SEMINAR PAPER

ON

INTERNET SECURITY

BY

PETER A. AKHIHIERO ESQ.

PRESENTED AT THE SEMINAR ON BASIC COMPUTER TRAINING AT THE MIKON INSTITUTE OF INFORMATION TECHNOLOGY, 34A, BOUNDARY ROAD, G.R.A, BENIN CITY, ON TUESDAY, 23RD MAY, 2006

INTRODUCTION:

Time is said to be the mother of change. With time, almost every object on this earth will change its colour or texture. It is for this reason that change is said to be a perfect law of nature. With time, even human beings grow from an infant stage to an adult stage of maturity.

In the past, the entire human race lived in agricultural societies. Today, many countries of the world have grown to industrial societies. In this age of industrialization, these countries are being transformed into information societies. The advent of computers has introduced a revolution in the practice of information technology.

The focus of this paper is on the subject of **INTERNET SECURITY** as a salient aspect of the practice of modern information technology. In the course of my research into the subject, I discovered that the field of Internet Security is not only vast, but highly technical and complex. I must confess that for my elementary level, as a beginner in the basic study of computer science, I am unable to comprehend most of the hi-tech aspects of the paper.

Thus, this presentation is my humble attempt to articulate the concept of Internet Security, from some of the materials which I stumbled upon in the course of my research.

I have adopted the simple approach, of identifying some fundamental definitions, principles and processes. Furthermore, I will attempt a critique of the practice of Internet Security. Finally, I will leave the rest to my very erudite instructors, to fill all the gaping gaps in the paper.

THE INTERNET:

Literally speaking, the word **Internet** is the shortened form for **inter-connected net** work. The Internet is a collection of computer networks that connect millions of computers around the world. It is a vast spider web of computers that are all linked together.

To get a graphic picture of the system, consider the set up of your landline telephone connection. From your house, a line connects you to your local exchange. Your local exchange is linked to other exchanges. When you make a long distance call, your signal hops from one exchange to another exchange, until it gets to the other person's local exchange. From there, the signal is sent to that person's phone and it begins to ring. When he picks the phone, the line is opened and you can speak.

Now, imagine that your line is connected to your home computer, and that you can receive or send information from your PC to another computer at the other end of the phone line. That is the picture of the Internet. Once you are connected to the Internet, you can access a wealth of information, including pages on the World Wide Web, News groups, Weather information, Games, etc. The Internet is commonly used for communication, such as e-mail, commercial transactions, research, etc.

DEFINING SECURITY:

The need for computer security existed long before the advent of the Internet. Shortly after the computer was developed, the need to protect the computer became apparent. Presently, the well established field devoted to securing computers and other data is known as **Information Security**. The subject of Internet Security is merely a specialized aspect of Information Security. Hence, many of the principles and techniques of Internet Security

were actually adopted from the practice of Information Security. However, the public nature of the Internet creates new challenges in the practice of Information Security.

Security as a concept can be quite nebulous. Security can encompass activities that protect your computer systems from viruses, restrict the use of hardware, software, or data, or prevent users from performing bad activities or actions of malice. The basic goal is to allow only legitimate users to do only what they are supposed to do.

The point must be made that security is **a means to an end, not an end in itself**. The goal of the establishment is to enforce security, in order to conduct its business. The goal is not to be the most secured business on the planet. Properly used, security is merely a tool that minimizes and eliminates disruptions to your business.

Furthermore, there is nothing like full proof security. A 100% secure system does not exist. The standing joke is that the only system that is completely secured is one that is unplugged, switched-off, locked away and buried. That is a pretty secured system, but completely useless.

INTERNET CONTROLS:

In this age of hi-tech information technology, the Internet has provided the greatest access to freedom of information and communication. Like all kinds of freedom, the Internet has been exploited by many unscrupulous individuals to perpetrate their mischiefs.

These range from sending unwanted and sometimes offensive e-mails, to credit card fraud, advanced fee fraud (a.k.a. 419), having other systems infected with malicious virus, invasion of private information or communication, etc.

The emergence of these unwholesome practices has necessitated the development of some forms of **Internet Controls**. These are control measures, to prevent abuses by users in the system. Some control measures provide security at the level of the computer system, while some others operate at multiple layers.

The categories of control measures are not closed. With continuous research in the field, new measures are being introduced. We may safely consider some of the operating controls in two broad categories: **Intrusion Detection System** (**IDS)** and **Honey Pots**.

INTRUSION DETECTION SYSTEM:

The Intrusion Detection System (IDS) is a type of monitoring, which is designed to specifically detect malicious activities at the earlier opportunity in order to respond appropriately. The IDS is divided into two categories: the **Host-based Intrusion Detection System (HIDS)** and the **Network-based Intrusion Detection System (NIDS)**. The Host-based Intrusion Detection System (HIDS) uses software running in the system, to monitor the activity of the system itself – and to detect signs of malicious activity. HIDS runs at the level of the operating system, rather than at the network level, a common example is the **anti-virus software**, which is used to protect the system against computer virus attacks. On the other hand, the Network Intrusion Detection System (NIDS) uses software that examines network activity for signs of an intruder.

Research findings have shown that the most common type of IDS in use is the NIDS. Consequently, we shall examine some of the prominent Network based Intrusion Detection Systems:

(i) **SIGNATURE-BASED NETWORK INTRUSION DETECTION SYSTEM:**

This type of system works much like the virus-detection software. A database of signatures is developed for known attacks. The network intrusion detection system package listens to all network traffic passing by, compares it to the stored signatures, and triggers an alarm if it detects a match.

(ii) **ANALYSIS-BASED NETWORK INTRUSION DETECTION SYSTEM:**

This system is based on the analysis of packets. Instead of using signatures to screen the network traffic, this system actually examines or analyses the packets for signs of malicious user activity.

Upon detecting any such malicious user activity, the alert is issued. One of the first analysis based NIDS products was the shadow system which was designed by Stephen Northcutt and his crew for use at Navy Facilities. Shadow uses the freeware **top dump** to gather the headers from the network traffic. These headers are examined for signs of malicious activity.

(iii) **FIREWALLS:**

A firewall is a system (hardware, software or both), designed to control external access to a company's internal systems and information. The firewall approach is that computers holding sensitive information are isolated from the Net, while still being capable of receiving consumer information from it. The server computer, which does all the communication with outside users, acts as a '**middle man'**, receiving any confidential information, without storing it and then passing it on, via an internal link, to the organization's main computers. These main computers have no other link to the Net and are programmed to only respond to the server's computer. Thus, there is a fire wall protecting the main computer.

(iv) **ENCRYPTION PROGRAM:**

As the use of the e-mail has increased, so too has concern over the issue of the privacy and confidentiality of the mails. To solve the problem, the encryption program was developed. The approach of the program is to scramble your data before it leaves your browser. For this to work effectively, the recipient must have the same software with which to unscramble the message. The encryption program is not restricted to e-mails alone. It is also used to safeguard sensitive information in credit cards and other electronic cards, to prevent credit cards fraud.

HONEY POTS:

Honey pots are designed to attract potential hackers, the way honey draws insects. This idea is to cause would- be attackers to waste time and effort cracking what is (in effect) a fake target, giving you an opportunity to trace them, or decide how to respond to their attack.

Honey pots vary widely in scope. They can be as simple as a trap you can construct yourself, using tools such as **net cat**, or as elaborate as the two commercial products currently in use – **Man trap** and **Cyber Cop Sting**. The examination of these alternatives is beyond the scope of this paper.

CRITIQUE OF THE PRACTICE OF INTERNET SECURITY:

As was earlier observed, no security system can be full-proof. Every system must have its Achilles heel. Security is ultimately a process, not a product. It is an ongoing activity, not a once-and-for-all event. With the radical developments in the practice of information technology, there is the urgent need to beef up security in the sector.

Intrusion Detection and Honey Pots are both effective security systems when used appropriately. But they have their drawbacks. For example from research findings, a major weakness of the signature based network intrusion detection system is that the software is unable to detect new attacks if the signature does not match exactly. Thus, a clever hacker may modify the attack in some fashion to beat the system. Also, it has been observed that when overloaded, the performance of the system suffers. Thus a skilled attacker can render the system ineffective by carrying out multiple attacks on packets.

Another problem is that sometimes, the system is so sensitive, that they will not only pick up the activities of the hackers, but the activities of legitimate users may set off the alarm, thus constituting a nuisance.

Honey Pots can be a useful security system, but they have proved to be more time and resource consuming. The cost of maintaining the system is not commensurate with the level of security which it provides. Moreover, one of the early releases of **Man Trap**, a variant of the Honey Pots system, was found to have several security lapses. It would be an irony if your Honey Pot was used to break into your corporate network because of security holes in it.

CONCLUSION:

With the advent of the Internet, the world has become a global village. With the aid of the Internet, people can send and receive letters, files and information from all over the world. The web is the interactive, informative area with each area linked together so that you can move from one location to the other in an instant. This has posed a lot of challenges in the area of Information Security. I have tried to articulate the need to beef up security in this area. The strengths and weakness of the Internet control system have been examined.

My conclusion is that like every human system, the possibility of full-proof security is a mirage. I hope I have been able to stir the waters on this subject.

Thank you.

PETER A. AKHIHIERO ESQ.