Journal of Physical Science and Innovation
ISSN: 2277-0119
Volume 10, No. 1, 2018

A MULTI-DIMENSIONAL INTERNET SECURITY

Eloho Goodluck Okeno
Department of Computer Science
Delta State Polytechnic, Otefe, Oghara.

ABSTRACT

Today, the World Wide Web is used for information, commerce, news, weather, music, audio and video conferencing, database access, file sharing, with new features cropping up almost daily. Each has its own security concerns and weaknesses. The frequency and sophistication of Internet attacks have increased. These changes in the Internet community and its security needs prompted the first bona fide defense measures. The network must be protected from outside attacks that could cause loss of information, breakdowns in network integrity, or breaches in security. As the Internet has matured, however, so have the threats to its safe use, and so must the security paradigms used to enable business use of the Internet. This paper presentation summarizes a multi-dimensional (which is mandatory these days to discourage ever-more sophisticated threats to the network) approach to security in the present scenario as against a single-dimensional approach, which is no longer adequate, and very much a popular target to attack. The will eventually make the country a safer nation on the net.

INTRODUCTION

Single dimensional approach to security is unable to handle the commercialization of Internet and the changing dynamics of the attacks. Two widespread viruses—Melissa and the Love Bug—caused major disruptions of e-mail systems around the world. Business transactions when conducted over an insecure channel pose great risk and attract real criminal activity. A series of distributed denial-of-service attacks interrupted service at many high-profile sites, including Yahoo, CNN, and eBay. As against single dimensional approach, multi dimensional approach uses better security techniques thus preventing attacks that have disrupted businesses. This approach provides a defense mechanism, which gives a controlled and audited access.

Many people today are familiar with the Internet and its use. A large number of its users however, are not aware of the security crisis they face when using the Internet. Most users feel they are anonymous when on-line, yet in actuality they are not. There are some very easy ways to protect the user from future problems. The Internet has brought many advantages to its users but has also created some major problems. Most people believe that they are anonymous when they are using the Internet. Because of this thinking, they are not careful with what they do and where they go when on the "net." Security is a major issue with the Internet because the general public now has access to it. When only the government and higher education had access, there was no worry about credit card numbers and other types of important data being taken. There are many advantages the Internet brings to its users, but there are also many problems with the Internet security, especially when dealing with personal security, business security, and the government involvement to protect the users.

The Internet is an amazing and intimidating place. It can help make your dreams come true and it can manifest your worst nightmares. It is a global phenomenon and encompasses all aspects of modern day life from shopping to communicating off world. We use it as readily as the telephone or the car. In the click of a mouse you can order a shirt from a clothing store, buy a book and have it delivered to your door or book a vacation. This colossal convenience comes with an equally impressive responsibility. The potential for crime is directly proportional to this speed and convenience. Modern day muggers use the Internet to make off with your money and be long gone before you even know that anything is wrong. The only good thing about this is that you don't wake up with a bump on your head and a horrible headache.

Security is a growing business everywhere in the world and especially in the area of the Internet. Criminals are everywhere on the Internet and are just waiting for you to make a mistake. Therefore it is necessary for a heighten sense of awareness for the consumer.

The challenges of the internet security crisis are growing. With the electronic commerce spreading over the Internet, there are issues such as non-repudiation to be solved. Financial institutions will have both technical concerns, such as the security of a credit card number or banking information, and legal concerns for holding individuals responsible for their actions such as their purchases or sales over the Internet. Issuance and management of encryption keys for millions of users will pose a new challenge.

AIMS AND OBJECTIVES OF THE STUDY

The aim of this paper is to show that there is the need for a multi-dimensional approach to internet security in Nigeria.

The objectives of this study are as stated below:

- To examine the concept of internet security issues.
- To examine the various approach to curbing internet security
- To examine the various types of internet security mechanisms.
- To seek a purpose oriented solutions to internet security crisis and make recommendations that will go a long way in solving the identified problems.

DEFINITION OF TERMS

Access Control: Access Control ensures that resources are only granted to those users who are entitled to them.

Access Management Access: Management is the maintenance of access information which consists of four tasks: account administration, maintenance, monitoring, and revocation.

Active Content: Program code embedded in the contents of a web page. When the page is accessed by a web browser, the embedded code is automatically downloaded and executed on the user's workstation. Ex. Java, ActiveX (MS)

Activity Monitors: Activity monitors aim to prevent virus infection by monitoring for malicious activity on a system, and blocking that activity when possible.

Advanced Encryption Standard (AES): An encryption standard being developed by NIST, intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.

Asymmetric Cryptography: Public-key cryptography; A modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

Asymmetric encryption: An encryption method using a widely published public key to encrypt messages, and a corresponding private key to decrypt them.

Authentication: Authentication is the process of confirming the correctness of the claimed identity.

Authorization: Authorization is the approval, permission, or empowerment for someone or something to do something.

Autonomous System: One network or series of networks that are all under one administrative control. An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

Blended threat: An attack combining a number of traditional attack methods, like a worm, a Trojan horse, and a keylogger. Most require a combination of security tools and protection layers to defend.

Digital certificate: Also called *public key certificate* or *identity certificate*. In public key cryptography, validates that a public key is owned by the entity sending encrypted or digitally signed data with that key. Digital certificates are issued by a certificate authority and contain the sender's public key plus a digital signature verifying that the certificate is authentic and that the key belongs to the sender.

Digital signature: Used in public key cryptography to validate the integrity of encrypted data and to confirm both the identity of a digital certificate holder and the authenticity of the certificate itself.

Domain spoofing or Domain hijacking: Manipulation of the domain name system to associate a legitimate Web address with an imposter or otherwise malicious website. Used to perpetrate phishing and other types of attack, the user is sent to the imposter website with little or no warning.

Encryption: A security method that makes information unreadable to anyone who doesn't have a key to decipher it; commonly used to secure online purchases and other transactions. When a website indicates it's "secure," that usually means the data you send and receive is encrypted.

LITERATURE REVIEW

REVIEW OF RELATED LITERATURE

According to Andrew (2008), Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

The increased use of the Internet over the preceding decade has created considerable apprehension in the international community that it is being used to perpetrate various forms of fraud and economic crimes. Fears that the Internet has become an insecure environment in which to transact business have been widely discussed in the public media and the academic community alike and may have retarded the development of on-line commerce (Messmer, 2010).

Internet Security is the most important aspect of information technology. It has been years since computer has been invented and to keep the information confidential we have to safeguard this information. The importance of integrating security measures into systems development cannot be overemphasized. Every business has their own security systems to reach their goals of information security. The computer world created security systems in order to reduce risk, maintain confidentiality, ensure the reliability of data resources, and compliance with national security laws and privacy policies and laws (Bill, 2002).

According to Skinner (2012), in the on-line world, a crisis could be said to have occurred when one's computer stops working. This could take place through an interruption of the power supply, or because a malicious code such as a virus or worm has interfered with the proper functioning of the computer. A crisis in Internet fraud could also be seen to arise when a user receives a bill for thousands of dollars that relates to unordered goods or services obtained fraudulently by someone else on-line. If we are to believe the media, then such dishonesty is rife on the Internet.

PROBLEMS FACED BY SECURITY ON INTERNET

Fundamentally, the security problems on the Internet today come down to just two main problems:

i. Software for network services that is badly implemented

ii. A common desktop operating system with no protection against dangerous programs.

To break into a server on the network, one usually attacks individual network services that it provides (Web servers, mailers, file-transfer programs etc). The buffer-overrun bug in network softwares with which an attacker sends more input to a server than it is prepared to handle is a major typical case. If not checked it can disrupt the memory, causing it to execute the attackers' instructions.

The second problem is desktop operating systems without protected resources. Like Windows 95 and Windows 98, which are so susceptible to viruses that a program executed by a normal user on the system, can change anything about the system, often without being visible to the user. It is common to use "active content" or "active documents" that execute their own programs when opened. These are the same capabilities that enable an attacker to e-mail a dangerous program to a user.

VARIOUS TYPES OF SECURITY ISSUES ON THE INTERNET

Network layer security

TCP/IP can be made secured with the help of cryptographic methods and protocols that have been developed for securing communications on the Internet. These protocols include SSL and TLS for web traffic, PGP for email, and IPsec for the network layer security (Bradly, 2010).

IPsec Protocol

This protocol is designed to protect communication in a secured manner using TCP/IP. It is a set of security extensions developed by IETF, and it provides security and authentication at the IP layer by using cryptography. To protect the content, the data is transformed using encryption techniques. There are two main types of transformation that form the basis of IPsec: the Authentication Header (AH) and Encapsulating Security Payload (ESP). These two protocols provide data integrity, data origin authentication, and anti-replay service. These protocols **can be used alone or in combination to provide the desired set of security services** for the Internet Protocol (IP) layer.

The basic components of the IPsec security architecture are described in terms of the following functionalities:

- Security protocols for AH and ESP
- Security association for policy management and traffic processing
- Manual and automatic key management for the internet key exchange (IKE)
- Algorithms for authentication and encryption

The set of security services provided at the IP layer includes access control, data origin integrity, protection against replays, and confidentiality. The algorithm allows these sets to work independently without affecting other parts of the implementation. The IPsec implementation is operated in a host or security gateway environment giving protection to IP traffic.

Security token

Some online sites offer customers the ability to use a six-digit code which randomly changes every 30-60 seconds on a security token. The key on the security token have mathematical computations built-in and manipulate numbers based on the current time built into the device. This means that every thirty seconds there's only a certain possible array of numbers which would be correct to validate access to the online account. The website that the user is logging into would be made aware of that devices' serial number and therefore would know the computation and correct time built into the device to verify that the number given is in deed one of the handful of six-digit numbers that would work in that given 30-60 second cycle. After the 30-60 seconds the device will present a new random six-digit number which can log into the website.

Electronic mail security (E-mail)

Email messages are composed, delivered, and stored in a multiple step process, which starts with the message's composition. When the user finishes composing the message and sends it, the message is transformed into a standard format: an RFC 2822 formatted message. Afterwards, the message can be transmitted. Using a network connection, the mail client, referred to as a mail user agent (MUA), connects to a mail transfer agent (MTA) operating on the mail server. The mail client then provides the sender's identity to the server. Next, using the mail server commands, the client sends the recipient list to the mail server. The client then supplies the message. Once the mail server receives and processes the message, several events occur: recipient server identification, connection establishment, and message transmission. Using Domain Name System (DNS) services, the sender's mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client, delivering the message to the recipient(s).

APPROACHES TO INTERNET SECURITY ISSUES

SINGLE-LAYER, SINGLE DIMENSIONAL SECURITY

Before looking into multidimensional security techniques, let's have a look at what type of security techniques are available with us at present.

A single-layer, single-dimensional security system contains only one type of defense. The most common way of implementing this is: a router connects the site to the Internet, and a firewall protects the private network from being exposed to inherently insecure Internet protocols and corresponding services.

For example, most homes use single-layer security: a perimeter made up of locked doors and windows. In many cases, once this single level of security is breached, everything inside the house is vulnerable.

A firewall is a necessary part of the overall security, but alone it is insufficient to provide adequate network security.

MULTI-LAYER, SINGLE DIMENSIONAL SECURITY

Multi-layer, single dimensional security deploys additional internal firewalls for protection of one system from the rest of the organization as well as the Internet. However, the defense mechanism can be of any form as per the security requirements of the organization. An example of this type of security is a home with a wall around it, a locked gate, and locked doors and windows. The network equivalent is a setup that employs two or more firewalls — perhaps a simple filtering firewall and a more sophisticated application gateway firewall. An organization may deploy additional internal firewalls — to protect the accounting department, for example, from the rest of the organization as well as the Internet.

Nevertheless, these defense mechanisms are still of one type. And this setup does not provide protection from the people already on the inside of the network. To date, however, these systems have made relatively little progress in deployment, either because they are expensive or they are hard to use (sometimes, they are both).

Keeping in view the till date attacks and the flaws in the present security techniques multidimensional security will definitely cater to the security needs.

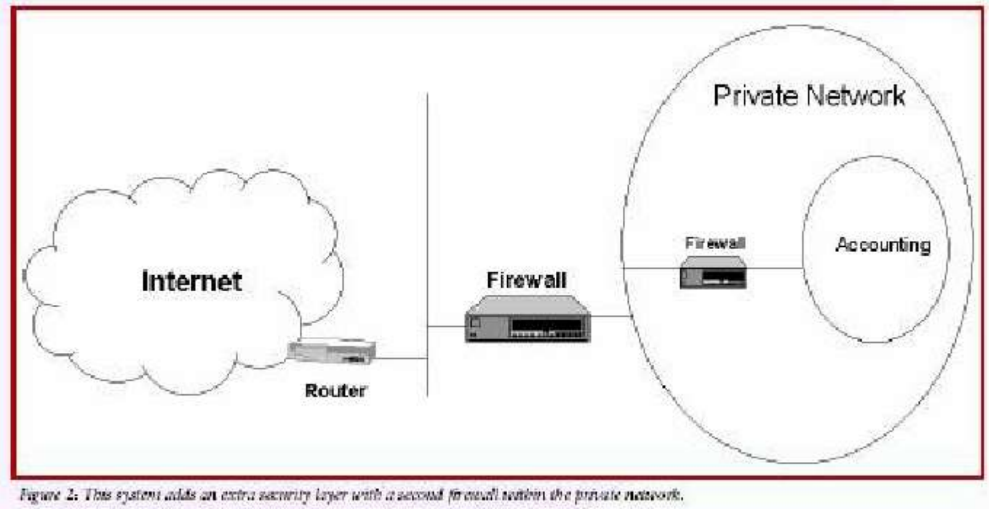

Figure 2: This system adds an extra security layer with a second firewall within the private network.

Figure 3.1: Multi-Layer, Single Dimensional Security

Multi-dimensional security uses different methods and mechanisms to create as comprehensive a security system as possible. With so many vulnerabilities, the defense requires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance.

Realization involves three distinct areas:

i. Steps in security management,

ii. Types of security,

iii. Platforms for deployment.

STEPS IN INTERNET SECURITY MANAGEMENT

It is the most important part of the multidimensional security. This can be achieved by implementing the following steps: Planning, policy and procedures; production and products; and research and analysis (Rolf, 2009).

Planning, Policy and Procedures

Security management starts with planning: a business-needs analysis and a risk analysis often triggered by a security survey. A company's business needs for connecting to the Internet may include the ability to send e-mail to clients, news services, electronic commerce, collaboration and corporate image projection. A risk analysis is an organization's review of potential threats to its network. A risk analysis attempts to answer such questions as "What am I trying to protect" and "What are the threats, vulnerabilities and risks?" A risk analysis ensures that a security policy matches reality. Because a security policy is a long-term document, the contents avoid technology-specific issues. Business-needs analysis and risk analysis provides a framework for making specific decisions.

Production and Products

The methods and mechanisms employed usually point to commercial off-the-shelf products, but may require homegrown software. They probably will include Internet firewalls, audit tools, encryption products (for Virtual Private Networks and application-level privacy, such as for e-mail), and anti-virus software. There are many security products to choose from and myriad product evaluations available.

Research and Analysis

Ongoing research and analysis are needed to keep up to date with potential attackers, as well as to keep abreast of the needs of employees to do their jobs while making use of the Internet's ever-expanding resources. Researchers postulate new threats and invent counter-measures for them, while reacting to actual new attacks in the cyberspace battlefield. Security audit logs and break-ins, both attempted and successful, must be analyzed. This analysis may reveal needed changes in the security policy and procedures, or in the devices deployed to protect a network.

TYPES OF INTERNET SECURITY MECHANISMS

There are different types of security mechanisms. Security products generally fall into three categories: prevention, detection, and response.

Prevention

Prevention mechanisms are meant to prevent break-ins, tampering or unwanted access. The Internet firewall is a classic prevention tool that controls access by individual, Internet service, source and destination.

Virtual Private Networks (VPNs) are used to prevent eavesdropping on communications. User authentication— can combine with access control mechanisms as part of an effective security scheme. Tools such as these, using cryptographic-based authentication tokens and access control lists, provide protection against unauthorized access to services and data. Content screening software and the old standby anti-virus software are still other prevention mechanisms. For example, a firewall with content screening can limit the downloading of Java or ActiveX code to only approved users and sites, or it can block viruses before they enter the network.

Detection

Detection devices add an important dimension to Internet security and constitute a second line of defense. Firewalls often detect and log all successful as well as unsuccessful attempts to use the firewall's services — triggered by events such as an attempt to connect to unsupported services on the Internet gateway.

Network and system scanners are two other types of detection tools. Network scanners survey network interfaces such as firewalls. System scanners do the same for server systems, looking for accounts without passwords, system files that can be written by anyone. Misuse and anomaly detectors constantly check a network or system.

Response

The third type of security system provides a response, like sounding an alarm, sending an e-mail message, or transmitting a message to a pager, misuse and anomaly detector systems can take defensive actions such as shutting down a log-in account, shunning connections from an attacker's Internet address, and replacing damaged files. Such systems are sometimes called "adaptive defense mechanisms."

THE PLACE OF FIREWALLS IN CURBING INTERNET SECURITY AND WEB SECURITY

Firewalls impose restrictions on incoming and outgoing packets to and from private networks. All the traffic, whether incoming or outgoing, must pass through the firewall; only authorized traffic is allowed to pass through it. Firewalls create checkpoints between an internal private network and the public Internet, also known as choke points. Firewalls can create choke points based on IP source and TCP port number. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network exposure by hiding the internal network system and information from the public Internet.

TYPES OF FIREWALLS

PACKET FILTERS: Packet filters are one of several different types of firewalls that process network traffic on a packet-by-packet basis. Their main job is to filter traffic from a remote IP host, so a router is needed to connect the internal network to the Internet. The router is known as a screening router, which screens packets leaving and entering the network.

CIRCUIT-LEVEL GATEWAYS: The circuit-level gateway is a proxy server that statically defines what traffic will be allowed. Circuit proxies always forward packets containing a given port number, provided the port number is permitted by the rules set. This gateway operates at the network level of an OSI model. The main advantage of a proxy server is its ability to provide Network Address Translation (NAT), which can hide the user's IP address from the Internet, effectively protecting all internal information from the Internet.

APPLICATION-LEVEL GATEWAYS: An application-level gateway is a proxy server operating at the TCP/IP application level. A packet is forwarded only if a connection is established using a known protocol. Application-level gateways are notable for analyzing entire messages rather than individual packets of data when the data are being sent or received.

MALICIOUS SOFTWARE AND ANTIVIRUS

Malware: Commonly, a computer user can be tricked or forced into downloading software onto a computer that is of malicious intent. Such programs are known as malware and come in many forms, such as viruses, Trojan horses, spyware, and worms. Malicious software is sometimes used to form botnets.

Viruses: Viruses are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.

Worms: Worms are programs that can replicate themselves throughout a computer network, performing malicious tasks throughout.

Trojan horse: A Trojan horse (commonly known as a Trojan) is a general term for malicious software that pretends to be harmless so that a user willingly allows it to be downloaded onto the computer.

Ransomware and Scareware: A botnet is a network of "zombie" computers that have been taken over by a "bot" that performs large-scale malicious acts for the creator of the botnet.

Spyware: The term spyware refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.

Antivirus: Antivirus programs and Internet security programs are useful in protecting a computer or programmable device from malware. Such programs are used to detect and usually eliminate viruses; however, it is now common to see security suites, containing also firewalls, anti-spyware, theft protection, and so on to more thoroughly protect users.

Traditionally, a user would pay for antivirus software; however, computer users now can, and do, download from a host of free security applications on the Internet.

CRYPTOGRAPHY AND THE ISSUE OF INTERNET SECURITY

High level encryption or cryptography is used in a number of applications ranging from those which impact national security to those which are more mundane. Essentially, cryptography is the methodology of encoding information so that one's privacy is ensured. This is particularly important when it comes to transactions which occur over the Internet. The risk of individuals gaining access to personal information or information which is critical to a country or a nation over the Internet is a very real one. The practice of cryptography lessens the likelihood of this happening (Gralla (2007).

Identification and Description of the Issue

A greater percentage of the world population is gaining access to the Internet and incorporating that access into their daily lives. More and more business transactions and personal transactions are occurring on the Internet. There is no questioning the fact that both the growth of the Internet and the number of sensitive transactions which occur on it are exponential.

In order to ensure the safety of Internet transactions, whether public or private, methodologies must be identified to safely and effectively encrypt information. Two methodologies are particularly associated with the issue of Internet security and deserve both an explanation and a contrast. These two methods are TCP/IP and cryptography.

CONCLUSION AND RECOMMENDATION

SUMMARY

Internet security crisis can damage data integrity, confidentiality or availability. Organizations must understand the potential costs: How would incorrect data affect decision making? What will happen if confidential information is made public? What is the cost (in lost time and credibility) of interrupted service? To understand threats, organizations should ask themselves: Does the information have a naira value? While more security equals more cost, the cost is slight compared to a single breakdown of services.

CONCLUSIONS

All of this technology exists today. Prices range depending on the deployment platform: Desktop and individual security is, of course, less expensive than server security, which in turn is less expensive than perimeter security. Typically, organizations start with desktop security such as anti-virus software. As they expand to Internet connectivity, perimeter defense mechanisms such as firewalls are deployed. As more sophisticated network access is needed, user authentication devices and VPNs are put in place. Intrusion and misuse detection devices are often next. Then, firewalls and intrusion detectors are spread across the internal network as access criteria become more granular. The mushrooming growth of the Internet is resulting in an expansion of possibilities for corporations that are serious about global business. But these companies must be equally serious about a well-thought-out, multi-dimensional approach to network security.¨

RECOMMENDATION

Haven established the fact that the Internet is a global network of interconnected computers, enabling users to share and transfer important and sensitive information such as credit card numbers and passwords; I hereby recommend that internet users should put security and privacy issues into consideration so as to avoid the loss or abuse of personal information.

REFERENCES

Andrew S. (2008). "Security of the Internet" 3rd edition The Internet Protocol Journal, June 2008 Volume 1, number 1

Bill Cheswick (2002), "The Design Of a Secure Internet Gateway," Proceedings of the 3rd USENIX Security Symposium, September 2002.

Bradly, Tony (2010). "It's Time to Finally Drop Internet Explorer 6"

Gralla, Preston (2007). How the Internet Works. Que Pub, Indianapolis. ISBN 0-7897-2132-5.

Messmer, E. (2010). All-in-one Security. "Google Chrome Tops 'Dirty Dozen' Vulnerable Apps List".

Rhee, M. Y. (2003). Internet Security: Cryptographic Principles, Algorithms and Protocols. Chichester: Wiley. ISBN 0-470-85285-2.

Rolf Oppliger (2009),"Internet Security: firewalls and Bey," Published in The Froehlich/Kent Encyclopedia of Telecommunications vol. 15. Marcel Dekker, New York, 1997, pp. 231-255.

Skinner, C. (2012) Opera Plugs "Severe" Browser Hole. Retrieved 19 November 2012.

Reference to this paper should be made as follows: Eloho Goodluck Okeno (2018), A Multi-Dimensional Internet Security. J. of Physical Science and Innovation, Vol. 10, No. 1, Pp. 18-38