SECURITY AND CONTROL IN AN INTERNET ENVIRONMENT WITH SPECIFIC REFERENCE TO PRIVATENET SYSTEM

BY

MALINDI NEMBAMBULA

SHORT DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

THE DEGREE OF

MASTER OF COMMERCE

IN

COMPUTER AUDITING

IN THE

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

AT THE

RAND AFRIKAANS UNIVERSITY

STUDY LEADER: PROF. ANTON DU TOIT

JOHANNESBURG
NOVEMBER 1997

DECLARATION

I declare that this shortt dissertation, hereby submitted to the Rand Afrikaans University for a degree of Master of Commerce, except to the extent acknowledged in the text, is my unaided work and has not been submitted previously for any degree to any other university.

MALINDI NEMBAMBULA

ACKNOWLEDGMENTS

I would like to thank Professor WH Boshoff for his invaluable ideas during the conceptual phase of this short dissertation, and for the excellent foundation during the formal study towards the M.COM. Also, Professor Anton Du Toit for his comments on the initial drafts of the first two chapters.

A special thank you to Unarine Nembambula for the typing, and her patience during the incessant revisions and re-types, Franckie Venter for the proof-reading.

I would especially like to thank my family and friends for the constant support throughout my academic career.

A big thank you to my husband, Nelson, and my children, Unarine, Udovhuya, and Zwikhodo, for being so understanding during the long days and nights they spent alone while I was locked up in my study-room - patience rewarded.

Lastly but not least, all the glory to the Almighty God who made it possible for me to go through my work during the two years study period.

INDEX

OPSOMMING

SEKURITEIT EN BEHEER IN DIE INTERNET OMGEWING MET

SPESIFIEKE VERWYSING NA DIE PRIVATENET STELSEL

DEUR

MALINDI NEMBAMBULA

OPSOMMING VIR DIE SKRIPSIE INGEDIEN VIR DIE GRAAD

MAGISTER COMMERCII IN REKENAAROUDITERING

IN DIE FAKULTEIT EKONOMIESE EN BESTUURWETENSKAPPE

AAN DIE RANDSE AFRIKAANSE UNIVERSITEIT

STUDIELEIER: PROF A DU TOIT

JOHANNESBURG
NOVEMBER 1997

Die doel met die opsomming is om die agtergrond, metodiek en gevolgtrekkings van die navorsing oor die sekuriteit en beheer in die Internet omgewing met spesifieke verwysing na die PrivateNet stelsel weer te gee. Hierdie opsomming is onder die volgende hoofde uiteengesit:

1. PROBLEEMOMSKRYWING EN DOEL VAN DIE NAVORSING
2. NAVORSINGMETODOLOGIE
3. OMVANG EN BEPERKINGS
4. RESULTATE
5. GEVOLGTREKKINGS

1. PROBLEEMSTELLING EN DOEL VAN DIE NAVORSING

Per definisie is die publieke Internet 'n reuse netwerk wat bestaan uit duisende klein tot groot netwerke. Dit is belangrik om te besef dat die Internet beskou word as 'n publieke netwerk, soortgelyk aan die publieke telefoonnetwerk, omdat dit maklik toeganklik is vir die algemene publiek. Alhoewel dit maklik is om te gebruik en toegang gee tot 'n onbeperkte hoeveelheid inligting, veroorsaak dit geweldige uitdagings om die inligting sekuriteit doelwitte van vertroulikheid, integriteit, toeganklikheid en rekenskap te bereik.

Die inligting sekuriteit doelwitte van vertroulikheid, integriteit, toeganklikheid en rekenskap is blootgestel aan risiko vanweë die verhoogde moontlikheid dat wanneer 'n maatskappy gekoppel word aan die Internet enige een van die honderde duisende Internet gebruikers die Internet dienste (m.a.w. telnet, leêr oordrag protokol, wêreld wye netwerk ens.) wat die organisasie beskikbaar stel kan gebruik om hulle privaat netwerk aan te val en ongemagtigde toegang te verkry tot die organisasie se rekenaar hulpbronne en inligting. Hierdie aanvalle kan daartoe lei dat vertroulike en beperkte inligting en rekenaar hulpbronne deur ongemagtigde persone beheer word. Die persone kan die vertroulike of beperkte inligting en rekenaar hulpbronne wysig of saboteer.

Nog 'n risiko vir die maatskappy ten opsigte van die inligtingsekuriteitdoelwitte bestaan omdat die Internet verkeer van die organisasie, bykans altyd, via 'n ander netwerk vloei waaroor die organisasie nie beheer het nie. Die risiko word verhoog deur die maklike toegang wat ongemagtigde persone kan verkry tot netwerk verkeer deur gebruik te maak van "snooping", "hijacking", en "spoofing". "Snooping" vind plaas wanneer 'n "data scope", wat 'n rekenaar mag wees met "snooping" sagteware of 'n algemene stuk netwerk analiserings hardeware, geplaas word op 'n gedeelte van die netwerk en inligting vertoon soos dit deur die netwerk versend word. "Hijacking", aan die anderkant, vind plaas wanneer Internet verkeer gesteel word deur 'n bedrieglike gasheer op dieselfde netwerk as die doelwit gasheer. "Spoofing" is soortgelyk aan "hijacking" behalwe dat 'n gasheer optree as 'n nabotser van 'n ander gasheer op dieselfde netwerk en verkeer steel wat bedoel is vir 'n doelwitgasheer en terselfdetyd die doelwitgasheer verwar deur vervalste inligting te stuur in die plek van die gesteelde inligting. Die metodes vir "snooping", "hijacking" en "spoofing" is veelsoortig en kan taamlik tegnies wees maar hulle is algemeen en hou gevaar in vir inigtingsekuriteitsdoelwitte.

Die sekuritietsdoelwit van toeganklikheid is ook blootgestel aan risiko vanweë verhoogde Internet verkeersvlakke en weiering-van-diens aanvalle soos die berugte Internet wurm wat veroorsaak het dat honderde Internet gashere tot stilstand gekom het vir etlike ure.

Die Internet is egter uiteraard nie veilig nie en sal uiteraard ook nie op sy beste presteer nie. Daar is dus 'n behoefte om die Internet te beveilig en meer spesifiek, vir die toepassing van PrivateNet stelsel tegnologie toe te pas.

Die doel van die kort skripsie is drieledig:

a) om die rekenaar ouditeur te help om die risiko's vir inligtingsekuriteit wat verband hou met die klient se gebruik van die Internet te verstaan;

b) om die vermoë van die funksies van die PrivateNet stelsel om die sekuriteitsdoelwitte van toeganklikheid, vertroulikheid, rekenskap en integriteit aan te spreek, te evalueer;.en

c) om inligtingsekuriteitsbestuurders te help om gebiede te identifiseer waar sekuriteit verhoog moet word in die Internet omgewing.

2. NAVORSINGSMETODOLOGIE

'n Literatuurstudie is gedoen van bestande gesaghebbende en ander literatuur, so wel as samesprekings met persone met tegniese kennis van Internet sekuriteit. Met al die inligting wat verkry is deur die literatuurstudie is die doelwit van Internet sekuriteit met spesifieke verwysing na die PrivateNet stelsel bereik.

3. OMVANG EN BEPERKINGS

Hierdie skripsie fokus op Internet sekuriteit met spesifieke verwysing na die PrivateNet stelsel. Alhoewel hierdie skripsie gemik is op 'n spesifieke omgewing, is dit bellangrik om daar op te let. dat dit slegs die toepassing van 'n model op die omgewing is. Dit bewys dus nie noodwendig 'n universele toepaslikheid van die model nie, maar dui op die belangrikheid van die PrivateNet stelsel vir 'n Internet omgewing se sekuriteit.

Sekere uitsuitings geld ten opsigte van die skripsie:

a) Die verskeie tipes van keerwalle word ge ingnoreer omdat die doelwit is om die vermoë van die PrivateNet stesel-tegnologie om die inligtingsekuriteitsdoel witte te bereik in 'n Internet omgewing, te evalueer.

b) Ander keerwalle is nie in detail behandel nie, alhoewel daar kortliks na hulle verwys is ter wille van die voolledigheid van die skripsie.

c) Ander vraagstukke wat nie 'n direkte invloed op die stelsel het nie (byvoorbeeld die "hacker's workbench", Internet bestuur en moniteringsinstrumente) is geignoreer.

d) 'n Omvattende tegniese ouditprogram vir evaluering van die sekuriteit en be heer in 'n Internet omgewing is geignoreer.

4. RESULTATE

'n Internet sekuriteitsmodel is ontwikkel uit die studie. Die Internet seuriteitstruktuur bestaan uit drie vlakke van sekuriteit, naamlik:

4.1 Netwerksekuriteit
4.2 Gasheersekuriteit
4.3 Kontrolebeleid en prosedure

4.1 Netwerksekuriteit

Netwerksekuriteit bestaan uit die sekuriteit van en beheer oor die verbinding en vloei van inligting na en van ander gashere, beide binne en buite die organisasie, asook sekuriteit in en kontrole oor netwerroetes en toepassings wat netwerk funksionaliteit het.

4.2 Gasheersekuriteit

Gasheersekuriteit bestaan uit sekuriteit van en beheer oor die bedryfstelsels van die rekenaars wat gekoppel is ann die netwerk. Dit is belangrik vir Internet sekuriteit omdat die sekuriteit van gasheer gebaseerde nerwerktoepassings afhang van die sekuriteit van die gasheerbedryfstelsel. 'n Sterk "firewall" kan die organisasie se privaat netwerk beskerm, maar 'n swak beveiligde gasheer stel die netwerk, ander gasheer en die "firewall" bloot.

4.3 Kontrolebeleid en-prosedures

Kontrolebeleid en-prosedures is bestuur gemagtigde beleid en prosedures wat in plek is om te verseker dat inligting en netwerkbates gebruik word in ooreenstemming met 'n organisasie se doelwitte. Beleid behoort werknemers se verantwoordelikhede te definieer, asok administratiewe en hulpbronbestuurbeleid, toepaslike gebruike van die Internet en beleid vir die hantering van beleidsoortredings. Geldigheid en integriteit word baie beinvloed deur die gebrek aan beleid en prosedures ten opgesigte van Internet verbinding in 'n organisasie.

5. GEVOLGTREKKINGS

Die hoofplrobleem wat geidentifiseer is, is die balans tussen die behoefte aan sekuriteit, die behoefte aan prestasie en die behoefte om koste te minimaliseer, oftewel die balans tusse doeltreffendheid, doelmatigheid en ekonomie van die Internet verbinding.

Samevattend kan gemeld word dat hierdie navorsing'n basis voorsien om die inligtingsekuriteitsrisko's betrokke by 'n Internet omgewing te verstaan, en die PrivateNet stelsel is suksevol toegepas om die sekuriteitsriskos aan te spreek.

Die nuwe model wat ontwikkel is, is gensins a plaasvervanger vir goeie Internet bestuursvaardighede nie, maar dit gaan die ouditeur help om die ouditprosedures te optimalisieer. Dit open dus nuwe velde vir akademiese navorsing op die gebied van Internet sekuriteitsoudit, soos die hersiening van die sekuriteit van die verskillende komponente van die Internet sekuriteitsbeheerstruktuur.

SYNOPSIS

1. PROBLEM DESCRIPTION AND OBJECTIVE OF THE RESEARCH

"For better for worse, most computer systems are not in that way today. Security is in general, a trade-off with convenience of remote access via networks to their computers. Inevitably, they suffer from some loss of security. It is the purpose of the research to discuss how Inter-networks connection could be secured." (Cheswick, 1994:3)

By definition, the public Internet is a giant network which is composed of thousands of small to large networks. It is important to realize that the Internet is considered a public network, similar to the public telephone network, because the general public has easy access to it. This is great for ease of use and accessibility of a virtually infinite amount of information, however it creates great challenges to achieving the information security objectives of confidentiality, integrity, availability, and accountability.

The confidentiality, integrity, availability, and accountability security objectives, are at risk due to the increased potential that, once connected to the Internet, any one of the hundreds of thousands of Internet users could use the Internet services offered by an organization (i.e. telnet, file transfer protocol, world wide web, etc.) to attack their private network and gain unauthorised access to computer resources and information. These attacks could result in confidential and restricted data and computer resources being controlled by unauthorised people, to the modification and sabotage of confidential and restricted data and computer resources.

Other major exposures to the information security objectives exist because an organisation's Internet traffic will, almost always, take a route on a network which the organisation has little or no control over. This risk is compounded by the ease of which network traffic may be accessed without authorisation through the tactics of

snooping, hijacking, and spoofing. Snooping occurs when a "data scope," which may be a computer with snooping software or a common piece of network analysing hardware, which is placed on a portion of a network and information is displayed as it is transmitted through the network. Hijacking, on the other hand, occurs when

Internet traffic is stolen by an imposing host on the same network as the target host. Spoofing, is similar to hijacking except that a host acts as an impostor of another host on the same network and steals traffic meant for a target host, at the same time confusing the target host by sending fake information in the place of the stolen information. The methods for snooping, hijacking, and spoofing are varied and can be quite technical but they are common and pose serious exposures to information security objectives.

The security objective of availability is also at risk due to increased Internet traffic levels, and denial-of-service attacks like the infamous Internet worm which caused hundreds of Internet hosts to grind to a halt for several hours.

However, Internet is not secure by default, nor will it perform at its best by default, thus there is a need for Internet to be secured, and more specifically for PrivateNet system technology to be applied.

The purpose of this short dissertation is threefold, namely:

a) To help the computer auditor to understand the information security risks associated with the client' use of the Internet;
b) To evaluate the capabilities of the features provided by the PrivateNet system in addressing the security objectives of availability, confidentiality, accountability and integrity in an Internet environment; and
c) To help the information security managers to identify the areas where security needs to be enhanced in the Internet environment.

2. RESEARCH METHODOLOGY

a) A literature survey has been done on existing authoritative textbooks and other literatures, as well as discussions with people with technical knowledge, on Internet security; and

b) With all the information obtained in the literature survey, the objective of Internet security with specific reference to PrivateNet system has been achieved.

3. SCOPE AND LIMITATIONS

This short dissertation focuses on the Internet security with specific reference to PrivateNet system.

Although this short dissertation is aimed at a specified environment, it is important to remember that it is merely the application of a model to the environment. This does not necessarily prove universal applicability of the model, but does demonstrate the relevance of PrivateNet system to an Internet environment security.

Certain exclusions apply to this short dissertation as follows:

a) The various types of firewalls are ignored as the objective is to evaluate the capability of the PrivateNet system technology to meet the information security objectives in an Internet environment;

b) Other firewalls have not been dealt with in detail, although they have been referred to, for the sake of the completeness of the short dissertation;

c) Issues which do not have a direct impact on the system (for example the hackers workbench, Internet management and monitoring tools) have been ignored; and

d) A comprehensive technical audit program for assessing the security & control over Internet environment has been ignored.

4. RESULTS AND CONCLUSION

An Internet security model has been developed as a result of the study. Internet security control structure consists of 3 levels of security, namely:

4.1 Network security

4.2 Host security

4.3 Control policies and procedures

4.1 Network security

Network security consists of security and control over the connections and information flow to and from other hosts, both internal and external to an organization, as well as security and control over network routing and applications that have networking functionality.

4.2 Host security

Host security consists of security and control over the operating systems of computers that are connected to a network. This is important to Internet security because the security of host based networking applications is reliant on the security of the host operating system. While a strong firewall may protect the organisation's private network, a poorly secured host exposes the network, other hosts and the firewall.

4.3 Control Policies and Procedures

Control Policies and Procedures are the management authorized policies and procedures in place to ensure that information and network assets are used in accordance with organizational goals. Policies should define employee responsibilities, administrative and resource management policies, appropriate uses of the Internet and policies for handling policy violations. Validity and integrity are greatly influenced by the lack of policies and procedures over Internet connection in an organisation.

5. CONCLUSION

The main problem identified is the balance between the need for security, the need for performance and the need to minimise cost or the balance between effectiveness, efficiency and economy of the Internet connection..

In summary, this research has provided a basis for understanding the information security risks involved in an Internet environment, and the PrivateNet system has been applied successfully in addressing the security risks raised.

The new model that has been developed, is not meant to be a replacement for good management skills, but it can assist the security manager in optimising his procedures.

It therefore opens new fields for academic research in the area of Internet security audit such as review of the security of the different components of the Internet security control structure.

CHAPTER 1

INTRODUCTION

CONTENTS PAGE

1.1 BACKGROUND

The Internet is a complex computer network, consisting of over 5 million computers and individuals in 144 countries offering a new set of opportunities and challenges to the commercial world. Suddenly, organisations can have a global presence free from geographical constraints; have access to information data-bases across the world; and form alliances quickly with others to exploit new lines of business.

"According to recent studies and current trends, the most common uses of the Internet include: electronic mail; information retrieval from the many organisations on the Internet; and access to computing power at other sites..." (Tzu, 1995:23).

Organisations can also provide their own services, such as: advertising and marketing applications; financial applications such as home banking; electronic sales for many diverse lines of products; customer support; and technical support and tracking.

The opportunities presented by the Internet have immense potential and can lead to significant business benefits.

But there are risks which can be grouped into four major areas:

- disclosure of information: where, intentionally or accidentally a company's information is divulged to others over the network, e.g. competitors, the press;

- unauthorised access: where unauthorised individuals - such as "hackers" or disgruntled employees - gain access to key systems and sensitive information;

- loss of information integrity: where data stored on a computer - or in transit, is amended, including alterations to files or business transactions; and

- denial of service: where the availability of computer systems and services such as electronic mail or a company database, is lost due to a computer or net work overload. (European Security Forum, 1996:11)

However, it is possible to reduce and manage the risks and thus use the Internet in a secure manner. This research to the Internet and Security sets out a series of fundamental steps that form the basis of an effective approach for securing against the threats presented above. It considers:

- the organisation's goals for use of the Internet;
- the need to assess the risks that will be faced and addressed in reaching those goals;
- the development of an Internet Policy, including the need for a set of intrusion response guidelines; and
- the identification (and subsequent installation) of appropriate technical solutions.

"Used properly, an Internet connection can provide an organisation with significant business opportunities. However, if security issues are not addressed properly, the Internet can expose an organisation to risks with potentially disastrous consequences (Leibowitz, 1995:123).

The auditor, specifically the computer auditor, is particularly equipped to assist management in assessing the extent of use of the Internet and security issues thereof. What makes the computer auditor particularly suitable for assessing the security of Internet connection, is the combined knowledge of the computers and of general business requirements and management needs. This does not mean that other

professionals, for example IT consultants, are not equipped to handle such an assessment. It just stresses the role which the computer auditor could play. In many cases, the auditor will be already familiar with the client's organisation and staff. The computer auditor would not have such a steep learning curve as someone who does not know the client. Staff members would also be more co-operative, because they know the auditor. Another factor is the independence of the auditor, which could be comforting to the staff involved. The ethical issues of the auditor's involvement are however not considered in this short dissertation, nor the responsibility of the auditor to ensure that he is equipped to perform such an audit.

1.2 PROBLEM DESCRIPTION

Over the past two years, use and awareness of the Internet has surged. However, being connected to the Internet is much like living in a rough neighbourhood. While many corporations and organisations need to be connected to the Internet, they also need to protect their trade secrets, innovative technologies, and private information. Stolen, altered, or deleted information can jeopardise the company's competitive edge in the market place, and vandalised or compromised data can be extremely expensive to replace. More and more people called "hackers" or "crackers" are breaking into private networks of corporate America, resulting in losses of billions of dollars (European Security Forum, 1996:5).

An increasing number of organisations are choosing to protect themselves from such intruders by erecting a security barrier, known as a firewall, between their private networks and the Internet. A firewall, when correctly implemented, enforces an organisation's rule or policies for access to and from the Internet (Blankley et.al 1996:35).

In addition, many organisations are now beginning to install firewalls inside their private networks, realising that while intruders from the Internet are getting most of

the press, greater threats can come from inside the organisation, from disgruntled employees, for example. Departmental firewalls make it possible to contain some of these threats without rendering the network useless (European Security Forum, 1996:19).

NEC Technologies Inc. now offers the PrivateNet system as both an Internet and a departmental Firewall server. It consists of the SocksPlus proxy, various application proxies for popular Internet protocols and encrypted communication between firewall servers. More than one PrivateNet system can be installed in a parallel configuration for high availability and/or high performance, and in a serial configuration supporting departmental firewalls and/or encrypted virtual private networks crossing the Internet.

The PrivateNet system provides the necessary framework to implement a corporate Internet security policy, allowing system administrators at an individual site to tailor the operation of the firewalls (through configuration files that govern the nature and volume of the traffic passing through the firewalls).

A common misconception which compounds the problem is that the mere purchase and implementation of the Internet security package, will provide all the answers to the Internet security problem. In fact:

"It should always be recognised that no matter how well .....any computer security package is installed, there will always be individuals within the organisation who must have access to the sensitive information.....there must be good.....controls..... to ensure that the objectives of the organisation are carried out successfully" (Decker, 1988:10)

1.3 OBJECTIVES OF THE RESEARCH

The objective of this short dissertation is threefold, namely:

- To help the computer auditor to understand the information security risks associated with the client's use of the Internet;
- To evaluate the capabilities of the features provided by the PrivateNet system in addressing the security objectives of availability, confidentiality, accountability and integrity in an Internet environment; and
- To help the information security managers to identify the areas where security needs to be enhanced in the Internet environment.

1.4 SCOPE, LIMITATIONS AND EXCLUSIONS

1.4.1 The predefined environment

This short dissertation is the culmination of two years of study towards a masters degree by the author. During this period, the Internet and security: a guide for business managers (European Security Forum, 1996) was used as a basis for building a security model for the Internet environment.

As stated earlier, due to the sophisticated nature and complexity of the predefined environment that we are dealing with, the use of extensive user controls is both inefficient and impractical.

Accordingly throughout this short dissertation, the concept of "using technology to control technology" is explored and user controls will only be investigated as compensating controls.

The concepts of user and integrity controls are well documented by the institutes governing the auditing standards, such as the American Institute of Certified Public

Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA) and the South African Institute of Chartered Accountants (SAICA).

1.4.2 Control Objectives

This research is driven by a number of what will be referred to as "information security control objectives" which need to be achieved in order to ensure adequate Internet security in the predefined environment.

On the basis that Internet security, in the context of a complex security installation, is of paramount importance, and that the need for Internet security is accepted, there is a need to develop a framework for the evaluation of controls in the predefined environment.

Information security controls generally have four main objectives: **confidentiality; integrity; availability; and accountability** (Blankley, et al. 1996:1):

- **Confidentiality** is protecting information from unauthorised disclosure;
- **Integrity** is protecting information from unauthorised modification;
- **Availability** is ensuring that data is accessible to all authorised users. It is also protecting the system from denial-of-service attacks that range from issuing system resources to crashing the system; and
- **Accountability** is identifying and holding a user accountable for actions that create, modify, provide access to, or disseminate information.

The purpose of Internet security is to ensure the information security objectives of confidentiality; integrity; availability; and accountability on the public Internet, and

on private hosts and networks that are connected to the public Internet. Internet security can be looked at as a control structure which has three main elements: **network security; host security; control policies and procedures.**

- **Network security**

  Network security consists of security and control over the connections and information flow to and from other hosts, both internal and external to an organisation, as well as security and control over network routing and applications that have networking functionality.

- **Host security**

  Host security consists of security and control over the operating systems of computers that are connected to a network. This is important to Internet security because the security of host based networking applications is reliant on the security of the host operating system. While a strong firewall may protect the organisation's private network, a poorly secured host exposes the network, other hosts and the firewall.

- **Control Policies and Procedures**

  Control Policies and Procedures are the management authorised policies and procedures in place to ensure that information and network assets are used in accordance with organisational goals. Policies should define employee responsibilities

1.4.3 Limitations and exclusions

Although this research is aimed at a specified environment, it is important to remember that it is merely the application of a model to the environment. This does

not necessarily prove universal applicability of the model, but does demonstrate the relevance of the PrivateNet system to an Internet environment security.

Certain exclusions apply to this short dissertation as follows:

a) The various types of firewalls are ignored as the objective is to evaluate the capability of the PrivateNet system features to meet the information security control objectives;
b) Other firewalls have not been dealt with in detail, although they have been referred to for the sake of the completeness of the short dissertation;
c) Issues which do not have a direct impact on the system (for example the hackers workbench, Internet management and monitoring tools) have been ignored;
d) It is not intended to provide a technical audit program for assessing the security and control over a client's Internet environment; and
e) Electronic Commerce has been excluded.

1.5 DEFINITIONS AND METHODOLOGY

1.5.1 Definitions

The basic definitions for Internet security and risk for the purpose of this short dissertation are not of any significance other than to provide comparative terminology and to enable the dissertation to concentrate on the relevant issues. As a result, more formal definitions are set out below.

1.5.1.1 Internet security

Internet security is any measure taken to safeguard against unauthorised access, disclosure of information, loss of information integrity and denial of service (Zwicky, 1996:15).

1.5.1.2 Risk

"...a risk is merely the degree of loss... a person, thing, event, or idea that poses some danger to an asset "(Stang, 1993:52).

1.5.1.3 Firewall

Firewalls are combinations of hardware and software that control information passing between two networks, such as a corporate network and Internet. They are generally considered to be the most effective security solution for a medium to a large size organisation (Blankley, et.al:1996:7).

1.5.1.4 Internet

The Internet in very simple terms is a network of networks. It is a collection of networks of thousands of organisations (governments, universities, businesses, etc.) all interconnected to form a global communications infrastructure, much in the same way that the individual LANs in corporate's offices are interconnected through the various office networks and form a WAN.

1.5.1.5 Audit objectives

The audit objectives are (Taylor 1994:23):

- **Completeness**
  To ensure that data is not lost erroneously or maliciously deleted.;

- **Accuracy**
  To ensure that data is reliable and not corrupt and that data is processed as it was intended;

- **Validity**

  To ensure that only authorised users, data and transactions are allowed; and

- **Integrity**

  To ensure that programs, data, files and transactions that are already resident in the system are not subject to:

  - unauthorised modifications /alterations/insertation **(validity);**
  - duplication **(validity);**
  - unauthorised deletion **(completeness);**
  - breaches of privacy **(confidentiality/validity);** and
  - errors **(accuracy).**

1.5.1.6 Proxy server

Porxy server is an application that mediates traffic between a protected network and the Internet.

1.5.2 Methodology

The following methodology has been used:

a) A literature survey has been done of existing authoritative textbooks and other literatures, as well as discussions with people with technical knowledge on Internet security; and

b) With all the information obtained in the literature survey, the objective of Internet security with specific reference to the PrivateNet system has been achieved.

This short dissertation can be summarised as shown below. In this chapter, the need for Internet security and more specifically by means of PrivateNet system has been established.

In chapter 2, Internet security will be discussed. The Internet security control structure will be defined to help identify the risks involved in Internet connection. The Internet provides different levels of security control structures which have an impact on the PrivateNet system, therefore the different levels of security control structures will also be discussed. Chapter 3 will cover the PrivateNet system in sufficient detail for the purpose of this short dissertation. The application of the PrivateNet system's features to the Internet environment will be discussed in chapter 4 by way of matrices.

The model developed in chapter 4 will help the computer auditor in understanding the capability of the features of the PrivateNet system in addressing the security risks in Internet connection.

Finally chapter 5 will conclude the short dissertation, and indicate whether the objectives of this short dissertation have been met.

Structure of the short dissertation:

The structure of the short dissertation is as follows:

a) **Chapter 1**
Introduction;

b) **Chapter 2**
Literature survey of Internet security;

c) **Chapter 3**
Literature survey of the PrivateNet system;

d) **Chapter 4**
Application of the features of the PrivateNet system to an Internet environment; and

e) **Chapter 5**

Conclusion.

1.6 RESEARCH APPROACH

The approach followed in the short dissertation, is one of developing a security model for Internet connection, a model quite different from the traditional mainframe environment. The security model was developed out of existing models.

The approach to the development of the security model was to put users' needs opposite technology and computer personnel, with security management and Internet connection between them.

"A carefully designed and maintained Internet firewall can go a long way to reducing the risk that general attacks from public Internet users will occur" (Blankley, et al. 1996:56).

1.7 SUMMARY OF THE RESULTS AND CONCLUSION

The security model that has been developed has, as its starting point, the overall organisational framework for Internet security, whereby management lays down its Internet security expectations and implements them.

The main problem identified is the balance between the need for security, the need for performance, and the need to minimise cost (or the balance between effectiveness, efficiency and economy) of an Internet connection.

The implementation is carried out using the model developed in this short dissertation which has as its basis the Internet connection security models. By developing the matrices using predefined information security control objectives and the control features of the PrivateNet system, security management can evaluate whether its Internet security requirements have been achieved.

In summary this short dissertation has provided a basis of understanding the information security risks involved in Internet environment.

An evaluation and analysis of the control features of the PrivateNet system and audit issues was successfully carried out in our predefined environment, using the model developed in this short dissertation.

This analysis revealed that, features of the PrivateNet system can successfully address the security issues in the Internet environment. The environment was therefore deemed to have achieved information security control objectives.

In conclusion, the information security control objectives that we have developed have been effectively used to evaluate a specified environment. This short dissertation has opened the door for more short dissertation on the following topics:

a) Advantages and disadvantages of connecting to the Internet,
b) The implementation and maintenance of the PrivateNet system; and
c) The development of a comprehensive and technical audit program for assessing the security and control issues over a client's Internet environment.

The new model that has been developed is in no way a replacement for good Internet management skills. It is developed merely to help the auditor in understanding and evaluating the Internet security control risks better. It therefore opens the door for new fields of Internet security involvement by the auditor for potential academic short dissertation.

"The two main lessons to be learned are that:

- No firewall, however well it is implemented, is 100% secure, and, with enough determination and time investment by crackers, a firewall can and will be broken into; and
- Firewall technology improves all the time, and the tools that are used to penetrate them also improve. Providing a highly secure firewall is an arms race, but a firewall based on a restrictive technology at least has the chance of surviving the longest" (Blankley, 1996: 56).

CHAPTER 2

INTERNET CONNECTION SECURITY

CONTENTS PAGE

2.1 OBJECTIVES

In order to derive maximum benefit from the literature survey, the objectives were defined to allow comparative analysis of references and to facilitate synthesis or normalisation of security in Internet connection . The objectives are:

a) To obtain authoritative views on the models or processes involved in Internet security in order to create a security orientated model for the Internet environment;

b) To obtain authoritative views on risks/threats involved during Internet connection, in order to relate, or link them to the security orientated model for the Internet environment with specific reference to the PrivateNet system; and

c) To obtain the authoritative views on the PrivateNet system as a means of security in the Internet environment.

2.2 NATURE OF LITERATURE SURVEY

To ensure credibility and acceptance of the findings and proposals of this short dissertation, it is essential that the underlying concepts should be based on authoritative views and be generally accepted among computer auditing professionals and information security managers. Theory based on an individual's experience without taking generally accepted professional views into account may be subject to personal bias. Other factors which may introduce bias are the individual's background and the absence of formal short dissertation. To avoid these problems, references have been restricted to those published by auditors and audit firms and to authoritative technical books by computer experts.

The main categories of authors/publishers are:

- Coopers & Lybrand L.L.P, an international audit firm;
- The Institute of Internal Auditors;
- Boyd and Fraser publishing company;
- NEC Technologie Inc;
- European Security Forum;
- William Cheswick; and
- UNIX security symposium.

The reason for choosing these authors/publishers are the following:

- They represent most of the internationally accepted Internet Security Models;
- Their emphasis on auditor-related references provides more and better background for finding risks relevant to the auditor involved in auditing an Internet environment;
- They represent between them most of the internationally accepted views on the PrivateNet system firewall technology; and
- In total, they represent a properly balanced view of Internet security with specific reference to, and include latest technology of the PrivateNet system.

Few models of the Internet security could be found. There are, however, instances where Internet security and firewall technologies are discussed. These discussions are given, as well as figures representing the different views on the various levels of security.

Also, very few references to the PrivateNet system, could be found - there are few instances where the PrivateNet system is discussed. These discussions are given, as

well as figures representing the different views on the various levels of the PrivateNet system.

Therefore the literature survey had to include quite a substantial number of references, to be able to create a security model that can be a representative of all existing literature on the subject of the PrivateNet system as a means of security in the Internet environment.

2.3 SCOPE OF THE LITERATURE SURVEY

Existing models for Internet security and the PrivateNet system, have had to be surveyed to create a model for Internet security with specific reference to the PrivateNet system as a proxy based firewall technology.

Existing models have not been examined with the view of including every possible step, but to enable information security control objectives to be related to certain steps.

Although this short dissertation is aimed at a specified environment, it is as important to remember that it is merely the application of a model to the environment. This does not necessarily prove universal applicability of the model, but does demonstrate the relevance of a PrivateNet System to an Internet environment.

2.4 LIMITATIONS AND EXCLUSIONS OF THE LITERATURE SURVEY

To achieve the objectives of the literature survey, it has been necessary to examine and analyse the Internet environment and the PrivateNet system. Consequently the following limitations and exclusions have been placed on the scope of this survey:

- Only issues which deal with Internet security and the PrivateNet system have been included;

- Sections in the references which deal with non-related issues , have thus been excluded;
- The detailed implementation phase and the maintenance of the PrivateNet system is not emphasised;

- Inferior references and opinions of the individuals are ignored; and
- As this short dissertation principally deals with Internet security and the PrivateNet system, references to applications controls and risks and other integrity conrols have not been included.

A great deal of preparatory work has been done to ensure that the short dissertation is based on sound theory and limitations, and that the exclusions imposed do not detract from the overall objective of this chapter, in fact they enforce concentration on those issues which are relevant to the topic.

2.5 DEFINITIONS

2.5.1 Internet

The Internet in very simple terms, is a network of networks. It is a collection of networks of thousands of organisations (governments, universities, businesses, etc.) all interconnected to form a global communications infrastructure. Much in the same way that the individual LANs in the organisations are interconnected through the various office networks and form WAN (Blankley, et al. 1996:45).

There are many tools available for working on the Internet. Below is a brief description of each of the basic services (Blankley, et al. 1996:46-47):

2.5.1.1 Electronic mail

Electronic mail is a system that allows people to send and receive messages with their computers. The system might be on a company's own network, across the Internet or any combination.

2.5.1.2 File Transfer Protocol (FTP)

As the name implies, FTP is an application used to move files between computers. To use FTP you are generally required to login to a remote host. However, to provide access to public information, many organisations allow "anonymous" FTP. This means that when presented with a login prompt, remote users simply enter the word "anonymous" and are granted access to the FTP area on that host.

2.5.1.3 Gopher

Gopher Is a text-based menuing system used to browse information on the Internet. Many Internet host sites provide a Gopher menu to reference information available at that site, as well as provide links to other sites. While the Intemet Gopher is older technology and is rapidly being replaced by the World Wide Web, it provides a reliable back-up when a World Wide Web interface is not available.

2.5.2 Search tools

The Internet offers a tremendous amount of information in almost any subject conceivable. Unfortunately, because there is no single directory or index to point you to the appropriate resources, finding the information that you need can be a difficult task. Therefore, several search tools are available on the Internet to assist users with their quests, a few of these include:

- **Archie:** Allows users to search for specific **files** based on their names and descriptions.

- **Web Crawler:** Allows users to search for **pages** on the World Wide web based on keywords.

- **Wide Area Information Service (WAIS):** Allows users to search through indexed articles and databases on their **content**.

2.5.3 Telnet

Telnet is a protocol that allows users to remotely login to other computers on the Internet. When the connection is established, it allows you to function as if you are a local user.

2.5.4 Usenet Newsgroups

A usenet newsgroup is a bulletin board where people can read or post messages on specific topics. There are thousands of Usenet Newsgroups on the Internet and they come and go daily. Proper etiquette is recommended when responding to a Usenet Newsgroup.

2.5.5 World Wide Web

The world wide web is similar to the Internet Gopher in that it is primarily a tool for providing a menuing type interface for browsing information on the Internet. The web however, provides a more sophisticated GUI interface which allows the remote user to display and interact with graphics and multi-media objects.

2.6 BACKGROUND

References were briefly surveyed to identify a reference which represents the security of the Internet connection with specific reference to PrivateNet system, in as detailed a manner as possible, keeping in mind the objectives of this survey.

These references were used as a basis for developing a representative model, which combines PrivateNet system as well as security of the Internet connection.

2.7 INTERNET AND SECURITY

According to (Blankley, et al. 1996:24) the Internet is considered a public network, similar to the public telephone network, because the general public has easy access to it. This is great for ease of use and accessibility of a virtually infinite amount of information, however it creates great challenges to achieving the information security objectives of confidentiality, integrity, availability, and accountability.

The confidentiality, integrity, availability, and accountability security objectives are at risk (refer to table 2.1) due the increased potential that, once connected to the Internet, any one of the hundreds of thousands of Internet users could use the Internet services offered by an organisation (i.e. telnet, file transfer protocol, world wide web, etc.) to attack their private network and gain unauthorised access to computer resources and information. These attacks could result in confidential and restricted data and computer resources being controlled by unauthorised people, to the modification and sabotage of confidential and restricted data and computer resources.

Other major exposures to the information security objectives exist because an organisation's Internet traffic will, almost always, take a route on a network which the organisation has little or no control over. This risk is compounded by the ease of which network traffic may be accessed without authorisation through the tactics of snooping, hijacking, and spoofing. Snooping occurs when a "data scope," which may be a computer with snooping software or a common piece of network analysing hardware, is placed on a portion of a network and information is displayed as it is transmitted through the network. Hijacking, on the other hand, occurs when Internet traffic is stolen by an imposing host on the same network as the target host. Spoofing, is similar to hijacking except that a host acts as an impostor of another host on the

same network and steals traffic meant for a target host, at the same time confusing the target host by sending fake information in the place of the stolen information. The methods for snooping, hijacking, and spoofing are varied and can be quite technical but they are common and pose serious exposures to information security objectives.

The security of availability is also at risk due to increased Internet traffic levels, and denial-of-service attacks like the infamous Internet worm which caused hundreds of Internet hosts to grind to half for several hours (Blankley, et al. 1996).

Security Objectives	Exposures
Confidentiality	General attacks from the public Internet. Snooping, hijacking, and spoofing, of network traffic.
Integrity	General attacks from the public Internet. Hijacking, spoofing of network traffic.
Availability	General attacks from the public Internet. Hijacking and spoofing of network traffic. Denial of service attacks.
Accountability	General attacks from the public Internet. Hijacking and spoofing of network traffic that contains user authentication information.

Table 2.1: Internet security exposures (Blankley, et al. 1996:3).

"There is rarely a single solution that will meet all of an organisation's Internet security needs. A combination of a number of different technical approaches is likely to be needed to meet any large organisations needs." (Cronim, 1996:16)

2.8 CONNECTING TO THE INTERNET

Connecting to the Internet (European Security Forum, 1996:5) involves contacting an Internet service provider and requesting a connection to their network. There are three types of Internet connections, each offering different levels of functionality and security risk (refer to figure 2.1):

- **Terminal access**

  Terminal access is access by an e-mail account through an Internet service provider, or a connection to an on-line provider, such as CompuServe. These connections allow limited usage of the provider's computing resources, but tend to expose the organisation to fewer risks;

- **Dial-up access**

  The dial-up access facility offers a comparatively slow direct connection to the Internet through an Internet service provider. Unlike terminal connections dial-up connections can offer the full spectrum of Internet capabilities. However due to the bandwidth limitations of dial-up lines, the connection may prove prohibitively slow for some Internet applications; and

- **Dedicated access**

  Dedicated access is using a high-speed dedicated lines or data services. These connections provide the full spectrum of capabilities, but can also expose the organisation to greater security risks.

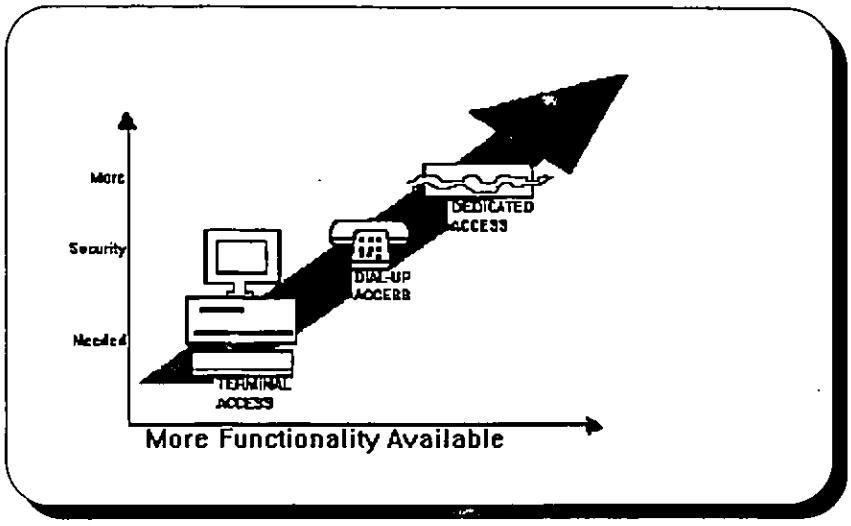

Figure 2.1: Functionality versus security for the different types of Internet connection (European Security Forum, 1996:5)

In general, terminal access allows Internet access for a single user, while dial-up and dedicated connections can be configured to support a multi-user environment. The relative functionality and security risks inherent in the different connection types is illustrated in figure 2.1 above. Note that this figure illustrates the relative risks only if nothing is done to enhance security. As it will be seen from this project, a number of technical means are available to reduce the risk associated with the more functional Internet connections (European Security Forum, 1996:5).

2.9 THREATS AND CONSEQUENCES OF CONNECTING TO THE INTERNET

2.9.1 Troublemakers (European Security Forum, 1996:19)

These troublemakers are variously referred to as hackers, attackers, or crackers. Whatever their motives, they take advantage of Internet security flaws and characteristics of the Internet's design to gain access to proprietary networks and threatens network resident information and services.

While these people existed before the Internet came to the attention of the commercial world, the problem is magnified. The Internet offers hackers a greater number of

'targets' than a corporate network and then allows them to openly discuss their success within minutes on globally available bulletin boards.

These individuals are motivated by a number of factors. Corporate espionage has grown in recent years, and a number of organisations are actively engaged in spying on their competitors. Increasingly, the growth of 'hacker for hire' services is becoming evident, where an individual is paid to break into a system and retrieve a confidential piece of information from a competitor (e.g., a competitor's new business plan, specifications for a product, an industry pricing model). There have always been incidents of individuals around the world reselling illegally obtained computer and telecommunications services (European Security Forum, 1996:9).

2.9.2 The threat from 'inside'

However, not all threats come from outside the organisation. It is equally important to protect against the possibility of an employee will-fully or accidentally divulging proprietary information or maliciously altering system content. This is a particular concern during times of change - such as organisational restructuring or downsizing - when disgruntled or careless employees continue to have access to computing facilities. (European Security Forum, 1996:11)

2.9.3 The four major threats areas

The threats posed to an organisation using the Internet can be grouped into four major areas: **disclosure of information; unauthorised access to systems and applications; loss of information integrity; and denial of service.** Each of these areas is described in turn below, along with a table of examples and consequences (Blankley, et al. 1996: 44).

2.9.3.1 Disclosure of information (European Security Forum, 1996: 11)

For many organisations, the most serious threat is the release, whether by intention or accident, of proprietary information. One inherent property of the technology underlying the Internet is that it is quite possible for someone to 'eavesdrop' on a conversation over the Internet. By virtue of being connected to the same network, any computer can 'see' messages involving other computers on that network, including e-mail, files being transferred, passwords, and in some cases, even keystrokes as they are being entered in real time. Examples and consequences of disclosure of information is explained in table 2.2, below (European Security Forum, 1996: 10):

1WHAT CAN HAPPEN	HOW IT CAN HAPPEN	CONSEQUENCES
'Eavesdropping'	A service provider could be breached, or could be run / managed by unprofessional or dishonest people. A disgruntled employee could 'listen' to communications on the network.	Propriety information (e.g. customer information, product specifications, industry pricing model) may end up in the hands of a competitor.
Password sniffing	A programme which 'collects' passwords information, is installed on a service provider's computer without their knowledge.	Employees', managers', or administrators' passwords are disclosed, possibly leading to unauthorised access to systems.

WHAT CAN HAPPEN	HOW IT CAN HAPPEN	CONSEQUENCES
Accidental disclosure	An employee inadvertently sends a highly confidential electronic mail message to a wide distribution over the Internet (e.g. a newsgroup, or an electronic mailing list).	Proprietary information is disclosed to the public, leading to a loss of competitive advantage and/or reputation.

Table 2.2 Examples and consequences of disclosure of information (European Security Forum, 1996: 11)

2.9.3.2 Unauthorised access to systems and applications (European Security Forum, 1996: 12)

The most highly-publicised of all security breaches involve unauthorised access to private systems. Poor choice of passwords, inadequate security administration, and software bugs may render systems subject to attack. Once access to a system has been gained, an attacker may be able to control completely a computer or network.

Additionally, he or she could use that computer to launch further attacks on other organisations' computers and networks.

Another common method of gaining unauthorised access occurs when a user masquerades as someone else. Due to the lack of mechanisms for checking identification, that is fairly easy to do.

Examples and consequences of unauthorised access are depicted in table 2.3 below:

WHAT CAN HAPPEN	HOW IT CAN HAPPEN	THE CONSEQUENCES
Internal systems are breached	A hole in gateway software could be exploited (e.g. WWW sever, electronic mail gateway). User passwords can be stolen or guessed.	•Systems could be brought down. •All data and applications could be modified or erased. •Information can be stored on the systems by the 'hacker'. •Systems could be modi fied to foil recovery attempts.
'Spoofing'	A third party can impersonate a trusted user and act with that user's privileges in order to gain access to a system	As above. Communications could be diverted to a third party, e.g. a competitor or the press. 'Viruses' or 'Trojan Horses' could be planted in the system to restrict the ability of the organisation to 'see' or investigate the attacker.

WHAT CAN HAPPEN	HOW IT CAN HAPPEN	THE CONSEQUENCES
Attack on other systems launched	Attacks on other organisations are launched from an internal system, by either and intruder or an unscrupulous insider.	Legal and financial liability. Loss of public confidence. Damage to reputation.

Table 2.3: Examples and consequences of unauthorised access (European Security forum, 1996:12)

2.9.3.3 Loss of information integrity (European Security Forum, 1996: 14)

One threat that is often overlooked is the modification of data, both while stored on a computer and while in transit. A number of recent incidents have uncovered automated tools being used to alter the content of data on a network (refer to figure 2.4).

WHAT CAN HAPPEN	HOW IT CAN HAPPEN	CONSEQUENCES
Modification of data in transit	Message contents are eavesdropped, altered, and retransmitted.	Diversion of funds. Modification of contracts or transactions. Misrepresentation of an organisation.
Modification of data on a system	Unauthorised access as a privileged user. Introduction of viruses.	False information given to partner/clients. Damage or destruction of data. Alteration of files contents on a system.

Table 2.4: Examples and consequences of loss of information integrity (European Security Forum, 1996: 14)

2.9.3.4 Denial of service (European Security Forum, 1996: 15)

Denial of service occurs when a computer or network is rendered ineffective, due to an inability to communicate with others. Denial of service is an example of an active attack and is difficult to protect against. Refer to table 2.5 for examples and consequences of the denial of service.

WHAT CAN HAPPEN	HOW IT CAN HAPPEN	CONSEQUENCES
'Packet storms'	A large quantity of data is sent to a computer which must process it. The computer cannot do anything else during this time.	Inability to conduct business. Possibility for unauthorised access via 'spoofing'.
Network outage	Unauthorised access to a service provider brings down a network.	As above.

Table 2.5: Examples of denial of service (European Security Forum, 1996:15)

There are co-dependencies among these threats as well - i.e., masquerading as another entity can lead to unauthorised access to a system, which can, in turn, lead to denial of a service provided by that system.

2..10 CONCLUSION

For the objectives of this study, the purpose of Internet security is to ensure the information security objectives of confidentiality, integrity, availability, and accountability on the public Internet, and on private hosts and networks that are connected to the public Internet. Internet security can be looked at as a control structure which has three main elements:

- **Network security** consists of security and control over the connections and information flow to and from other hosts, both internal and external to an organisation, as well as security and control over network routing and applications that have networking functionality,

- **Host security** consists of security and control over the operating systems of computers that are connected to a network. This is important to Internet security because the security of host based networking applications is reliant on the security of the host operating system..

- **Control Policies and Procedures** are the management authorised policies and procedures in place to ensure that information and network assets are used in-accordance with organisational goals.

In the next chapter, the PrivateNet system will be surveyed to be able to evaluate the effectiveness of the system in ensuring the security of the Internet environment.

CHAPTER 3

THE PRIVATENET SYSTEM

CONTENTS PAGE

3.1 BACKGROUND

The PivateNet system (NEC Technologies Inc.1996.23) is an off-the-shelf commercial firewall product combining the hardware and software that provides security for TCP/IP networks. The PrivateNet system can also provide a secure communication over public networks, such as the Internet, to reduce network costs through its Virtual Private Network (VPN) technology. The PrivateNet Firewall Security server blends two technologies to create a secure Internet communications environment:

a) Applications that originate their connections from within an internal network are managed by the SocksPlustm proxy, NEC's advanced circuit-level proxy technology;

b) Applications that originate their connections from outside the network are managed by security-hardened application-level proxy servers. Application services include Telnet, Email (SMTP) Web Server (HTTP) and NetNews (NNTP);

c) The PrivateNet system is suitable for securing a network from the Internet, as well as isolating subnetworks within a corporate network; and

d) The PrivateNet system provides easy installation and configuration through CD-ROM-based software, friendly administration, user transparency, SOCKS protocol comparatibility, and parallel and serial firewall configurations.

The PrivateNet system has been designed to provide the best technologies for both a firewall and a virtual private network. It covers a very high level of security while providing adequate access. Like most commercial firewall products, the PrivateNet system uses a number of different technologies to establish the required connectivity.

A firewall's primary purpose is to provide security. To do so, all components of Internet security control structure must be secured, and they must be tested both individually and in combination with the other components. The PrivateNet system is a complete system, including hardware, a security hardened operating system, and

firewall system software. The advantage of a turnkey firewall product with completely integrated components is that it achieves **the highest possible level of security and performance.**

Like most other commercial firewall products, the basic assumption in the design of the PrivateNet system is that anything not explicitly allowed is denied. However, the design of the PrivateNet system goes much further than that, making every attempt to provide an effective and secure firewall.

One example of this approach is that all software, including the operating system and other programs, is stored on a CD-ROM and is always loaded directly from the CD rather than from a hard disk. This allows a high degree of trust in the integrity of the software as it is not possible for anybody to modify the content of the CD-ROM.

The design of the firewall software is based on the philosophy that being small is good. The software that implements the firewall is split into small individual programs so that each can be easily verified and tested. In addition, different proxy technologies are applied to different levels of security requirements.

The operating system used for the PrivateNet system is a scaled-down and security-hardened version of BSD UNIX 4.4 from Berkeley Software Design, Inc. NEC Technologies Inc. has chosen this platform believing it is the best possible operating system today for Internet connectivity, as opposed to other common UNIX implementations with bloated kernels, which are much more difficult to effectively secure.

3.2 THE PRIVATENET SYSTEM

The PrivateNet system is analysed under the following subheadings :

3.2.1 The PrivateNet system firewall technology;

3.2.2 Circuit level proxy;

3.2.3 Application level proxy;

3.2.4 Connection Filtering;

3.2.5 Address hiding;

3.2.6 User Authentication;

3.2.7 Firewall-to-Firewall connectivity;

3.2.8. Parallel Configuration for High Performance and High Availability;

3.2.9 Use of an Encryption in the PrivateNet system.;

3.2.10 Implementation of the UDP Circuit-Level Gateway;

3.2.11 The Configuration files;

3.2.12 Name Service; and

3.2.13 Mail Service.

3.2.1 The PrivateNet system firewall technology

NEC Technologies Inc. (1996:13) summaries the PrivateNet Firewall Technology as follows:

The PrivateNet system uses two different types for two different levels of security. For connections originating from inside the organisations, the PrivateNet system is a circuit level proxy. A circuit-level proxy provides a medium level of security, while being both flexible and adaptable to the various access requirements of the organisation. However, NEC believes that circuit-level proxies give an inadequate level of protection for access from the Internet to the inside of an organisation's private network. Therefore, it provides application-level proxies for such access.

3.2.2 Circuit level Proxy

The circuit level proxy (NEC Technologies Inc.1996:6) implements a generalised proxy mechanism that relays IP connections from the originating application through the firewall to its destination. Before completing the connection, the circuit-level proxy verifies that the connection is permitted in its configuration file. When the connection is verified and establish, the circuit-level proxy program relays packets back and forth between the user application program and the Internet service to which it is connected. The SocksPlus proxy:

- Uses proper software layering, leaving it much less vulnerable to bad packet formats;
- Can be configured to listen only to client connections on the inside network, and properly identifies IP spoofing attacks originating from the outside but usi- ng an inside IP address;
- Provides UDP support in addition to the TCP support found in the original SOCKS implementation;
- Provides encrypted data communication between the servers;
- Supports parallel configuration, providing both high availability and load balancing between servers;
- Does not require a configuration file at each client. The server information is obtained from DNS; and
- Does not accumulate log information to each client.

The SocksPlus proxy uses its own improved protocol when communicating with the SocksPlus proxy clients and other SocksPlus proxy servers, but it is also fully backward-compatible with existing SOCKS servers and clients.

As for UNIX, other network applications can be easily converted to operate with the SocksPlus proxy through a simple recompilation and relinking procedure. Existing SOCKS clients are fully supported by the SocksPlus proxy.

3.2.3 Application Level Proxy (NEC Technologies Inc. 1996:7)

An application-level proxy implements a specific proxy mechanism for each application. It is a program that understands the application protocol, and that can screen the traffic passing through the gateway with a comprehension of context not present in either circuit-level proxies or packet filtering.

The main advantage of an application-level proxy over a circuit-level proxy is its ability to understand the flow of information and make intelligent decisions about requests. For example, the PrivateNet system provides a proxy for electronic mail over Simple Mail Transfer Protocol (SMTP). An application-level proxy eliminates the possibility of someone extracting information about the local user population using SMTP commands such as EXPN (expanding a mail alias) or VRFY (verify the presence of a user).

The disadvantages of this mechanism are that it is not transparent to the user, and it is necessary to design and implement an individual application-level proxy for each supported protocol. The PrivateNet system currently supports the following application-level proxies:

- A Telnet proxy with good user authentication based on the challenge/response system. SNK is available in Release 1.0, and other mechanisms will be added in future releases.
- An SMTP proxy, which acts as a security wrapper for sendmail.
- An NNTP proxy for support of network news.
- An HTTP proxy, primarily intended for support of HTTP servers on a screened subnet.
- An FTP proxy, intended for support of FTP servers on a screened subnet.

3..2.4 Connection Filtering (NEC Technologies Inc. 1996:7)

The access control style used for both a circuit-level proxy and application-level proxy is called "connection filtering" because filtering is performed at the time of connection. In other words, a proxy-based connection needs to be verified only when the connection is initially established, while packet filtering needs to verify each and every packet.

Because verification is performed only once per connection, it is possible to verify the connection thoroughly. When a connection request is received by an application-level proxy, the connection is verified based on a source/destination address and port number. In addition, more checks are performed. For example, it is verified that all connections arrived on the expected interface. If a connection request claims to originate from the internal network but arrives on the interface connected to the outside network, it is recognised by the system as a spoofing attempt. The system reports the attempt in the system log, and the connection is refused. Similarly, as a matter of routine, all name servers lookups are validated by a reverse lookup. While this does not guarantee that name server spoofing does not take place, it does decrease the likelihood of a successful name server spoofing attack.

3.2.5 Address Hiding (NEC Technologies Inc. 1996:8)

One of the desirable side effects of the proxies is that, because all network traffic either originates or terminates at a proxy program on the firewall, internal networks are completely hidden from those outside. This means that a cracker cannot obtain information by scanning internal networks, and the internal networks do not need to be the official registered network addresses. While NEC does not advocate the internal use of network addresses that have been registered by somebody else, the Internet Engineering Task Force (IETF) has set aside several networks guaranteed not to be registered by anyone else and that should be routed by anyone else on the Internet.

Using such addresses gives an organisation all the address space it needs and helps protect the firewall from IP spoofing because the addresses are not supposed to be routed across the Internet.

3.2.6 User Authentication (NEC Technologies Inc. 1996:8)

Users from outside the PrivateNet system can Telnet to hosts in the internal network with the Telnet proxy. However, for security reasons challenge and response is the only supported authentication method using non-reusable passwords. It is common practice for crackers on the Internet to run a packet sniffer, which intercepts and records traditional UNIX login name and passwords pairs.

Non-reusable passwords employ a mechanism to ensure that a given password can be used only once. The current version of the PrivateNet system uses Digital Pathways' SNK calculator for this purpose.

3.2.7 Firewall-to-firewall Connectivity (NEC Technologies Inc. 1996:8)

The PrivateNet system (as depicted in figure 3.1 below) also supports connectivity to other PrivateNet systems within the same organisation. This ensures that large organisations can install departmental firewalls that work in unison with the corporate Internet firewall

When a client requests a connection to a destination host through several PrivateNet servers, each PrivateNet system verifies the request before forwarding it to the next PrivateNet system. After all servers have been verified, and the connection is allowed, an acknowledgement is sent to the client. This strategy ensures that the client receives its acknowledgement only after all verifications have been conducted and the connection to the destination has been established. (Refer to figure 3.1)

Because the PrivateNet system is designed to encrypt communication between servers, it can be used to build encrypted tunnels or virtual private networks across the

Internet, allowing transparent access for SockPlus proxy applications. It maintains the same level of security provided by a privately leased line, in effect giving an organisation a cost-effective and secure long distance service.

For geographically distributed organisations, it is possible to allow connections either through the application proxy mechanism or to perform server-to-server connection if the organisation has standardised on the PrivateNet system.

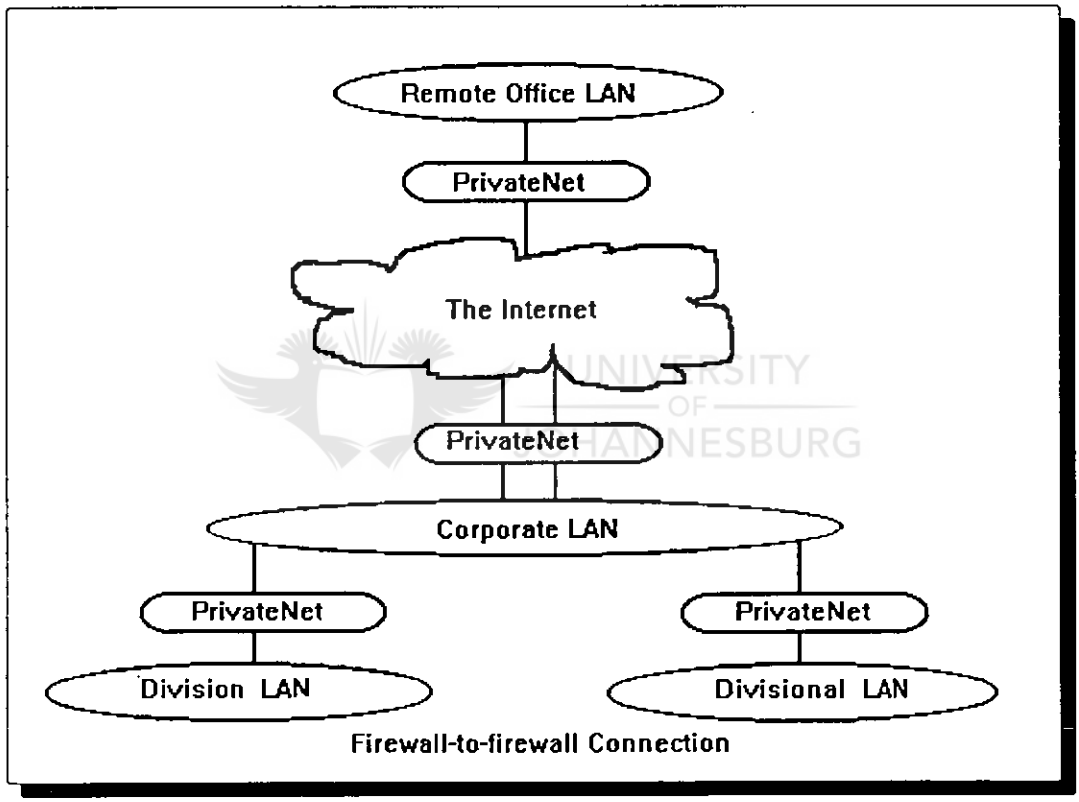

Figure 3.1: Firewall to Firewall connection

(NEC Technologies Inc, PrivateNet system white paper, 1996:9)

3.2.8 Parallel Configuration for High Performance and High Availability. (NEC Technologies Inc. 1996:9)

For network sites that require high performance and availability, multiple PrivateNet units can be connected in parallel and configured as a single firewal refer to figure 3.2. This configuration ensures that the firewall is not overloaded. To distribute the

networking load evenly between PrivateNet servers, the internal name server is set up in a round-robin configuration, enabling clients to switch back and forth between servers.

If a server becomes unavailable, any client (1 or 2) attempting to connect through that server waits only a few seconds, and then moves on to the next server. Therefore, when a firewall consists of multiple servers, high availability is ensured because the remaining servers continue to transparently service all client connection requests.

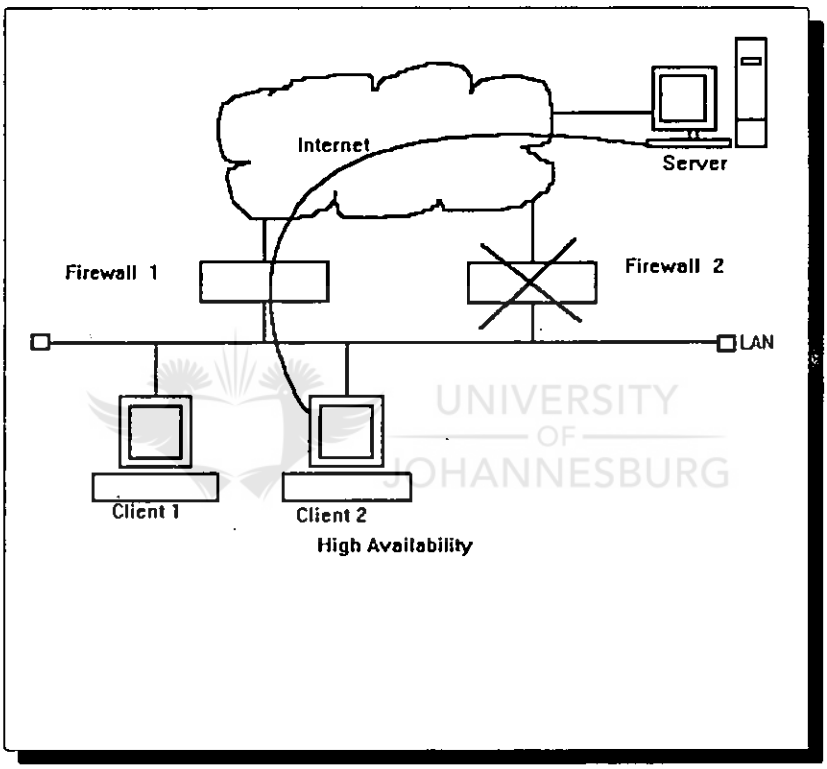

Figure 3.2 High availability

(NEC Technologies, PrivateNet system white paper, 1996:10)

3.2.9 Use of Encryption in the PrivateNet System (NEC Technologies Inc. 1996:10)

As mentioned above, encryption is used in communication between two PrivateNet servers to ensure secrecy. The encryption method is negotiated between the origination and destination servers, while any intermediate server is not allowed to see, and is unable to decrypt, the data that passes through them. Currently, the PrivateNet system supports and uses DES and triple DES encryption.

3.2.10 Implementation of the UDP Circuit-Level Gateway (NEC Technologies Inc. 1996:10)

While filtering TCP circuits is difficult at best, securely filtering UDP connections is almost impossible. The difficulty is in the difference between the two types of connections. The TCP protocol implements a virtual circuit and keeps a context for the connection, while a UDP connection is a datagram protocol where each packet is an independent message.

Therefore, the UDP connectivity between PrivateNet system clients and servers is implemented as UDP over TCP. Providing UDP connectivity in this manner simplifies the implementation of the UDP relays significantly, and to a large degree removes the problems normally experienced in providing UDP support through a firewall. While this strategy may be less efficient than a native UDP implementation, its simplicity and ease of security management by far justify the additional overheaded.

This implementation lets the PrivateNet system provide relatively safe support for internal UDP clients, such as Archie or Xarchie, to connect through the firewall. However, in general the recommendation from CERT (Computer Emergency Response Team) that UDP not be allowed through the firewall should be respected as much as practically possible.

3.2.11 The Configuration Files (NEC Technologies Inc. 1996:10)

The PrivateNet system uses two text-based configuration files, allowing a security officer or system administrator to read these files at any time to understand the current configuration. It also lets those who do not like using a graphical user interface (GUI) configure and maintain these files without the GUI. They can log in on the console and perform all configurations with a text editor such as *vi*.

The two configuration files are Socksplus.conf and authorize.conf.

The Socksplus.conf configuration on file contains all rules for access control server-to-server interaction. There are three major sections:

- the first section is an access control list for SocksPlus proxy clients connecting to the server. These rules are fairly traditional, using source and destination addresses and port numbers to determine if a given client should be allowed to connect through the server. In addition, there is a configuration clause specifying which interface on the PrivateNet system should accept requests for SOCKS and SocksPlus proxy connections;
- The second section configures the rules for behaviour when performing server-to-server connections. This section also has a set of access control lists for the connections, which applies to SOCKS and SocksPlus proxy connections from the servers. When an organisation has both departmental and corporate firewalls, the PrivateNet system allows corporate access rules to be enforced at the corporate firewall independent of access rules implemented at the departmental level. This section also contains configuration clauses that determine which other PrivateNet system to accept connections from, and how SOCKS and SocksPlus proxy connections should be routed when using server-to-server connectivity; and
- The final section contains configuration clauses for time-outs and the limitation of connection types. For example, this allows the system administrator to limit the number of WWW connections allowed through the server at a given time.

The authorize.conf configuration file contains the rules for how a user can connect through the firewall. These rules define which users can Telnet to hosts inside the firewall, and what kind of authentication should be used.

3.2.12 Name Service (NEC Technologies Inc. 1996:12)

The domain name server on the PrivateNet system is configured, by default, as what is often referred to as a split name server. In this configuration, two tightly coupled

primarily name servers are each used with an appropriate number of secondaries. The software for both name servers is the unmodified standard UNIX name server. The PrivateNet system uses bind version 4.9.3, which has many security improvements over the older versions of the software. The name server on the PrivateNet system is configured as a traditional name server with the exception that it has information only about the systems connected to the public networks (typically this is the PrivateNet system alone). This allows sites on the Internet to obtain the information necessary to connect to the services offered by that site.

Resolution of host name and addresses for the internal hosts are handled by an internal name server, which has all information about the internal hosts. Because the PrivateNet system does not perform any kind of packet forwarding, there is no way for the internal name server to connect to any name server on the outside. Instead, resolution for such inquiries is handled through the name server's "forwarder" mechanism, where the inquiry is forwarded to the external name server on the PrivateNet system for resolution. Because this name server can connect to other name servers across the Internet, it can resolve the inquiry in its usual manner and return the result to the internal name server.

Special consideration should be given to the PrivateNet system itself since it needs to resolve the inside host names and addresses while still keeping the name server cache uncontaminated with this information. The mechanism for this already exists through the resolve library. Because the PrivateNet system has a local revolver configuration file pointing to the internal name servers, all enquiries originating on the PrivateNet system are resolved by those name servers instead of the name server running on the PrivateNet system.

3.2.13 Mail Service (NEC Technologies Inc. 1996:13)

The PrivateNet system provides a simple SMTP mail exchanger for e-mail connectivity between internal and external hosts. All mail passes through the PrivateNet system in three steps:

a) The SMTP proxy receives the e-mail and stores it in its spool directory on the hard disk. This program has been kept as simple as possible to prevent attacks through e-mail;

b) The postmaster program picks up the mail, stores it in the file, changes all occurrences of shell meta character, if any, in the address portion of the mail and then hands the result to Sendmail for delivery; and

c) Sendmail delivers the mail in the usual manner.

This strategy has an advantage in that it isolates Sendmail, a common source of security problems, from the network while still using it as a mail delivery agent. It keeps the SMTP proxy mechanism simple and does not require reimplementation of the address rewrite and the delivery mechanism. This implementation has the following noteworthy advantages:

- System administrators familiar with Sendmail configuration can make configuration changes as usual. Because the basic mechanism is uncharged, users are assured that no new bugs have been introduced into this complex system;
- By default the Sendmail configuration on the PrivateNet system uses a simple forwarding strategy. That is, all incoming email is forwarded to a central mail hub or mail exchanger. This moves all user address resolution (such as the alias file) from the firewall to an internal host with presumed easier access. The internal host is, therefore, simpler to maintain. System administrators with a large user population can implement more complex mail delivery schemes by configuring Sendmail and the name service accordingly; and
- Outgoing mail is delivered in a similar way using the PrivateNet system as a mail relay. In its simplest configuration, this is achieved by having all hosts

forward email to the mail hub which, in turn, uses the PrivateNet system as a smart host.

3.3 CONCLUSION

For each component of the PrivateNet system, the key features/parameters for achieving the information security control objectives, have been documented and will be used in developing the matrices in chapter 4.

With the information security control objectives defined, it is considerably easier to identify the key components of the Internet security control structure.

Accordingly, by specifying the information security control objectives and the features provided by the PrivateNet system, the identification of significant concepts and facilities is made easier, as it is an overall evaluation of the relevant environment. This issue will be covered fully in chapter 4 and the conclusion in chapter 5.

CHAPTER 4

APPLICATION OF THE PRIVATENET SYSTEM TECHNOLOGY TO THE INTERNET ENVIRONMENT

CONTENTS **PAGE**

4.1 INTRODUCTION

In this chapter, the model and environment identified and explained in previous chapters will be depicted in the form of matrices. These matrices will be simple views of the main features of the PrivateNet system in the Internet environment, and the corresponding control objective met by each of these features

It is important to note that in certain instances, the facilities of one feature of the PrivateNet system may be used to accomplish more than one security control objective.

The matrices will therefore provide a view of the technological components (features) of the PrivateNet system which can be used to achieve the predefined objectives.

In other words, the matrices provide a map of how technology can be used to control technology using the model in the PrivateNet system environment.

4.2 THE MATRICES

The matrices developed, are presented in Table 4.1 where a matrix is developed for each of the components/features of the PrivateNet system. The vertical axis contains the key components/feature and explanations of the capabilities thereof. The horizontal axis contains the information security objectives which need to be achieved. If the feature achieves any of the security objectives, it is indicated by a tick "✓" under the applicable objective.

The matrices can then be used as a reference point by the implementor of the system, i.e security managers for identification of the control areas where security needs to be enhanced, and the auditor in the assessment of information security control risks in the Internet environment where the PrivateNet system is in use.

It is important to examine briefly the applicability of each security objective to the firewall technology that is being dealt with.

Security controls have four main objectives:

- **Confidentiality** is protecting information from unauthorised disclosure;
- **Authority** is to ensure that only valid transactions /business processing takes place
- **Integrity** is protecting information from unauthorised modification;
- **Availability** is ensuring that data is accessible to all authorised users. It is also protecting the system from denial-of-service attacks that range from issuing system resources to crashing the system; and
- **Accountability** is identifying and holding a user accountable for actions that create, modify, provide access to, or disseminate information.

The application of the PrivateNet features to the five information security objectives is aimed at ensuring that the technology available within them, can be used to provide adequate controls to meet these five objectives.

Table 4.1: PrivateNet system features

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
1. Authentication Methods Token-based authentication is provided through SNK for external-to-internal access. Access to internal resources from outside the firewall uses strong authentication without disclosing passwords to eavesdroppers.	✓		✓		✓	2.9.3

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
2. Blocks IP Adress Spoofing Internal hosts cannot be spoofed because all IP traffic is filtered at the firewall. The PrivateNet system protects itself against spoofing by briefing and segregating internal and external traffic.	✓			✓		2.9.3.2
3. Connect Limits The system can be configured to limit the number of connections by client service type.	✓	✓	✓			2.9.3.4
4. Connect time/Traffic All connection times and amount of traffic are logged.			✓			2.9.3.4

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
5. Connection auditing All connection attempts are logged whether successful or not.			✓	✓	✓	2.9.3.3
6. DNS (Domain Name Service) The PrivateNet system runs a split DNS configuration, which allows internal systems to resolve both internal and external host addresses and names. External systems cannot resolve names or addresses for internal systems.	✓		✓	✓		2.9.3.1
7. Services use logging Services used are logged.	✓		✓		✓	2.9.3.3

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
8. Log-in attempts Logging All access attempts, from outside to inside, are logged.			✓	✓	✓	2.9.3.3
9. Encryption Site-to-site traffic can be encrypted between two PrivateNet systems. This allows for VPNs (Virtual Private Networks) between these sites using inexpensive public networks. The VPN supports other UDP/IP and TCP/IP traffic. DES and Triple-DES security methods are used for encryption.	✓			✓		2.9.3.2

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
10. Exportable Logs All PrivateNet systems logging is written to a remote system, which provides a secure audit trail even in the event of a PrivateNet system security breach.	✓		✓	✓	✓	2.9.3.3
11. Floppy based Key Distribu- tion Security keys needed to provide VPN functionality between PrivateNet systems are securely exchanged through a floppy diskette. It is recommended that the security administrator tightly control the diskettes	✓		✓	✓		2.9.3.2

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
12. High Availabilty Installation of parallel PrivateNet systems allows access to the external network to continue in the event of the failure of one of the PrivateNet systems.		✓				2.9.3.4
13. IP Address Hiding The only IP addresses exposed to the external network are those assigned to the PrivateNet system's external interface (s). Internal IP addresses are effectively translated to an IP address on the PrivateNet server itself. Internal IP addresses are not exposed to the external network.				✓	✓	2.9.3.1

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
14. Load balancing The SocksPlus proxy clients (Telnet, FTP, etc.) used in conjunction with the PrivateNet system distribute the load between parallel PrivateNet systems. This allows the system to easily scale up for users at large sites. (This is based on random distribution, not on actual load).		✓				2.9.3.4

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
15. Transparent to users Authorised internal users can transparently access external resources with no additional steps required. The PrivateNet server provides access controls to restrict the internal systems that have access to external resources.	✓		✓	✓	✓	2.9.3.2

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
16. Versatile SocksPlus proxy clients The SocksPlus proxy clients are suitable for internal as well as external access. When making internal connections, PrivateNet system clients connect directly to these systems. This avoids unnecessarily loading the PrivateNet server and eliminates the need to have clients for both internal and external access.		✓				2.9.3.4

PrivateNet system feature	Security controls objectives					Ref.
	Autho-rity	Availa-bility	Acounta-bility	Confi-dentiality	Integri-ty	
17. Maximum security of the bastion host on which the firewall software runs. All software including the operating system, is on the PrivateNet system CD-ROM All insecure functions in the operating system are removed or modified. The PrivateNet system is offered as a hardware and software product to maximize security.	✓		✓	✓		2.9.3.2

4.2.2 FIREWALL RISKS/BOMBS

Risks are there. where use is made of any firewall technology to secure the network connection. Cheswick and Bellovin, (1994:277) gives a list of firewall risks/bombs each describing a problem that can allow a firewall to be penetrated. The PrivateNet system has been designed and implemented so that it is able to protect against all of these risks.

The application of the PrivateNet system technology to address the firewall risks/bombs is depicted in table 4.2. The risks/bombs that firewalls are exposed to, are given in column 1 whilst the application of the PrivateNet system to address the related risk, is given in column 2.

Table 4.2: Firewall bombs/risks

Column 1 **Firewall Bombs/Risks**	**Column 2** **PrivateNet System**	**Ref.**
1. Password system failures are the single biggest problem.	The PrivateNet system allows users to authenticate themselves only through challenge-response system authentication methods. Users are not allowed direct access to the firewall machine. The only exception is when the system administrator is logging in on the console. Because this connection does not cross any network, it does not present this problem.	2.9.3.2
2. Sequence number attacks can be used to subvert address-based authentication.	This is a problem in the implementation of TCP/IP has been corrected by BSDI.	2.9.3.3

Column 1 Firewall Bombs/Risks	Column 2 PrivateNet System	Ref.
3. It is easy to spoof UDP packets.	The PrivateNet system does not allow UDP connections through the firewall. The SocksPlus proxy allows clients using UDP to connect through the PrivateNet system, but the connections on the inside are implemented as UDP over TCP, eliminating this problem.	2.9.3.1
4. ICMP packets can tear down all connections between a pair of hosts.	The PrivateNet system does not allow ICMP packets to pass through the firewall.	2.9.3.4
5. ICMP redirect messages can subvert routing tables.	The PrivateNet system uses static routing tables and is therefore not subject to this type of spoofing.	2.9.3.1
6. IP Source routing can subvert address-based authentication.	It is not appropriate for a firewall to honor source routing. The PrivateNet system does not allow source routing information and is therefore not subject to this type of spoofing.	2.9.3.1
7. It is easy to generate false RIP messages.	The PrivateNet system uses static routing for its routing tables, and does not forward any RIP messages. It is therefore not subject to this type of spoofing.	2.9.3.3

Column 1 Firewall Bombs/Risks	Column 2 PrivateNet System	Ref.:
8. The inverse DNS tree can be used for name-spoofing.	The PrivateNet system uses reverse-name-serve-lookup to minimise this risk. Users are strongly encouraged to use only IP numbers in the configuration tables, which eliminates name server spoofing.	2.9.3.1
9. The DNS cache can be contaminated to foil crosschecks.	The PrivateNet system uses a new version of the name-server, but for this bomb, users are strongly advised to use only IP numbers in the configuration table. This eliminates name server spoofing.	2.9.3.1 & 2.9.3.3
10. Return addresses in mail are not reliable.	This problem cannot be solved by firewall technology. However, the SMTP proxy is implemented so that it does not give out information though the "EXPN" and "VRFY" commands, and it examines and prevents "mail header" attacks.	2.9.3.1
11. Sendmail is a security risk.	The PrivateNet system uses an SMTP proxy to receive email. This prevents Sendmail attacks based on network access or header corruption.	2.39.3.1
12. Don't blindly examine MIME messages.	The PrivateNet system does not interpret MIME messages, and is therefore not sensitive to this kind of spoofing.	2.9.3.1

Column 1 Firewall Bombs/Risks	Column 2 PrivateNet System	Ref.
13. It is easy to wiretap Telnet sessions.	Telnet (and all other connections) between multiple PrivateNet systems are encrypted, and a challenge/response system is used for authentication. However, these are only partial solutions. The correct solution to this problem requires an end-to-end solution. A redesign of the Telnet protocol, as well as reimplementation of the Telnet client and server are required. This is outside the scope of what a firewall can provide.	2.9.3.3
14. You can subvert NTP to attack authentication protocols.	NTP is not an appropriate service to offer on a firewall. The PrivateNet system does not offer this service, and is therefore not subject to this risk. Sites that use NTP internally are advised to get their own time source, rather than rely on this service from the Internet.	2.9.3.3 & 2.9.3.1
15. Finger discloses too much information.	The PrivateNet system does not support fingering of internal hosts. Therefore, no information can be disclosed in this manner.	2.9.3.1
16. Don't trust RPC's machine name field.	RPC is not an appropriate service to offer on a firewall. The PrivateNet system does not offer this service, and is therefore not subject to this risk.	2.9.3.3

Column 1 Firewall Bombs/Risks	Column 2 PrivateNet System	Ref.
17. The portmapper can call RPC services for its caller.	Portmapper is not an appropriate service to offer on a firewall. The PrivateNet system does not offer this service, and is therefore not subject to this risk.	
18. NIS can often be persuaded to give out password files.	NIS and NIS+ are not appropriate services to offer on a firewall. The PrivateNet system does not offer these services, and is therefore not subject to this risk.	2.9.3.1
19. It is sometimes possible to direct machines to phoney NIS servers.	This is a risk only when NIS is offered as a service. The PrivateNet system does not offer this service, and is therefore not subject to this risk.	2.9.3.3
20. It is hard to revoke NFS access.	NFS is not an appropriate service to offer on a firewall. The PrivateNet system does not offer this service, and is therefore not subject to this risk.	2.9.3.2
21. If misconfigured, TFTP will hand out /etc/ password.	TFTP is not an appropriate service to offer on a firewall. The PrivateNet system does not offer this service, and is therefore not subject to this risk.	2.9.3.2
22. Don't make FTP's home directory writable.	The PrivateNet system does not offer FTP services at this time.	2.9.3.2

Column 1 Firewall Bombs/Risks	Column 2 PrivateNet System	Ref.
23. Don't put real passwords on the anonymous FTP area.	The PrivateNet system does not offer FTP services at this time.	2.9.3.1
24. FTP is often abused to give out files to those who should not have them.	The PrivateNet system does not offer FTP services at this time.	2.9.3.1
25. Be careful about interpreting WWW format information.	This is a risk for WWW clients. There are currently no solutions a firewall can provide, other than to deny WWW access.	2.9.3.2
26. WWW servers should be careful about file pointers.	This is a risk for WWW clients. There are currently no solutions a firewall can provide, other than not to offer WWW services.	2.9.3.2
27. Attackers can use FTP to create Gopher control information.	The PrivateNet system does not offer Gopher services at this time.	2.9.3.3
28. Poorly written query scripts pose a danger to WWW servers.	This is a risk for WWW servers. There are currently no solutions a firewall can provide, other than not to offer WWW services.	2.9.3.2
29. The MBONE can be used to route through some firewalls.	The PrivateNet system does not offer MBONE service at this time.	2.9.3.2

Column 1 Firewall Bombs/Risks	Column 2 PrivateNet System	Ref.
30. An attacker anywhere on the Internet can probe for X11 servers.	X11 is not an appropriate service to offer on a firewall without an application proxy. The PrivateNet system does not include X11 proxy and does not otherwise offer this service. It is therefore not subject to this risk.	2.9.3.2
31. Don't trust port numbers supplied by outside machines	This risk is for packet filters only and does not apply to proxy servers. Because the PrivateNet system allows access only through a proxy mechanism, it is not subject to this risk.	2.9.3.2
32. It is all but impossible to permit most UDP traffic through a packet filter safely.	The PrivateNet system uses proxy severs, not packet filters. It is therefore not subject to this risk.	2.9.3.3
33. A tunnel can be build on top of almost any transport mechanism.	This is a management problem, not a technical one. This problem is almost impossible to prevent, but relatively easy to detect.	2.9.3.2
34. Firewalls cannot block attacks at higher levels of the protocol stack.	The PrivateNet system uses proxy technology everywhere because proxies are less sensitive to this problem than packet filters. However, they are not immune to it.	2.9.3.1

Column 1 Firewall Bombs/Risks	Column 2 PrivateNet System	Ref.
35. X11 is very dangerous, even when passed through a gateway.	X11 is not an appropriate service to offer on a firewall without an application proxy. The PrivateNet system does not include an X11 proxy and does not otherwise offer this service. It is therefore not subject to this risk.	2.9.3.2
36. Network monitoring tools can be very dangerous on an exposed machine.	The proxy mechanism implemented in the PrivateNet system does not allow any packets to pass through the firewall. This minimises the information that can be gained through packet sniffing. Because the PrivateNet system uses a challenge/response mechanism to authenticate users, password sniffing does not reveal any useful information for the cracker.	2.9.3.3 & 2.9.3.1
37. Be careful at directing finger to a subverted machine.	This is a problem that must be addressed in a finger client program. PrivateNet system does not offer this services.	2.9.3.2
38. Logging failed logins will often capture passwords.	The PrivateNet system does not capture passwords in its logs. Even if it did this information would be useless, because one-time passwords are used.	2.9.3.1

Column 1 Firewall Bombs/Risks	Column 2 PrivateNet System	Ref.
39. Hackers plan silent password grabbers.	Passwords in the PrivateNet system are stored and loaded directly from the CD-ROM.	2.9.3.1

4.3 EVALUATION

Using the methodology established in this short dissertation, it is found that each organisation needs to choose one of the basic types of firewall technologies. The right choice depends on the organisation's access and protection requirements. Companies with substantial information assets at risk will have to choose a higher-security solution, such as that offered by the PrivateNet system.

The advantages of using a proxy server are as follows (NEC Technologies, 1996:17):

- A proxy server allows no direct traffic through a firewall, packet filters;
- A proxy server prevents direct communication with an outside network or internal subnetworks;
- Packet filters denies/permit each network packet based on source and distination addresses, making this type of firewall at risk for spoofing;
- A proxy server uses a "connection filtering" authorisation mechanism to deterine whether a connection should be made. Before a connection is made, the proxy examines the data within the packets rather than just the packet headers, virtually eliminating spoofing attempts; and
- A proxy server hides the internal networks from those outside the firewall. A hacker cannot obtain information by scanning internal addresses.

4.4 CONCLUSION

All the features of the PrivateNet system evaluated, provided facilities which are aimed at Internet environment security. The PrivateNet system features of the model have, as their main objective, the performance of the specific tasks for the firewall. The security facilities that they provide are of primary importance.

In light of the above, the objectives set for this chapter have been met. As a result of the successful application of the PrivateNet system to an Internet environment, a positive contribution to the field of Internet security has been made.

Whether and to what extent the control facilities provided by each feature must be evaluated in terms of Internet security control structure. In the environment given, the various features do provide sufficient facilities to meet the required security control objectives.

It is therefore the responsibility of the security managers to implement their security philosophy by "using technology to control technology", while at the same time applying necessary application (or user controls). This means that a security package will need to be used in conjunction with the security features provided by the PrivateNet system. The investigation and the implementation of the package is beyond the scope of this short dissertation.

In view of the above, the objectives set for this short dissertation have been achieved.

CHAPTER 5

CONCLUSION

The objectives set for this short dissertation have been met, which are:

- To help the computer auditor to understand the information security risks associated with the client's use of the Internet;
- To evaluate the capabilities of the features provided by the PrivateNet system in addressing the security objectives of availability, confidentiality, accountability and integrity in an Internet environment; and
- To help the information security managers to identify the areas where security needs to be enhanced in the Internet environment.

The Internet security risks/exposures have been identified and the solution has been achieved. That is to say, by means of the use of the PrivateNet system the security exposures of the Internet environment have been addressed. The scope of this short dissertation remains as originally stated, even though it is contended that the methodology that has been developed to evaluate the selected environment may have universal applicability in the assessment of Internet security.

The main problem identified has been the balance between the need for Internet security, the need for performance and the need to keep costs to a minimum or the balance between the effectiveness, efficiency and economy of an Internet connection. The security model that has been developed has, as its starting point, the overall organisational framework for security, whereby management lays down its Internet security expectations and implements them. The implementation is carried out using the model developed in this short dissertation which has as its basis the Internet connection security control objectives.

The model developed in chapter 4 is in no way a replacement for good Internet management skills, but can assist the auditor in understanding the risks of the Internet connection exposures. Client service (where auditors also give business advice and

not only do the compliance audit for a client), which has become more important recently, can be maximised by using this model.

It therefore opens new fields for academic short dissertation in the area of Internet security auditing, such as drawing-up of an Internet audit guide/program. The different security control structures of an Internet environment can be further analysed, and the priority of each level of security, in terms of predefined objectives can be evaluated. Since the PrivateNet system is a new technology in firewalls, it would also be worthwhile to subject its security capabilities as well as performance aspects to further analysis. Other aspects that can be researched further are as follows:

a) Advantages and disadvantages of connecting to the Internet;
b) The implementation and maintenance of the PrivateNet system; and
c) The development of a comprehensive and technical audit program for assessing the security and control over a client's Internet environment.

In conclusion it can be said that in light of the above, the objectives set for this short dissertation have been met.

As a result of the successful application of the PrivateNet system to secure the Internet environment, a positive contribution to the field of Internet security has been made.

It is also significant that the methodology used may have universal applicability in the evaluation of Internet security. Furthermore, it is suggested that the matrix concept may have further applicability, for example, for a security team/managers to control the implementation/installation of the Internet firewalls.

"The two main lessons to be learned are that:

- No firewall, however well it is implemented, is 100% secure, and, with enough determination and time investment by crackers, a firewall can and will be broken into; and
- Firewall technology improves all the time, and the tools that are used to penetrate them also improve. Providing a highly secure firewall is an arms race, but a firewall based on a restrictive technology at least has the chance of surviving the longest"(Blankley, 1996: 56).

"The face of network security problem will certainly change over the years. But we are certain of one thing: it won't go away" (Cheswick and Bellovin, 1994:237).

BIBLIOGRAPHY

a) Angell, David, and Heslop, Brent. The Internet Business Companion: Growing Your Business in the Electronic Age. New York: Van Nostrand Reinhold, 1994.

b) Bill Cheswick, "An Evening with Berferd in which a cracker is Lured, Endured, and Studied," USENIX proceedings, Jan 20, 1990 Available for FTP from short dissertation.att.com: /dist/internet_security/berferd.ps

c) Bill Cheswick, 1997. The design of a Secure Internet Gateway, USENIX proceedings. [Online]. Available URL address: /dis/secure-internet-gateway.ps

d) "Building Internet Firewalls" by Brent Chapman and Elizabeth Zwicky, published by O'Rielly and Associates.

e) Cliff Stoll, "The Cuckoo's Egg 1994.

f) Comer, Douglas. The Internet book. Englewood Cliffs, NJ: Prentice Hall, 1994.

g) Cronin, Mary J. Doing Business on the Internet. New York: Van Nostrand Reinhold, 1994.

h) Cronin, Mary J. Doing More Business on the Internet. New York: Van Nostrand Reinhold, 1995.

i) Dan Farmer, *COPS and Robbers, UNIX System Security*. [Online]. Internet software. Available for FTP from cert.sei.cmu.edu: /pub/cops

j) Dave Koblas and Michelle R Koblas, SOCKS, Third USENIX UNIX Security Symposium Proceedings, 1992.

k) Ernst & Young Information Survey, Information Week, November 28, 1994.

l) European Security Forum, The Internet and security a guide for managers, 1996

m) "Firewalls and Internet Security: pursuing the wily hacker" Bill Cheswick and Steve Bellovin, published by Addison-Wesley.

n) Hafner, Katie, and Markoff, John. Cyberpunk. New York: Simon & Schuster, 1991.

o) Ira S. Winkler and Brian Dealy Information Security Technology? ... Don't rely on It. A Case study in Social Engineering, Fifth USENIX UNIX Security Symposium Proceedings, 1995.

p) Marcus J. Ranum, 1992 "An Internet Firewall," *proceedings of World Coference on Systems Management and Security.[Online]* Available for FTP from decuac.dec.com: /pub/docsfirewall/firewall.ps

q) Mungo, Paul, and Clough, Bryan. Approaching Zero. New York: Random House, 1992.

r) NEC Tcehnologies Inc, PrivateNet system white paper, 1996

s) Simson Garfinkel and Gene Spafford, "Practical UNIX Security," O'Reilly and Associates, June 1991

t) Smoot Carl-Mitchell and John Quarterman, "Building Internet Firewalls," UNIX World, February 1992

u) Stoll, Clifford. The Cuckoo's Egg. New York: Doubleday, 1989.

v) Stoll, Clifford. Silicon Snake Oil: Second Thoughts on the Information Superhighway. New York: Doubleday, 1995

w) William R. Cheswik and Steven M. Bellovin, Firewall and Internet Security, Repelling the Wily Hacker, Addison-Wesley Professional Computing Series