Login

4.3.2 index.html

The index page contains pertinent information in regards to the system. It contains an executive summary explaining the purpose of the system and its application and usage. The brief summary introduces the user to the basic details of its existence.

Diagram 4: index.html


NIMRUES
localhost/nimrues.net/index.html
Search with Google
NIMRUES
NETWORK INTRUSION MONITORING AND REPORTING USING EMAIL AND SMS
HOME
LOG EVENTS
E-MAILS
CONTACTS ENTRY
SYSTEM USERS
LOG OUT

Introduction....

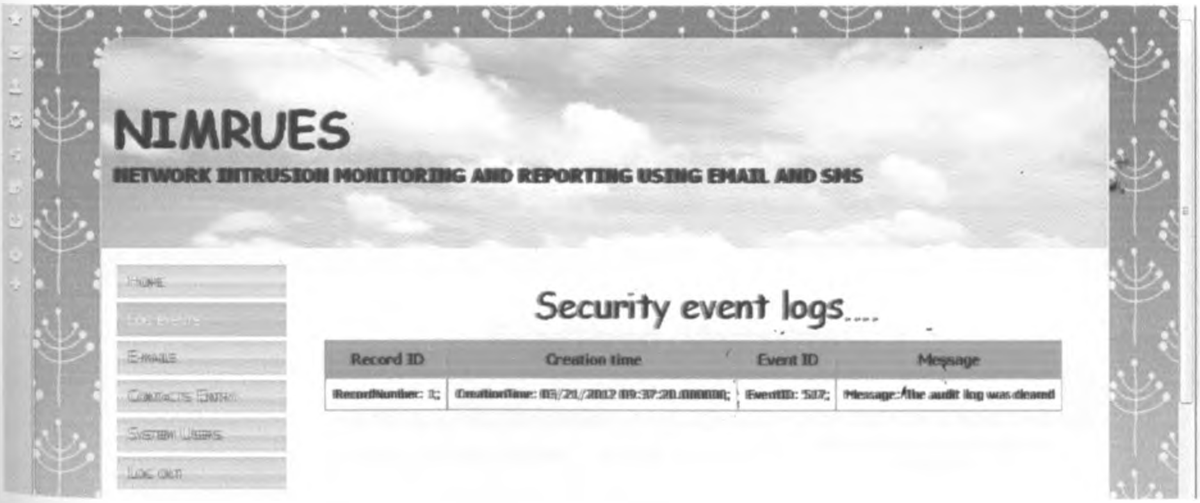
The fundamental problem with any security administrators today is its ability to cope with the rising amount of network intrusions. With 40 percent of the global economy driven by e-business, attacks on networks are becoming more frequent, more varied, and more costly.

The ever changing network use and operation along with the public concern for protection of sensitive information makes implementing an efficient and effective security plan a must. This includes many different pieces of software and hardware working together to provide the desired protection.

4.3.3 Show.php

This file retrieves critical data stored in the database in-order to display to security administrators who may prefer to use the web access since it provides more details than the SMS and E-mail system. i.e additional features of the web includes creation time and Event ID which are not in use SMS systems in order to reduce bulkiness and enhance efficiency.

Diagram 5: Log events: Used to retrieve the messages from the database and display.


NIMRUES
NETWORK INTRUSION MONITORING AND REPORTING USING EMAIL AND SMS
HOME
LOG EVENTS
E-MAILS
CONTACTS ENTRY
SYSTEM USERS
LOG OUT

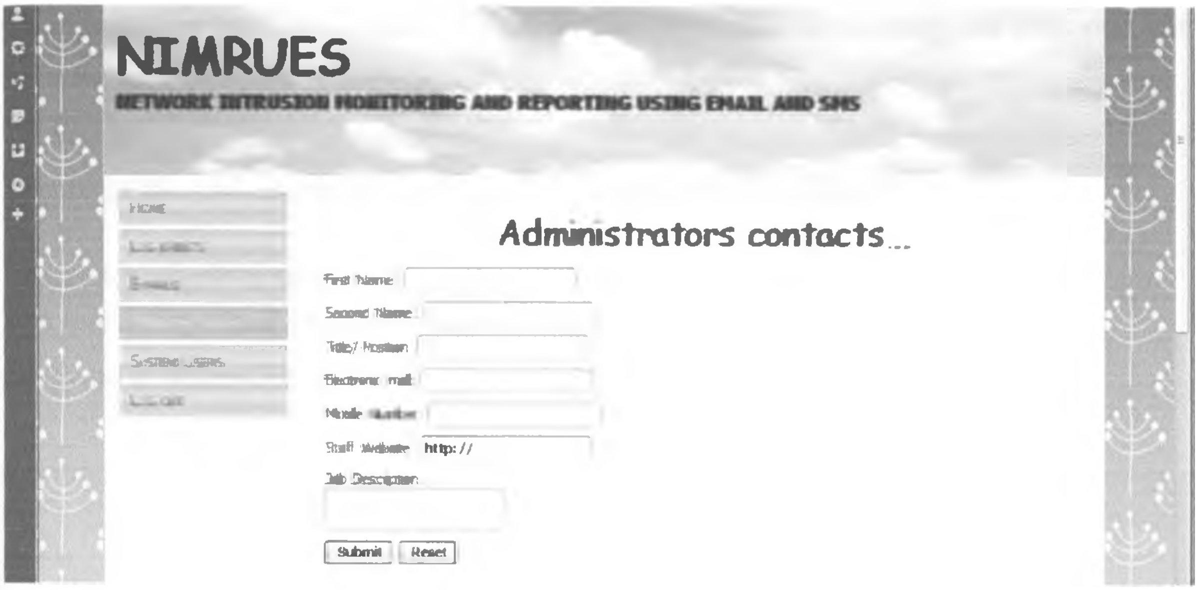
Security event logs....

Record ID	Creation time	Event ID	Message
RecordNumber: 1;	CreationTime: 03/21/2012 09:37:20.000000;	EventID: 517;	Message: The audit log was cleared

4.3.4 Contacts.php

This is a form to capture security administrator details. The details are used in relaying both SMS and E-mails from the network intrusion system to the respective administrator for action.

Diagram 6: Administrators' details form


NIMRUES
NETWORK INTRUSION MONITORING AND REPORTING USING EMAIL AND SMS
HOME
LOG EVENTS
E-MAILS
SYSTEM USERS
LOG OUT
Submit
Reset

Administrators contacts...

First Name

Second Name

Title/ Position

Electronic mail

Mobile Number

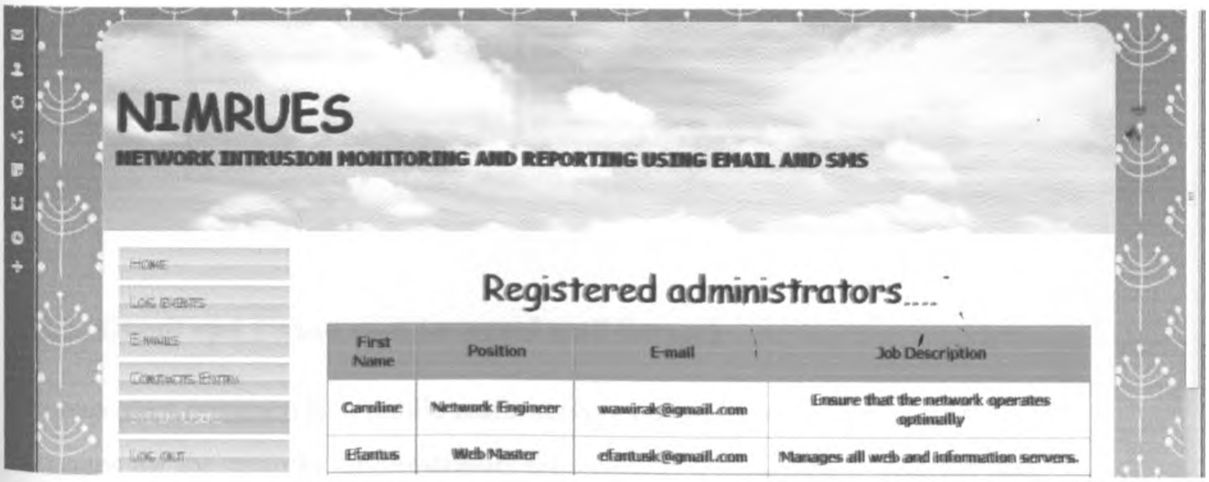
Staff Website http: //

Job Description

4.3.5 System users.php

This php file retrieves administrators details stored in the database in-order to displays to security administrators who be interested to know the status and position of users who can receive messages from the nimrues system.

Diagram 7: Registered system users.


NIMRUES
NETWORK INTRUSION MONITORING AND REPORTING USING EMAIL AND SMS
HOME
LOG EVENTS
E-MAILS
CONTACTS ENTRY
SYSTEM USERS
LOG OUT

Registered administrators....

First Name	Position	E-mail	Job Description
Caroline	Network Engineer	wawirak@gmail.com	Ensure that the network operates optimally
Efantus	Web Master	efantusk@gmail.com	Manages all web and information servers.

4.4 Electronic mail (E-mail) interface implementation

The server side of the e-mail implementation is done by configuring the Mercury 32 server that comes embedded with XAMPP server. While the client side of E-mail is implemented using electronic mail client software in our case we are using Microsoft Outlook express to retrieve the email messages from the Mercury mail server.

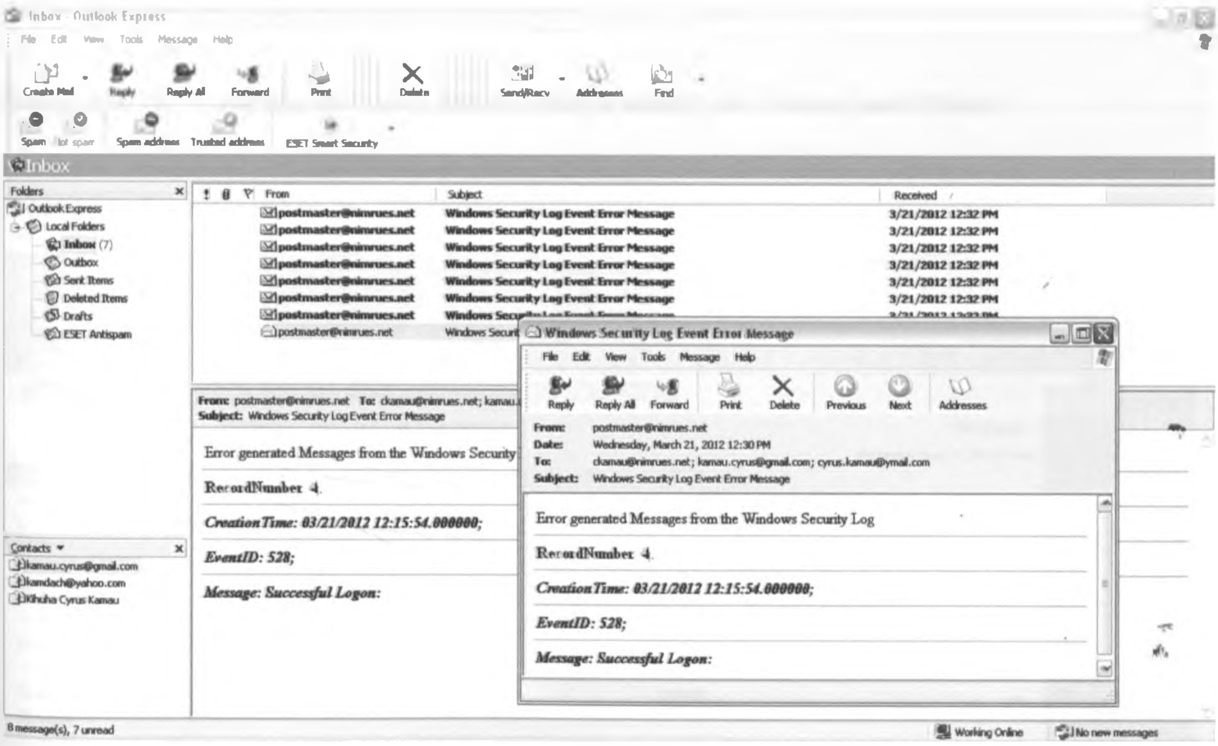
The configuration of Microsoft Outlook express involves the setting up of two communication ports SMTP (port 110) and POP3 (port 425) for sending and retrieving mails from the inbox respectively.

Results of the sent mail as displayed on the client side are as follows:

4.4.1 Microsoft outlook express (Local mail server)

The screen capture of Microsoft outlook is as shown below.

Diagram 8: Microsoft outlook express mails received from nimrues.net server



From	Subject	Received
postmaster@nimrues.net	Windows Security Log Event Error Message	3/21/2012 12:32 PM
postmaster@nimrues.net	Windows Security Log Event Error Message	3/21/2012 12:32 PM
postmaster@nimrues.net	Windows Security Log Event Error Message	3/21/2012 12:32 PM
postmaster@nimrues.net	Windows Security Log Event Error Message	3/21/2012 12:32 PM
postmaster@nimrues.net	Windows Security Log Event Error Message	3/21/2012 12:32 PM
postmaster@nimrues.net	Windows Security Log Event Error Message	3/21/2012 12:32 PM
postmaster@nimrues.net	Windows Secu	
postmaster@nimrues.net	Windows Securi	

From: postmaster@nimrues.net **To:** ckamau@nimrues.net; kamau.

Subject: Windows Security Log Event Error Message

Error generated Messages from the Windows Security

RecordNumber 4.

CreationTime: 03/21/2012 12:15:54.000000;

EventID: 528;

Message: Successful Logon:

Contacts

kamau.cyrus@gmail.com

kamdach@yahoo.com

Kihuha Cyrus Kamau

From: postmaster@nimrues.net

Date: Wednesday, March 21, 2012 12:30 PM

To: ckamau@nimrues.net; kamau.cyrus@gmail.com; cyrus.kamau@ymail.com

Subject: Windows Security Log Event Error Message

Error generated Messages from the Windows Security Log

RecordNumber 4.

CreationTime: 03/21/2012 12:15:54.000000;

EventID: 528;

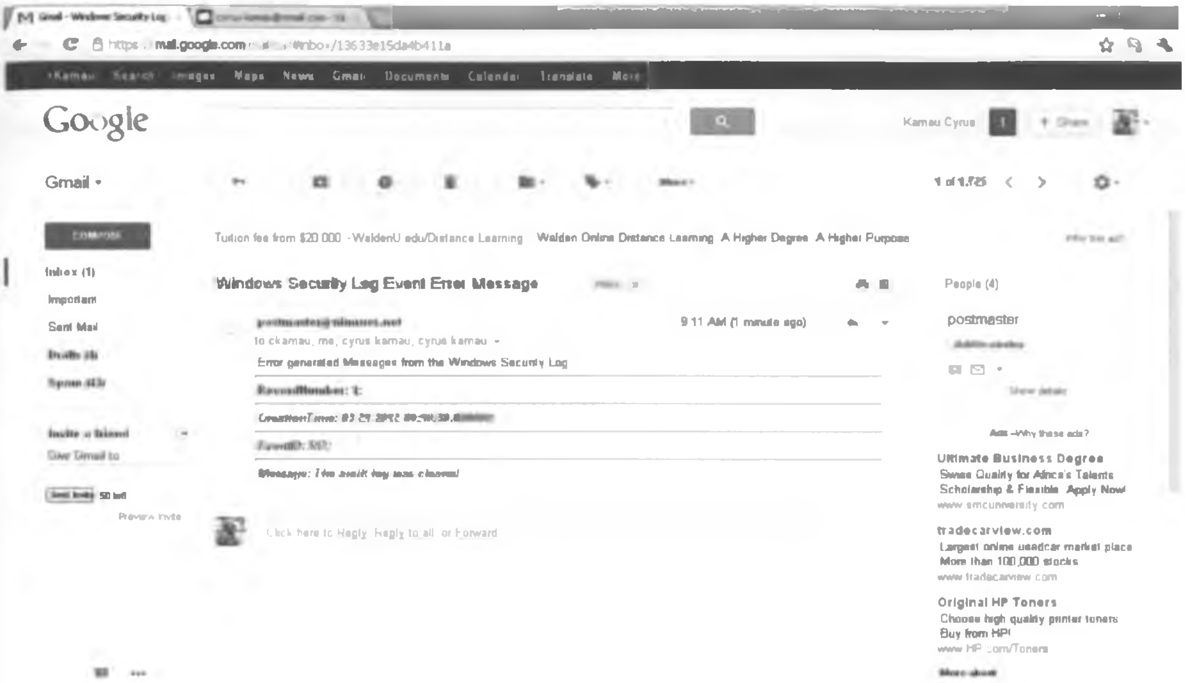
Message: Successful Logon:

8 message(s), 7 unread

4.4.2 Gmail and Yahoo mail (external mail Server)

The two most common free public mails servers can be used to receive relayed error messages for the security administrators this requires a dedicated IP address line.

Diagram 9: Nimrues.net mail server relays mail(s) to Google mail client



Windows Security Log Event Error Message

postmaster@nimrues.net 9 11 AM (1 minute ago)

to ckamau, me, cyrus kamau, cyrus kamau

Error generated Messages from the Windows Security Log

RecordNumber: 1:

CreationTime: 03 29 2012 09:50:38.[illegible]

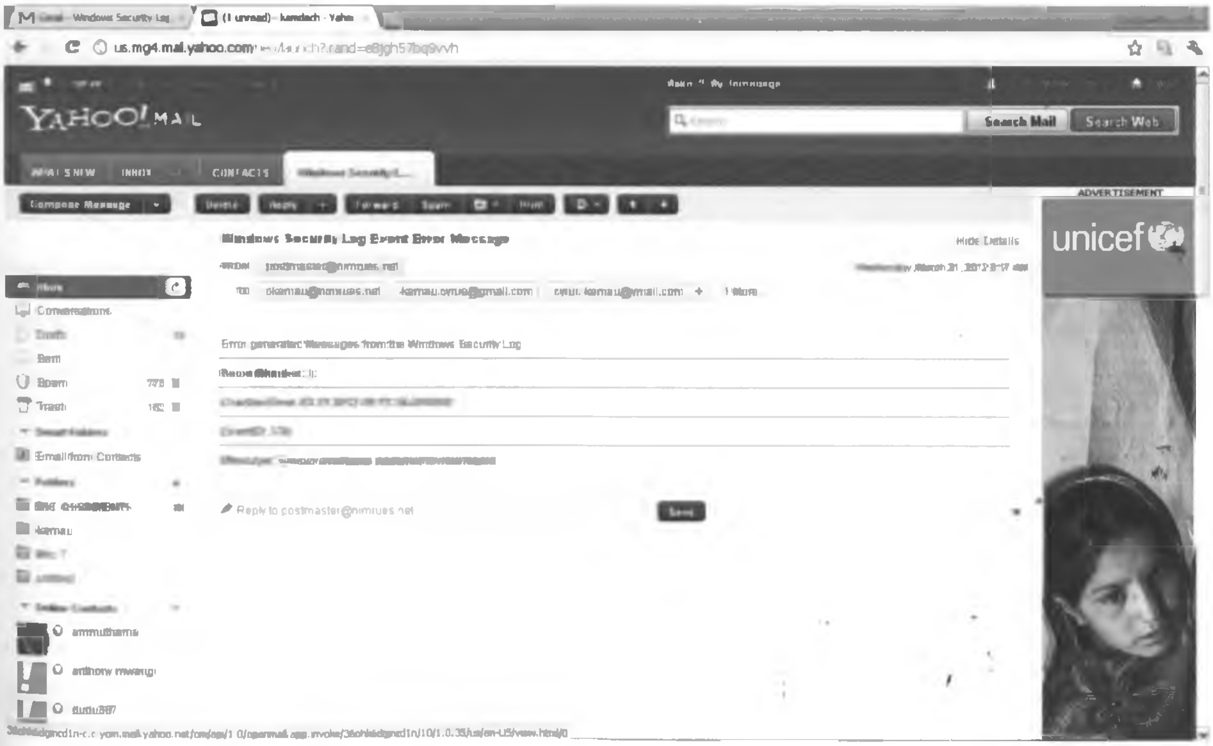
EventID: 517:

Message: The audit log was cleared

Click here to Reply, Reply to all, or Forward

https://mail.google.com/mail/#inbox/13633e15da4b411a
+Kamau Search Images Maps News Gmail Documents Calendar Translate More
Google
Kamau Cyrus
+ Share
Gmail
COMPOSE
Inbox (1)
Important
Sent Mail
Drafts
Spam
Invite a friend
Give Gmail to:
Send Invite 50 left
Preview Invite
1 of 1,725
Tuition fee from $20 000 - WaldenU edu/Distance Learning   Walden Online Distance Learning A Higher Degree A Higher Purpose
People (4)
postmaster
Show details
Ads – Why these ads?
Ultimate Business Degree
Swiss Quality for Africa's Talents
Scholarship & Flexible. Apply Now!
www.smcuniversity.com
tradecarview.com
Largest online usedcar market place
More than 100,000 stocks
www.tradecarview.com
Original HP Toners
Choose high quality printer toners
Buy from HP!
www.HP.com/Toners
More about...

Diagram 10: Nimrues.net mail server relays mail(s) to Yahoo mail client



Windows Security Log Event Error Message

FROM postmaster@nimrues.net Wednesday, March 21, 2012 9:17 AM

TO ckamau@nimrues.net kamau.cyrus@gmail.com cyrus.kamau@ymail.com + 1 More

Error generated Messages from the Windows Security Log

RecordNumber: 1:

CreationTime: 03 29 2012 09:[illegible]

EventID: 517:

Message: [illegible]

Reply to postmaster@nimrues.net

4.5 Testing

a) Module testing

Each module has undergone white box testing and black box testing. In white box testing, walkthroughs were performed on the source code to eliminate syntax errors and improve on quality of the source code in terms of readability. This means indentation, spacing and commenting were all used in improving the readability of the source code.

In black box testing, each module was tested using specific test data and the actual results compared against the expected results. This helped in detecting logical errors and in some cases run time errors which have been rectified.

Web client: Test data tests both client side and server side scripts.

SMS Server: Test data test the server module that sends SMS from SMS Server.

b) Integration Testing

Modules reference the same database. Integration testing has been done in search of any incompatibilities. Issues to do with integrity of data with respect to concurrent requests for read and write have been left to the default SQL server (MySQL) settings but would certainly need further refinement to improve on integrity.

c) System Testing

System testing has been carried out in a test scenario the configuration process involved is complex due to the multiple different tools and configuration management required. The system test has proved it is ready for deployment if all requirements are available.

4.6 Resources

a) Hardware:

The following hardware components were crucial in the implementation of the project.

i). A mobile phone which is a client in the system and interacts with the SMS server and is able to recieve SMS-short message services generated from the log files.

ii). GSM modem which provides for the network gateway.

iii). The SMS server that will forward event messages from the modem.

b) Software

The following software components are crucial in this project:

i). Computer installed with Windows and MySQL server on which the schema resides

ii). SMS server that will receive the event message and pass it over for processing by the application server.

iii). Xampp which is the web server hence services requests from client(browsers)

iv). HTML and JavaScript which provide the client with a suitable interface and enhance interactivity respectfully and PHP which is extensively used in server side scripting

v). JavaScript which is used for client side scripting and Java Eclipse which is used to generate the adapter file.

4.7 Project schedule

The project is expected to take a total of 36 weeks. A scheduled Gantt chart below shows the activities that are to take. The activities to be undertaken during this period are displayed against the schedule shown below.

Table 7: schedule 1

Research	■	■	■	■	■	■	■	■	■	■
Analysis	■	■								
Design			■	■	■	■	■			
Construction					■	■	■	■	■	■
Testing								■	■	■
Documentation	■	■	■	■	■	■	■	■	■	■
	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
Year	2010			2011						

Chapter 5

5 DISCUSSIONS AND CONCLUSIONS

5.0 Introduction

This research and development project involved studying and developing a working system in Network Intrusion Monitoring and Reporting Using E-mail and SMS (NIMRUES) system and the challenges that security administrators faced when dealing with issues of network intrusion. The issues of network intrusion have been in the computing world for over a decade now and so it's not anything new; however the issue of reporting the intrusion occurrences has not been addressed in-depth especially in trying to design and develop an effective and yet relatively cheap means to inform security administrators if and when they occur using mobile technology.

5.1 Discussions

The web, email and mobile technologies remain the most common and widely used form of electronic communication today. The NIMRUES system has been developed to make use of these three technologies to report error occurrences from Windows security log operating system.

A Windows event log extractor and out putter by the name Generic Log Adapter (GLA) has been used to generate a text log file from Windows security event log which are binary in nature. Once the log file has been parsed, Java code is used to read the parsed text file which is in form of a regular expression and send to the security administrator using a GSM gateway. The regular expression is selectively then written into the **seclog** table hosted in the **nimrues** database. Using PHP and JavaScript the messages are then retrieved for display using the link http://localhost/nimrues.net/index.html and simultaneously send to the Mercury mail server where the security administrator using e-mail client Microsoft outlook express can access the sent information.

All the tools and software's used in this project are open source and readily available. The system can be installed and be configured hustle free in any networked environment. The NIMRUES application provides an efficient, working and simplified solution to an important and complex field of network security monitoring. Comparatively to other products in the market NIMRUES offers an effective and available alternative to intrusion detection and reporting in terms of cost (development, setup and operational), availability, ease of use, output delivery to security administrators.

5.2 Assumptions

At present there are no universally acceptable standards for intrusion detection and reporting systems. This has resulted in making some assumptions regarding the project they include but not limited to:-

1. One of the main problems with the NIMRUES system is to be able to dynamically update the database. Keeping intrusion detection and reporting system updated however this is not possible since the reporting is done based on a java method Current thread () which has a set time to control update.
2. Only one recipient can receive the SMS alerts. The system places the assumption that an organization has a single security administrator who can perform the necessary action(s) when alerted, if not available then contact a second person to perform the required actions.
3. The Web Server is locally hosted for the purpose of the project demonstration however the assumption that the server is public can be realized by having a public IP address to host it as a public domain.

5.3 Limitations

The Internet Engineering Task Force (IETF) which is in charge of developing new Internet standards is trying to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to management systems which may need to interact with them. Intrusion Detection Exchange Protocol (IDXP), an application-level protocol for exchanging data between intrusion detection entities and Intrusion Detection Message Exchange Format (IDMEF) are two frameworks that are currently being developed. The failure of possible standards in defining data formats and exchange procedures has resulted in practical limitations in regard to this project they include:-

1. The system has several areas that limit the efficiency of event to log generation. The batch file used can only generate a parsed text file and thus a great deal of complex coding is needed to deal the issues of automated recovery of errors or failures.
2. The SMSLib tools make use GSM networks to send the short message service (SMS's) to administrators. The default gateway of the system is based on the GSM network modem; the system has not been tested in a local area environment where the setting for short messaging service server will differ especially in the area of sending messages to registered mobile server users.
3. The mercury mail used in XAMMP is local; users using general and corporate mail accounts available in the web cannot receive the messages since most corporate mail servers don't receive mails from non-registered domains. However this can be solved by liaising with internet service providers in provision of domain registration services that can facilitate the sending of the messages
4. The system has only been tested on Windows Operating system environment. The SMSLib tools in use can also be implemented in a Unix or Linux operating system; however, proper configuration is necessary in-order to output the desired results.

5.4 Recommendations

The use of network monitoring and reporting tools and related technologies is on the rise. As awareness and interest in network monitoring and reporting tools increases so will its use in an organization as a security tool. The scope captures development of network monitoring and reporting tools which facilitate the different aspects like logging, tracing back to the source etc. System modules for sophisticated keystroke logging, better filtering tools and utilities to capture encrypted traffic are a few things that could be worked on. One can even consider an out-of-the-box network monitoring and reporting tools.

5.5 Impact of Future Technologies

5.5.1 IP Version-6

IP version-6 has been designed with strong emphasis on security. Many inherent security deficiencies in IPv4 have been addressed in IPV6. Another important addition is the authentication header. This header ensures data integrity thus eliminating IP spoofing which was an unavoidable problem in IPv4. The header also proposes a reliable authentication mechanism. Another security feature is the "Encapsulating Security Payload" header which provides confidentiality to the encapsulated payload. IPv6 promises a lot but it has to be tested on a large scale. The implications of IPv6 to existing intrusion detection systems and also to existing attack techniques will be an interesting research topic in the coming years.

5.5.2 Encryption

The use of encryption in technologies like SSL (secure socket layer) or SSH (secure shell) protocol add a new dimension and a new challenge to intrusion detection. Encrypted data allows data to be transmitted securely between two end points and hence adds to security. But it adversely affects the ability of signature-based NIDS to detect malicious packets. Also encrypted packets cannot be used to recreate a session. A NIDS can detect intrusions at different TCP/IP layers like the IP, ICMP or TCP. Protocols like SSH and SSL fall under top layer(application layer) of the TCP/IP suite. In order for a NIDS to do proper analysis and detect attacks it must be able to understand these protocols and their working. The solutions to these challenges are varied and not clearly understood.

5.5.3 Wireless Technologies

Wireless technologies have opened up a whole new security threat. Wireless is the direction in which computers especially laptops, palmtops and other hand-held's are heading. The intruder can now compromise your system from your parking garage or a palmtop hidden in his backpack. At the onset this appears disastrous to security but there are quite a few solutions already available. Techniques like wired equivalency privacy (WEP), Extensible Authentication Protocol (EAP) have been developed and are subject to evaluations and studies. Many vendors like Cisco have also introduced proprietary technologies. For example, Cisco's Lightweight Extensible Authentication Protocol (LEAP) algorithm provides user-based centralized authentication. All this means that there will be more to do in the intrusion detection front, especially the handling of wireless physical layer. Wireless network monitoring and reporting tools will be another interesting proposition. Wireless has a long way to go in terms of standards and security measures and hence provides an interesting area for research.

5.6 Conclusions

The result from the developed prototype provides adequate and sound information as per the stated objectives which provides basis for the conclusion. The System provides a working application development tool (NIMRUES) that can be deployed and make use of the existing web and mobile applications.

This will largely ease the needs of security administrators in the area of real time monitoring and reporting of security event error occurrences in Windows server and client operating systems.

Chapter 6

6 REFERENCES AND BIBLIOGRAPHY

[1]. Berst, J.; (1998), *The Biggest Threat to Your Network's Security.* (It Isn't What You Think). Ziff Davis Network (ZDNet). [On-Line]. Available
http://www.zdnet.com/anchordesk/story/story_1959.html
[Last Accessed on January 2011]

[2]. Shipley, G.; (1999), *Defending the Enterprise.* Network Computing. [On-Line]. Available http://www.nwc.com/1010/1010f11.html
[Last Accessed on January 2011]

[3]. Shipley, G.; (1999), *The State of Security 2000, Intrusion Detection Systems.* Network Computing. [On-Line]. Available

http://www.nwc.com/1020/1020f25.html
[Last Accessed on January 2011]

[4]. Saadat M.; (2002), *Network Security Principles and Practice*, Publisher: Network General, 1st edition;

[5]. Knowles, A.; (1996), *The Enemy Within. CIO Magazine.* [On-Line]. Available
http://www.cio.com/archive/061596_security_print.html
[Last Accessed on January 2011]

[6]. SANS (System Administration, Networking, and Security) Institute (2000), *Intrusion Detection Frequently Asked Questions.* [On-Line]. Available
http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm.

[Last Accessed on January 2011]

[7]. SANS (System Administration, Networking, and Security) Institute. (2001), *The 7 Top Management Errors that Lead to Computer Security Vulnerabilities.* [On-Line]. Available http://www.sans.org/newlook/resources/errors.htm
[Last Accessed on March 2011]

[8]. Radcliff, D.; (1998), *The Danger Within. InfoWorld Electric.* [On-Line]. Available
http://www.infoworld.com/cgi-bin/displayShow.pl%3F980429security.htm

[Last Accessed on March 2011]

[9]. Kontovasilis K., Kormentzas G., Mitrou N., Soldato J. s and Vayias E.; vol. 24 (2001), '*A Framework for Designing ATM Network Management Systems by way of Abstract*

Information Models and Distributed Object Architectures', in Computer Communications, Elsevier, The Netherlands, pp.641-653.

[10]. Strauss F.; (Copyright (c) 1999-2008) *LIBSMI, A library to access SMI MIB information*, [On-Line]. Available (http://www.ibr.cs.tu-bs.de/projects/libsmi/)

[Last Accessed on March 2011]

[11]. Cisco Systems, Inc. (2002), *"Cisco's PIX Firewall Series and Stateful Firewall Security."* Accessed URL: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.pdf. [Last Accessed on June 2011]

[12]. Zwicky, E. D., Cooper, S., and Chapman, D. B.; (2000), *Building Internet Firewalls,* 2nd Edition. O'Reilly & Associates, 101 Morris St, Sebastopol, CA 95472 USA.

[13]. Yavwa, Y.; (2000), *The firewall technology.* Whitepaper, available at: http://www.cs.uct.ac.za/courses/CS400W/NIS/resources.html [Last Accessed on June 2011]

[14]. NFR, (2002) NFR Network Intrusion Detection [Online], Available URL: http://www.nfr.com/products/NID/features.html.[Last Accessed on June 2011]

[15]. Higgins, H.; (1999), *"Corporate system security: towards an integrated management*

Approach", Information Management & Computer Security, 7/5, pp. 217-22

[16]. Debar, H. & Wespi, A. (2001), *"Aggregation and Correlation of Intrusion-Detection Alerts"*, Proceedings of RAID 2001 Fourth International Symposium on Recent Advances in Intrusion Detection, Davis, CA, USA, pp. 85-103 [Online], Available: http://www.docshow.net, [Last Accessed on June 2011]

[17]. Srisuresh P., Holdrege M.; (1999), *"IP Network Address Translator (NAT) Terminology and Considerations"*, draft-ietf-nat-terminology-01.txt.

[18]. Suri, S. and Varghese, G. (2002). *Packet filtering in high speed networks. In Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'99).* SIAM, 3600 University City Science Center, Philadelphia available at: http://siesta.cs.wustl.edu/~suri/psdir/soda_filter.ps [Last Accessed on June 2011]

[19]. Thomas, K.; (2006), *"A proxy server helps speed up Internet access by storing frequently accessed pages"* Beginning Ubuntu Linux: From Novice to Professional.

[20]. Microsoft Windows XP Service Pack 3 *"Deploying Windows Firewall Settings",* Microsoft Download Center Available URL:http://go.microsoft.com/fwlink/?LinkId=23277
[Last Accessed on June 2011]

[21]. *Introduction to Windows 2000 Group Policy.* Available URL: http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicyintro.as[Last Accessed on March 2011]

[22]. *Step-by-Step Guide to Understanding the Group Policy Feature Set.* Available URL: http://www.microsoft.com/windows2000/techinfo/planning/management/groupsteps.asp
[Last Accessed on June 2011]

[23]. *Securing your Microsoft IIS Web.*
Server http://www.its.uiowa.edu/cio/itsecurity/bestprac/iis.htm

[Last Accessed on June 2011]

[24]. *Maintaining IIS Security Available* URL:
http://wwwtus.csx.cam.ac.uk/pc_support/security/iismaintain.html
[Last Accessed on June 2011]

[25]. *NCSA*: Available URL:
http://publib.boulder.ibm.com/tividd/td/ITWSA/ITWSA_info45/en_US/HTML/guide/c-logs.html
[Last Accessed on June 2011]

[26]. Luotonen A.; (1995), *The Common Logfile Format*, Luotonen95, Available URL:
http://www.w3.org/pub/WWW/Daemon/User/Config/Logging.html

[Last Accessed on June 2011]

[27]. ISS X-Force (2005), *iPlanet (Sun ONE) Web Server chunked transfer encoding heap buffer overflow.* Available URL:
http://www.iss.net/security_center/static/9799.php.
[Last Accessed on June 2011]

[28]. Frisch A.; (1995), *Introduction to syslog, and tcp wrappers.* Essential System Administration (2nd Edition), Available URL:
http://www.unix.org.ua/orelly/perl/sysadmin/ch09_02.html

[Last Accessed on June 2011]

[29]. Philippe L. B.; (1998), *Win32 EventLog and other Win32 packages.* Accessed URL:
http://www.le-berre.com/
[Last Accessed on June 2011]

[30]. James D.; (1998), *"Windows NT Event Logging".*

[31]. Pethia, R., Paller, R. & Spafford, G.; (2000), *Consensus Roadmap for Defeating Distributed Denial of Service Attacks* [Online],
Available: http://www.sans.org/ddos_roadmap.htm,
[Last Accessed on March 2011]

[32]. Intrusion, Inc.; (2001), *Applying Network Intrusion Detection Under HIPAA* [Online],
Available: http://www.intrusion.com/, [Last Accessed on March 2011]

[33]. The SANS Institute (2000), *Top Twenty Computer Vulnerabilities in October of 2001*
Available http://www.sans.org/top20/2000/
[Last Accessed on March 2011]

[34]. Vigna, G. & Kemmerer, R.; (1999), *NetSTAT – A Network-Based Intrusion Detection System* [Online], Available: http://www.cs.ucsb.edu/~rsg/papers.html,
[Last Accessed on March 2011]

[35]. Vigna, G. & Kemmerer R,; (2001), *SecureNet Series Network Intrusion Detection System /*Online], Available: https://www.intrusion.com/products/downloads/nids_01-0716.pdf,

[Last Accessed on March 2011]

[36]. Cunningham R. K., Lippmann R. P., Fried D. J., Garfinkel S. L., Graf I., Kendall K. R., Webster S. E., Wyschogrod D., Zissman M. A.; (1991) "*Evaluating Intrusion Detection Systems without Attacking your Friends: The 1998 DARPA Intrusion Detection Evaluation*," SANS.

[37]. Roberts-Witt, S.; (1999), *Intrusion Detection: Patrol Network Traffic. PC Magazine.* [On-Line]. Available:
http://www.zdnet.com/products/stories/reviews/0,4161,410490,00.html
[Last Accessed on April 2011]

[38]. Houle, K. & Weaver, G.; (2001), *Trends in Denial of Service Attack Technology* [Online],
Available: http://www.cert.org, [Last Accessed on April 2011]

[39]. Sterne, D., Djahandari, K., Wilson, B., Babson, B., Schnackenberg, D., Holliday, H. & Reid, T.; (2001), *'Autonomic Response to Distributed Denial of Service Attacks'*, *Proceedings of RAID 2001 Fourth International Symposium on Recent Advances in Intrusion Detection*, Davis, CA, USA, pp. 134-49 - - [Online], Available: http://www.docshow.net,
[Last Accessed on April 2011]

[40]. Schuba C. L., Krsul I.V., Makus G. K., Spafford E.H., Sundaram A., Zamboni D.; (1996), *Analysis of a Denial of Service Attack on TCP*, Purdue University, West Lafayette, IN,

[41]. Illena A.; (2001), *"Computer Forensics, Tracking Down the Clues"*, Security Magazine

[42]. Matt V.; (2001), *"I.T. Autopsy"*, CIO Magazine.

[43]. Thomas R.; (2003), CISSP, "*Evidence Seizure Methodology for Computer Forensics"* Available: URL: http://www.crazytrain.com/seizure.html

[Last Accessed on March 2011]

[44]. New Technologies Inc.; (2003), *"Computer Evidence Processing Steps"* Available: URL: http://www.forensics-intl.com/evidguid.html

[Last Accessed on March 2011]

[45]. *Using MonitorMagic Policies, Monitors, Rules and Alarm actions.* Available URL: http://www.tools4ever.com/resources/pdf/monitormagic/chapter-06-using-monitormagic.pdf [Last Accessed on June 2011]

[46]. Sterne, D., Djahandari, K., Wilson, B., Babson, B., Schnackenberg, D.; (2005). *An introduction to the Generic Log Adapter*, Accessed URL: http://dev.eclipse.org/viewcvs/indextools.cgi/hyadeshome/docs/gla/GLA_Intro/GLA_Intro.viewlet/GLA_Intro_viewlet_swf.html
[Last Accessed on June 2011]

[47]. Balan S.; (2004), *Improve the run-time performance of the Generic Log Adapter, Part 1: A guide to writing efficient rule sets, developerWorks*, Accessed URL: http://www-128.ibm.com/developerworks/autonomic/library/ac-savvy/index.html
[Last Accessed on June 2011]

[48]. David B.; (2005), *Standardize messages with the Common Base Event model, developerWorks*, Accessed URL:
http://www128.ibm.com/developerworks/autonomic/library/a

c-cbe1/index.html.
[Last Accessed on June 2011]

[49]. Rao, C.H., Chang, D.-F., and Lin, Y.-B.;(2001*). "iSMS: An Integration Platform for Short Message Service and IP Networks,"* IEEE Network, volume 15, number 2, pages 48-55,

[50]. Lin, Y.-B., Haung, Y.-R., Chen, Y.-K., and Chlamtac, I., (2001) *"Mobility Management: From GPRS to UMT.,"* Wireless Communications and'Mobile Computing, volume 1, number 4, pages 339-360.

[51]. Y.-R. Haung and Yi-Bing L,; (2002), *"A Software Architecture for GPRS Session Management,"* Wireless Communication and Mobile Computing, volume 2, number 2, pages 151-167.

[52]. Mobile Data Association, (2003). *Text messaging total tops 16.8 billion for 2002*, available: http://www.mdamobiledata.org/resource/hottopics/smsjan03.asp.[Last accessed on June 2011]

[53]. Li, J., Hong, Y. (2010), *Webservice SMS delivery platform based on the design and implementation [J] information technology and information,* (2) : 43-46.

[54]. Fan, J. (2010), *SMS-based network failure alarm system design and implementation* [J]. China Education Information: Higher Vocational Education, , (11) : 53-55.

[55]. Short, M.; (2002), *New Mobile Data Services and Growth* [On-Line]. Available http://www.touchbriefings.com/pdf/20/wire02_p_SHORT.PDF
[Last accessed on June 2011]

[56]. Taylor-Powell E,. Steele S,. (1996). *Collecting Evaluation Data*: Direct Observation. University of Wisconsin Cooperative Extension Available at http://learningstore.uwex.edu/pdf/G3658-5.PDF arningstore.uwex.edu/pdf/G3658-5.PDF

[57]. Lincoln, Y.S., and Guba, E.G. (1985). *Naturalistic Inquiry.* Beverly Hills, CA: Sage.

[58]. Fetterman, D.M. (1989). *Step by Step. Applied Social Research Methods Series*, Ethnography: Vol. 17. Newbury Park, CA: Sage.

APPENDIX 1: DARPA 1999 EVALUATION

DARPA 1999 OFF-LINE INTRUSION DETECTION EVALUATION

(Abstract)

Eight sites participated in the second DARPA off-line intrusion detection evaluation in 1999. Three weeks of training and two weeks of test data were generated on a test bed that emulates a small government site. More than 200 instances of 58 attack types were launched against victim UNIX and Windows NT hosts. False alarm rates were low (less than 10 per day). Best detection was provided by network-based systems for old probe and old denial-of-service (DoS) attacks and by host-based systems for Solaris user-to-root (U2R) attacks. Best overall performance would have been provided by a combined system that used both host- and network-based intrusion detection. Detection accuracy was poor for previously unseen new, stealthy, and Windows NT attacks. Ten of the 58 attack types were completely missed by all systems. Systems missed attacks because protocols and TCP services were not analyzed at all or to the depth required, because signatures for old attacks did not generalize to new attacks, and because auditing was not available on all hosts.

(Lippman, Haines et al. 2000)

APPENDIX 2: MICROSOFT SECURITY TOOLS

Microsoft has released the following tools as part of their security push after the Nimda and Code Red incidents:

URLScan – validates each request made to a Web server (Microsoft 2001)

Microsoft Personal Security Advisor (MPSA) - scans a Windows NT or Windows 2000 computer remotely for vulnerabilities (Microsoft 2001a)

Microsoft Network Security Hotfix Checker (Hfnetchk) - checks the installation status of the Windows server and produces a list of software patches to be applied (Microsoft 2001b).

Both MPSA and Hfnetchk have been produced for Microsoft by Shavlik Technologies, a company specialising in computer security products. Shavlik Technologies markets the advanced versions of these products

(Shavlik 2001).

APPENDIX 3: SECURENET PRO OVERVIEW

The following information has been extracted from Intrusion, Inc.'s web site www.intrusion.com.

SecureNet Pro manages over 400 signatures are context analysis scripts. It contains a customisable scripting system and an option to create 'string matching (network grep) signatures'. (Intrusion Inc 2001a)

Intrusion, Inc. claims that the SecureNet Pro software handles 100% packet reassembly and TCP/IP reconstruction. The system is said to handle network traffic up to 700Mbps with 98% attack detection rate 'with randomly sized synthetic traffic, from 64 to 1500 bytes'.

The system runs on a hardened (where vulnerable services have been removed) RedHat Linux 6.2 operating system, and on a variety of rack-mountable appliances. The Gig model of the system connects through a fibre optic connector to a Gigabit backbone. It has also a 10/100 Mb connection from the sensors and the manager console inside the network. The PDS 5000 and 2000 models cover the 100Mbps networks.

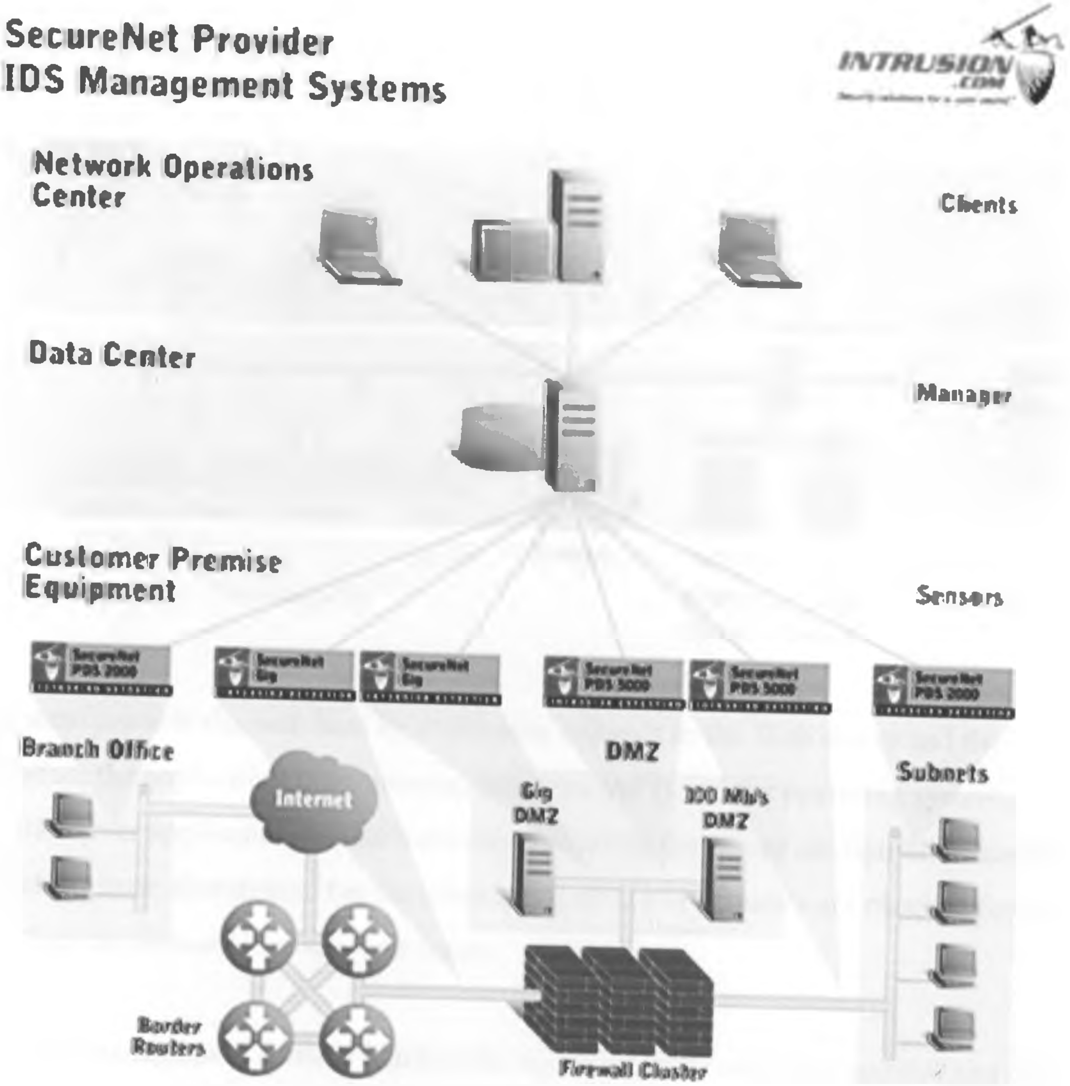
For security reasons the appliances do not usually have keyboard, video or mouse (KVM). The SecureNet Pro system supports notification by email or pager through SMTP messages, and SNMP alerting.

SecureNet Provider is a three-tier architecture for centralised monitoring and reporting, as shown on the following page:

Client workstations in the Network Management Centre

Manager, including Microsoft SQL 2000 database

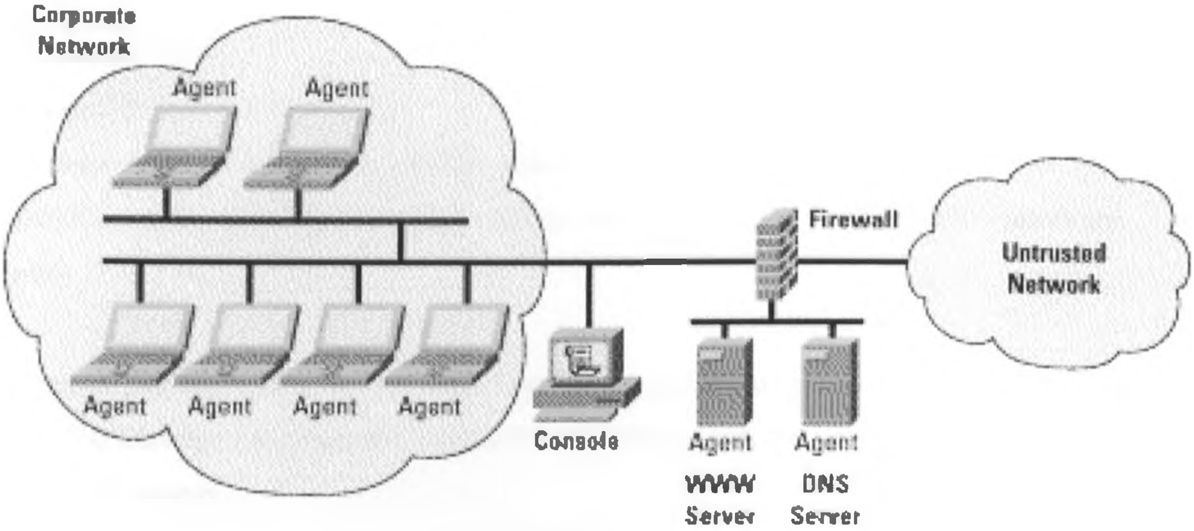
Sensors (SecureNet PDS Gig/5000/2000 or SecureNet Pro software)



(www.intrusion.com)

APPENDIX 4: CISCO PRODUCT LINE

Cisco IDS Host Sensor Web Server Edition



The system protects the web host by evaluating requests to the Web server and the application, the application programming interface (API) and the operating system. On one hand, the server application and its resources, including the server configuration and the data, are shielded from alterations. On the other hand, all HTTP requests are checked for validity before they are forwarded to the web server.

The central management console handles the signature, code and rules updates and reporting. Otherwise the agents are self-contained and independent from the console.
The signature database can be customised, to eliminate false positives.

All the communication between the server agents and the Console is Triple-DES encrypted.

Security events generate email and pager messages. The system provides SMTP data for integration with network management systems.

(Cisco 2001)

Cisco Secure Intrusion Detection Director for Unix

The system can provide a user defined response to an attack. The options are:

- generate an alarm
- generate IP session logs
- reset the TCP/IP connections after the attack has begun
- shun the attack, assuming particular models of Cisco Catalyst 5000 or 6000 routers are used

The Director running under the Solaris 2.8 operating system communicates securely with the agents. The Director can maintain a database and it links with the HP OpenView network management system.

(Cisco 2001a)

Cisco Secure Policy Manager

Cisco Secure Policy Manager (CSPM) runs in a central location in the network and distributes the security policies to different devices in the network, including Cisco routers, firewalls, VPN devices and IDS.

The same high level policies, defined using a visual interface, can be distributed to multiple devices. The system provides event notification, monitoring and Web-based reporting.

Cisco Catalyst 6000 Intrusion Detection System Module

Rather than using the Switched Port Analyzer (SPAN) ports connected to external sensors for monitoring the switched traffic, it is possible to add a specialised IDS module into a slot in the Cisco 6000 switch. The device does not affect the processing speed or path of the switch because it works independently using a copy of the actual packets.

The device monitors a 100Mbps switch, processing 'approximately 47,000 packets per second, with a new flow arrival rate of 1000 per second'.

The product integrates with the Cisco Secure Policy Manager and the Cisco Secure Intrusion Detection Director.