Survey on the Network Security Incidents

Okoronkwo, Madubuezi C.

***Abstract*— This research is on the survey of Network security incidents .Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity. A recent survey on the network security incident has shown that security incidents are on the rise everywhere. Hackers frequently break into corporate organization and even military systems. Internet was originally conceived of and designed as a research and education network, usage pattern have radically changed. A typical attack pattern consists of gaining access to a user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites. The consequence of these incidents covers a broad range of possibilities: decrease in productivities, loss of money or staff man hour, loss of market opportunity, legal liability etc.**

***Index Terms*— Network, Security, Confidentiality, Integrity, Internet.**

I. INTRODUCTION

A network security incident is any network-related activity with negative security implication.This usually means that the activity violates an explicit or implicit security policy. Incidents come in all shapes and sizes. They can come from anywhere on the internet, although some attacks must be launched from specific systems or networks and some requires access to special accounts. An intrusion maybe comparatively minor event involving a single site or a major event in which tens of thousands of sites are affected. A typical attack pattern consists of gaining access to a user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites. It is possible to accomplish all these steps manually in a little as 45 seconds; with automation, the time decreases further. In many cases today, the "mediums" that hackers use to conduct illicit activities are "compromised" computers (sometimes called bots or botnets), usually owned by home Internet users and small businesses who are unaware that their computers have been "recruited" [1].

II. BRIEF BACKGROUND REVIEW

In 1986, the first well-publicized international security incident was identified by Cliff Stoll, then of Lawrence Berkeley National Laboratory in northern California. A simple accounting error in the computer records of systems connected to the ARPANET led Stoll to uncover an international effort, using the network to connect to computers in the United States and copy information from them [2]. In 1988, the ARPANET has its first network security incident, usually referred to as "the Morris worm". In 1989, the ARPANET became the internet and moved from a government research project to an operational network. Security problems continued, with both destructive and protective technologies becoming more refined. Today, the use of the World Wide Web and Web-related programming languages creates new opportunities for network attacks [3]. Intruders can steal or tamper with information without touching a piece of paper or a photocopier. They can create new electronic files, run their own programs, and hide evidence of their unauthorized activities.

Manuscript received October 21, 2014.

Okoronkwo, Madubuezi C., M.Sc. Department of Computer Science, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria

III. SOURCES OF INCIDENTS

It is difficult to characterize the people who cause incidents. An intruder may be an adolescent who is curious about what he or she can do on the internet, a college student who has created a new software tool, an individual seeking personal gain, or a paid "spy" seeking information for the economic advantage of a corporation or foreign country. A disgruntled former employee or a consultant who gained network information while working with a company may also cause an incident. An intruder may seek entertainment, intellectual challenge, and a sense of power, political attention, or financial gain. One characteristics of the intruder community as a whole is its communication [4]. There are electronic newsgroups and print publications on the latest intrusions, as well as conferences on the topic. Intruders identify and publicize mis-configured system; they use those systems to exchange pirated software, credit card numbers, exploitation programs, and the identity of sites that have been compromised, including account names and passwords. By sharing knowledge and easy-to- use software tools, successful intruders increase their number and their impact.

3.1. Types of incidents

Incidents can be broadly classified into several kinds; the probe, scan, account compromising, root compromise, packet-sniffer, denial of service, exploitation of trust, malicious code, and Internet infrastructure attacks.

A. Probe

A probe is characterized by unusual attempts to gain access to a system or to discover information about the system. One example is an attempt to log in to an unusual account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion.

B. Scan

A scan is simply a large number of probes done using an automated tool. Scans can sometimes to the result of a mis-configuration or other error, but they are often a prelude

to a more directed attack on systems that the intruder has found to be vulnerable.

C. Account compromise

An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges that a system administrator or network manager has). An account compromise might expose the victim to serious data loss, data theft, or theft of services. The lack of root-level access means that the damage can usually be contained, but a user-level account is often an entry point for greater access to the system.

D. Root compromise

A root compromise is similar to an account compromise; expect that the account that has been compromised has special privileges on the system. The term root is derived from an account on UNIX systems that typically has unlimited, or "super user", privileges. Intruders who succeed in a root compromise can do just about anything on the victim's system, including run their own programs; change how the system works, and hide traces of their intrusion.

E. Packet Sniffer

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travel over the network in the clear text. With perhaps hundreds or thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require privileged access. For most multi-user systems, however, the presence of a packet sniffer implies there has been a root compromise.

F. Denial of service

The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consumes a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.

G. Exploitation of trust

Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

H. Malicious code

Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some action on part of the user to spread inadvertently to other programs or systems. The sorts of programs can lead serious data loss, downtime, denial of service, and other types of security incidents.

I. Internet infrastructure attack

These are rare but serious attacks involving key components of the internet infrastructure rather than specific systems on the internet. Examples are network name servers, network access providers, and large archive sites on which many users depend. Widespread automated attacks can also threaten the infrastructure attacks affect a large portion of the internet and can seriously hinder the day-to-day operation of many sites.

3.2. Internet Vulnerabilities

Vulnerability is a weakness that a person can exploit to accomplish something that is not authorized or intended as legitimate use of a network or system. When vulnerability is exploited to compromise the security of systems or information on those systems, the result is a security incident. Vulnerability may be caused by engineering design errors or faulty implementation

3.3. Causes of internet vulnerability

Without a fundamental secure infrastructure, network defense becomes more difficult. Furthermore, the internet is an extremely dynamic environment, in terms of both topology and emerging technology. Because of the inherent openness of the internet and the original design of the protocols, Internet attacks in general are quick, easy, inexpensive, and may be hard to detect or trace [5]. An attacker does not have to physically present to carry out the attack. In fact, many attacks can be launched readily from anywhere in the world-and the location of the attacker can easily be hidden. It is always easy to break in to a site to compromise confidentiality, integrity, or availability of its information or service. This lack of secure configuration makes them vulnerable to attacks, which sometimes occur within minutes of connection.

3.4. Types of technical vulnerabilities

The following taxonomy is useful in understanding the technical causes behind successful intrusion techniques, and helps experts identify general solutions for addressing each type of problem.

A. Flaws in software or protocol design

Protocols define the rules and conventions for computers to communicate on a network. If a protocol has a fundamental design flaw, it is vulnerable to exploitation no matter how well it is implemented. An example of this is the Network File System (NFS), which allows systems to share files. This protocol does not include a provision for authentication; that is, there is no way of verifying that a person logging in really is whom he or she claims to be. NFS servers are targets for the intruder community [6]. When software is designed or specified, often security is left out of the initial description and later "added on" to the system. Because the additional components were not peat of the original design, the software may not behave, as planned and unexpected vulnerabilities may be present

B. Weakness in implementation of the protocols and software

Even when a protocol is well designed, it can be vulnerable because of the way it is implemented. For example, a protocol for electronic mail may be implemented in a way that permits intruders to connect to the mail port of the victim's machine and fool the machine into performing a task not intended by the service. If intruders supply certain data for the "To:" field

instead of a correct E-mail address, they may be able to fool the machine into sending them user and password information or gaining them access to the victim's machine with privileges to read protected files or run programs on the system. This type of vulnerability enables intruders to attack the victim's machine from remote site without access to an account on the victim's system. This type of attack often is just a first step, leading to the exploitation of flaws in system or application software. Software maybe vulnerable because of flaws that were not identified before the software was release. This type of vulnerability has a wide range of subclasses, which intruders often exploit using their own attack tools. For software design, the following examples of subclasses are included: Race conditions in file access, non-existent checking of data content and size, non-existent checking for success or failure, inability to adapt to resource exhaustion, incomplete checking of operating environment, inappropriate use of system calls, re-use of software modules for purposes other than their intended ones. By exploiting program weaknesses, intruders at a remote site can gain access to a victim's system. Even if they have access to a non-privileged user account on the victim's system, they can often gain additional, unauthorized privileges.

C. Weakness in system and network configurations

Vulnerabilities in the category of system and network configuration s are not caused by problems inherent in protocols or software programs. Rather, the vulnerabilities are a result of the way these components are set up and used. Products may be delivered with default settings that intruders can exploit. System administrators and users may neglect to change the default settings, or they may simply set up their system to operate in a way that leaves the network vulnerable. An example of a faulty configuration that has been exploited is anonymous File Transfer Protocol (FTP) service. Secure configuration guidelines for this service stress the need to ensure that the password file, archive tree, and ancillary software are separated from this staging area. When sites mis-configure their anonymous FTP archives, unauthorized users can get authentication information and use it to compromise the system.

IV. POLICY, PROCEDURE AND PRACTICE

4.1. Policy

A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long- term document, the contents avoid technology-specify issues. A security policy covers the following (among other topics appropriate to the organization):

- High-level description of the technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy.
- Risk analysis that identifies the site's assets, the threats that exist against those assets, and the cost of asset loss.
- Guideline for system administrators on how to manage systems.
- Definition of acceptable use f users.

Guidelines for reacting to a site compromise (e.gh, how to deal with the media and law enforcement, and whether to trace the intruder or shutdown and rebuild the system).

Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users. Management assigns responsibility for security, provides training for security personnel, and allocates funds to security. Technology support for the security policy moves some responsibility for enforcement from individuals to technology. The result is an automatic and consistent enforcement of policies, such as those for access and authentication. Technical options that support policy include (but are not limited to)

- Challenge/response systems for authentication
- Auditing systems for accountability and event reconstruction
- Encryption systems for the confidential storage and transmission of data.
- Network tools such as firewalls and proxy servers.

4.2. Procedure

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such as retrieving programs from the network, connecting to the site's system from home or while travelling, using encryption, authentication for issuing accounts, configuration, and monitoring.

4.3. Practices

System administration practices play a key role in network security. Checklists and general advice on good security practice are readily available. Below are examples of commonly recommended practices:

Ensuring all accounts have a password and that the passwords are difficult to guess. A one-time password system is preferable.

- Using tools such as MD5 checksum (8), a strong cryptographic technique, to ensure the integrity of the system software on a regular basis.
- Using secure programming techniques when writing software. These can be found at security-related sites on the World Wide Web.
- Being vigilant in network use and configuration making changes as vulnerabilities become known.
- Regular checks with vendors for the latest available fixes and keep systems current with upgrades and patches.
- Regular check on-line security archives, such as those maintained by incident response team, for security alerts and technical advice.
- Audit systems and networks, and regularly check logs. Many sites suffer computer security incidents report that insufficient audit data is collected, so detecting and tracing an intrusion is difficult.

V. NETWORK SECURITY TOOLS

To reduce the vulnerability of the Network Security incidents, there are many tools available. These tools are:

5.1. Encryption

This is a method of altering data so that it is not useable unless one change is undone. An example is the "Pretty Good Privacy" (PGP) a computer program written for encrypting computer massages that is putting them into secret codes. When data is encrypted, it is then scrambled to descript them, you must unscramble it. Encryption scrambles message before transmission. This will prevent interceptors to read the message as it flows over the network.

5.2. Digital signature

Digital signature allows us to authenticate each message that an applicant send. It is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

5.3. Integrated Security system

For smooth communication between two computers, there is need to implement several forms of security, and we need a process for doing this systematically and automatically. Integrated Security System (ISSs) implements this board spectrum of activities automatically as illustrated in figure 1below.

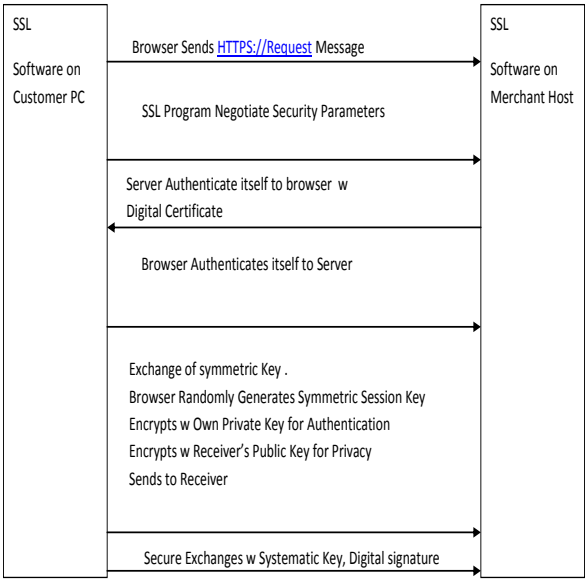

Figure 1: Integrated Security System (ISSs)

5.4. Multi-layer security

In multiplayer security, security can be applied in any layer. Often, as in figure.., illustrates, integrated security systems are implemented at several layers. Old and established security algorithms have a nasty record of having hackers discover security problems after years of effective use. If a security is employed at a multiple layer, a single breakdown in an algorithm will not compromise security. On the negative side, each layer of security produce delays and increases costs. Table 1 shows a Multi-layer security

Table 1: Multi-layer security

Layer	Example
Application	Application-specific(for instance, passwords for a database program)
Transport	SSL (TLS)
Internet	IPsec
Data Link	Point-to-Point Tunneling Protocol, layer 2 Tunneling Protocol
Physical	Physical locks on computers

5.5. Firewalls

Intruders often attempt to gain access to networked systems by pretending to initiate connection from trusted hosts. They squash the emissions of the genuine host using a denial-of-service attack and then attempt to connect to a target system using the address of the genuine host [7]. To counter these address-spoofing attacks and enforce limitations on authorized connections into the organization network, it is necessary to filter all incoming and out coming network traffic. A firewall is a collection of hardware and software designed to examine a stream of network traffic and service requests. Its purpose is to eliminate from the stream those packets or request s that fails to meet the security criteria established by the organization. In addition to network management, set rules about access and be accessed , cut off access which is prohibited, the firewall in the computer systems also need to analysis and filter out the data package, to monitor and record content and activities of the information through the firewall. It also can detect and alarm the attack acts from the network. These are the basic functions of the firewall. Whether hardware firewall or software one should have these five basic functions. Firewall works in the network layer or application layer. Firewall working in the network layer filters the information of transmission mainly through packet filtering technology, which selects the data in the network exports (routers) .Just only those packets that meet the conditions are allowed to pass, and others are abandoned. Network layer firewalls can allow the host and the servicer which are authorized, directly access to the internal network. You can also filter a specified port and Internet address information of the internal users, and limit the internal network to access the external network. The application layer firewall is to control applications access [8]. It is essentially an application gateway, also called a proxy server (Proxy Server). When users use a TCP / IP applications, the proxy server will ask users to provide external network host name. If the users answer and provide the correct user identity and authentication information, the proxy server establishes connections between internal network and Internet hosts, and acts as a relay for two communication entities.

VI. RESULT ANALYSIS AND DISCUSSION

From the design and implementation of security measures in our networks emerge the following results.

6.1. Cryptography

Cryptography is the science of writing in secret code. It secures information by protecting its confidentiality. It can be used to protect information about the integrity and

authenticity of data. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. There are three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions.

A. Secret Key Cryptography

With secret key cryptography, a single key is used for both encryption and decryption. As shown in the figure, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. Figure 2 shows Secret Key Cryptography.

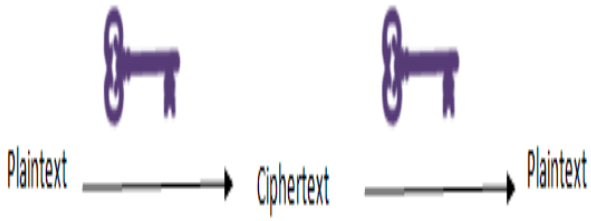

Figure 2: Secret Key Cryptography using a single key for both encryption and decryption

B. Public Key Encryption

Public-key cryptography has been said to be the most significant new development in cryptography. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme. Figure 3 shows Public Key Encryption.

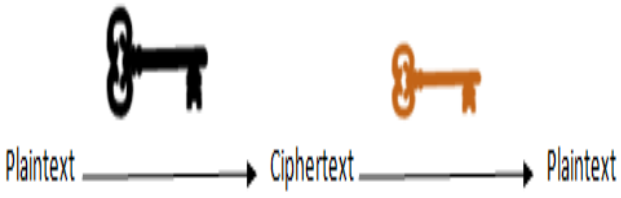

Figure 3: Public Key Encryption using two keys, one for encryption and the other for decryption

C. Hash Functions

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file. Figure 4 shows a Hash Function

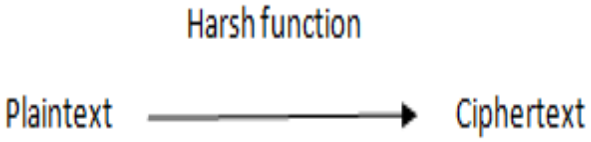

Figure 4: Hash Function, have no key since plaintext is not recoverable from ciphertext

6.2 Operational technology

A variety of technologies have been developed to help organizations secure their systems and information against intruders. These technologies help protect systems and information against attacks, detect unusual or suspicious activities, and respond to events that affect security. No single technology addresses all the problems and threats. Nevertheless, organizations can significantly improve their resistance to attack by carefully preparing and strategically deploying personnel and operational technologies. Data resources and assets can be protected, suspicious activity can be detected and assessed, and appropriate responses can be made to security events as they occur.

6.3. Security analysis tools

Because of the increasing sophistication of intruder methods and the vulnerabilities present in commonly used applications, it is essential to assess periodically network susceptibility to compromise. A vulnerability identification tools are available, which have gained praises.

6.4. Authentication

One purpose of encryption is to prevent anyone who intercepts a message from being able to read the message. Encryption brings confidentiality, which is also called privacy.

6.5. Integrity

Digital signatures do more than authenticate the message. Integrity is an important by-product of digital signatures. Integrity, in terms of data and network security, is the assurance that information can only be accessed or modified by those authorized to do so.

6.6. Availability

Availability of information refers to ensuring that authorized parties are able to access the information when needed. Ensures that a system is operational and functional at a given moment, usually provided through redundancy; loss of availability is often referred to as "denial-of-service"

6.7. Access control

Access control ensures that users access only those resources and services that they are entitled to access and that qualified users are not denied access to services that they legitimately expect to receive

6.8. Non-Repudiation, Authentication, Confidentiality Authorization and Privacy

One purpose of encryption is to prevent anyone who intercepts a message from being able to read the message. Encryption brings confidentiality, which is also called privacy. Privacy ensures that individuals maintain the right to control what information is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted, the user cannot later deny that he or she performed the activity. This is known as non-repudiation.

VII. SUMMARY OF RECENT INTERNET NETWORK SECURITY THREATS, DATE AND ITS AREA OF ATTACK.

Below is the summary of recent threats, date and its area of attack.

Table 2: summary of recent internet network security threats, date and its area of attack

NAME OF THREAT	DATE DISCOVERED	TARGET SYSTEM
Tequila Polymorphic viruses	June 18, 1991	System running and network servers
Michelangelo panic	March 6, 1992	Computer hard disks
Hoax	Sep. 7, 1994	Computer hard drive
macro virus	Aug. 30th, 1995	MS word
Morris	Nov.2, 1988	VAX and SUN-3 running Blerckly UNIX
Melissa	Mar. 26, 1999	System running Unpatched Microsoft IIS
Code Red 1	Jun.19, 2001	Microsoft windows 2000 and other systems with IIS 4.0
Nimda	Sep.18, 2002	System running Microsoft window 95, 98, NT and 2000 with IIS
SQL Slammer	Jan.25, 2003	System running Microsoft window SQL
BOT Roster 1	Nov. 3, 2005	System running and network servers
Nyxem version D	Jan.2006	System running and network servers
Bot Roast 11	Nov.29, 2007	Microsoft windows 2000 and other systems with IIS 4.0
Conficker	Apr.4, 2009	System running and network servers
Stuxnet	Jun, 2010	System running Microsoft windows
Lulzraft	Apr., 2011	System running and network servers
FORTS3V3N	May 4, 2012	Network servers
iThug	Feb. 18, 2013	Microsoft windows and network servers

VIII. ANALYSIS AND CONCL USION

From the result in Table 2, it is obvious to say that the mainly rampant internet security threats are Tequila Polymorphic, Michelangelo panic, Hoax, Macro virus, Morris, Melissa, Nimda, SQL Slammer, BOT Roster Nyxem Version D, Bot Roast, Conficker, Stuxnet, Lulzraft, FORTS3v3N, iThug, whileVirtual Private Network (VPN), IPSec, Anti-Malware Software and scanners, Secure Socket Layer, intrusion-detection, security management, firewalls, encryption and cryptography mechanisms has been identified as a veritable means of securing Internet Network Systems. In this research, the evaluation of Network Security incidents has been reviewed with a combination of diverse security system tools.

REFERENCES

[1] Caelli, W., Longley, D., and Shain, M., Information Security Handbook, Stockton Press, New York, 1991.

[2] Denning, P.J. ed., Computers Under Attack Intruders, Worms and Viruses, ACM Press, Addison-Wesley, New York, 1990

[3] CERT coordination center, CERT advisories and other security information, CERT/CC, Pittsburgh, P.A. Available on line: http://www.cert.org.

[4]"SecurityOverview,"www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[5] Garfinkel, S., and Spafford, G. Practical UNIX and Internet Security, 2nd ed, O'Reilly & Associates, Sebastopol, C.A. 1996

[6] Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). An inquiry into the nature and causes of the wealth of Internet miscreants. *Proceedings of the ACM Conference on Computer and Communications Security*, Washington, DC, October 29-November 5, 2007.

[7] Chapman, D.B. and Zwicky, E.D. Building Internet Firewall, O' Reilly & Associates, Sebastopol, C.A, 1995.

[8] Chapman, D.B. and Zwicky, E.D. Building Internet Firewall, O' Reilly & Associates, Sebastopol, C.A, 1995.

Author

Okoronkwo Madubuezi C. is currently a lecturer in Computer Science Department of Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria. He has a Bachelor Degree in Computer Science from Michael Okpara University of Agriculture, Umudike, and a Master's Degree in Computer Science from Ebonyi State University, Abakaliki. He is presently pursuing a PhD programme in Computer Science from Nnamdi Azikiwe University, Awka, Anambra State of Nigeria with interest in System analysis, Design and Development. He is a member Computer Professionals of Nigeria..