Network Security and Privacy in Medium Scale Businesses in Nigeria

Modesta .E. Ezema[1] , Ifeyinwa .N. NwosuArize[2]

[1]Department of Computer Science, University of Nigeria Nsukka
[2]Department of Health Economices, University of Nigeria Nsukka

Abstract— *Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. This study investigates a general framework for assessing the security and privacy of current networks. We ask a more general question: what security and privacy mechanisms are available to the medium sized businesses in Nigeria and to what extent have they utilized these mechanisms for the safety of organizational data. The study made use of both primary and secondary data sources. The primary source was a questionnaire administered to a total of 105 medium scale businesses in some of states i, Nigeria. The result showed that medium scale businesses in Nigeria store electronic data to a very high extent but lack the adequate hardware/software to prevent unauthorized access to electronically stored data. However, many of these companies do not have official policy as regards customer data privacy. In cases where they exist, customers are not aware of such policies. This study therefore recommends that government and regulatory bodies should give serious attention to network security and privacy of medium scale businesses in Nigeria. Network security standards should be set for any organization setting up or providing a wireless network. Government should also review existing data privacy laws and ensure that customers are aware of such laws before engaging in any transaction that involves giving aware their personal data to the third party.*

Keywords— Network security, privacy, wireless network, data privacy, businesses.

I. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technologies [1]. Internet itself is now acting as a data store which has information related to personals, commercial, military and government sectors. So security of this kind of data is taken as a serious aspect [2]. Fundamentally there are two different types of networks and they are: Synchronous Network and Data Network [2]. The internet is considered a data network. Since the current data network consist of computer based routers , information can be obtained by Synchronous Network and Data Network [2]. The internet is considered a data network. Since , information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources [3]. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions.

Network attacks have been discovered to be as varied as the system that they attempt to penetrate. Attacks are known to either be intentional or unintentional and technically competent intruders have been interested in targeting the protocols used for secure communication between networking devices [9].

Businesses face an increasingly diverse and sophisticated array of threats to the security of their information management systems. Cyber theft, fraud, sabotage, espionage, and hacking (including from governments) [4] are more frequent in the social media age and the associated costs with information security breaches are increasing for entities in every industry sector—from Retail, Financial Institutions, Healthcare, Hospitality, Media, Communications, Technology, Consulting and Professional Services to Manufacturing and Transportation [5]. For instance, recent hacktivist attacks have targeted energy companies, agribusiness, political parties, media outlets, educational institutions, religious groups, governmental entities, and even organizations devoted to cybersecurity [6].

The hacking of The Associated Press' Twitter account in April 2013 caused a fake tweet about the White House being the target of a bomb that injured President Obama, causing the stock market to plunge—a $136 billion drop in the Standard & Poor's 500 Index [7]. A group of international cybercriminals hacked into two credit card processors, India-based EnStage and ElectraCard Services, and withdrew $45 million from two Middle Eastern banks through ATMs in 24 countries in just over 10 hours [8]. Global Payments, Inc., a payments processor, suffered a security breach in the spring of 2012, exposing an estimated 1.5 million Visa and Mastercard accounts and losses in excess of $84 million.

Sadly enough, many medium sized businesses in Nigeria do not employ adequate network security and privacy measures to secure organizational data. With the advent of mobile technology, leakage of personal information, especially one's identity may invite malicious attacks from the real world and cyberspace, such as stalking, reputation slander, personalized spamming, and phishing [10]. We believe that more effective and flexible security mechanisms are therefore required for the safety of customers as well as the continued thriving of these organisations. In this article we present a general framework for assessing the security and privacy of current networks. We ask a more general question: what security and privacy mechanisms are available to these medium sized businesses in Nigeria and to what extent have they utilized these mechanisms for the safety of organizational data.

II. LITERATURE REVIEW

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.There exists a "communication gap" between the developers of security technology and developers of networks [11]. Network design is a well-developed process that is based on the TCP/IP model. The TCP/IP model has several advantages when designing networks. It offers

It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well-developed process. It is in a growing stage. There is no proper methodology developed to manage the complexity of security requirements.The protocols of different Secure network design does not contain the same advantages as network design. When considering network security, it must be emphasized that the whole network is secure. Network security does not concern the security in the computers at each end of the communication chain. When transmitting data, the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message. To reduce the vulnerability of the computer to the network, there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Businesses throughout the world are using a combination of some of these tools. The Internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the Internet greatly assists in developing new security technologies and approaches for networks with Internet access and Internet security itself.

2.1 Common Network Attack Methods

Common Internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and Trojans. The other form of attack is: when the system's resources are consumes uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not so popular like DoS attacks, but they are used in some form.

Eavesdropping

Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way [12].

Viruses

Viruses are self-replication programs that use files to infect and propagate [12]. Once a file is opened, the virus will activate within the system.

Worms

A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate [12]. There are two main types of worms, mass-mailing worms and network-aware worms. Mass mailing worms use email as a means to infect other computers. Network-aware worms are a major problem

for the Internet. A network-aware worm select a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

Trojans

Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus [12].

Phishing

Phishing is an attempt to obtain confidential information from an individual, group, or organization [13]. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

IP Spoofing Attacks

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IPspoofed packets cannot be eliminated [12].

Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors [13]. Until the handshaking is complete, the system consumes resources. Eventually, the system cannot respond to any more requests rendering it without service.

2.2. Technology for Network Security

Different defence and detection mechanisms were developed to deal with different attacks. These include:

Cryptographic systems

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

Firewall

A firewall is a typical border control mechanism or perimeter defence. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defence mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [12].

Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack. Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware. Anti-Malware tools are used to detect them and cure an infected system.

Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, between a web browser and the web server, so that any information exchanged is protected within the secured channel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity

Current Methods Used In Network Security

The network security field is growing by implementation of new features. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented. The research being performed assists in understanding current development and projecting the future developments of the field. Hardware developments as well as software development are also active areas in computer security.

Hardware Developments

The main use of Biometric network security will be to replace the current password system. Maintaining password security can be a major task for even a small organization. Passwords have to be changed every few months and people forget their password or lock themselves out of the system by entering incorrect password repeatedly. Very often people write their password down and keep it near their computer. This is of course completely undermines any effort at network security. Biometrics can replace this security identification method. The use of biometric identification stops this problem and while it may be expensive to set up at first, these devices save on administration and user assistance costs.Smart cards are usually a credit-card-sized digital electronic media. The card itself is designed to store encryption keys and other information used in authentication and other identification processes. The main idea behind smart cards is to provide undeniable proof of a user's identity. Smart cards can be used for everything from logging in to the network to providing secure web communications and secure e-mail transactions. It may seem that smart cards are nothing more than a repository for storing passwords. Obviously, someone can easily steal a smart card from someone else.

Fortunately, there are safety features built into smart cards to prevent someone from using a stolen card. Smart cards require anyone who is using them to enter a personal identification number (PIN) before they'll be granted any level of access into the system. The PIN is similar to the PIN used by ATM machines.

When a user inserts the smart card into the card reader, the smart card prompts the user for a PIN. This PIN was assigned to the user by the administrator at the time the administrator issued the card to the user. Because the PIN is short and purely numeric, the user should have no trouble remembering it and therefore would be unlikely to write the PIN down. The PIN is verified from inside the smart card. Because the PIN is never transmitted across the network, there's absolutely no danger of it being intercepted. The main benefit is that, the PIN is useless without the smart card, and the smart card is useless without the PIN. There are other security issues of the smart card. The smart card is cost-effective but not as secure as the biometric identification devices.

Software Developments

The software aspect of network security is very vast. It includes firewalls, antivirus, VPN, intrusion detection, and much more. The research development of all security software is not feasible to study at this point. The goal is to obtain a view of where the security software is heading based on emphasis being placed now. When new viruses emerge, the antivirus is updated to be able to guard against those threats. This process is the same for firewalls and intrusion detection systems. Many research papers that have been skimmed were based on analysing attack patterns in order to create smarter security software. As the security hardware transitions to biometrics, the software also needs to be able to use the information appropriately. Current research is being performed on security software using neural networks. Many small and complex devices can be connected to the internet. Most of the current security algorithms are computational intensive and require substantial processing power. Research in this area is currently being performed.

III. RESEARCH METHODS

Both primary and secondary data were used for the study. The researchers used a questionnaire as a key instrument for data collection. Secondary data was obtained from relevant literature like journals, internet and books. The use of questionnaires was preferred as it ensured confidentiality, saves time, and easy to administer. The primary data related to inquiries on what security and privacy mechanisms are available to medium sized businesses in Nigeria and to what extent they have utilized these mechanisms for the safety of organizational data. The questionnaire has two sections: section A, which contains the respondents' personal information and section B, which contains the research questions.

The instrument has a four point scale: "Very High Extent", High Extent", "Very Low Extent" and "Low Extent". Participants were asked to respond by ticking the box that actually reflected their opinions.

Data collected from the questionnaire will be analyzed, summarized, and interpreted accordingly with the aid of descriptive statistical techniques such as, mean and standard deviation. 4.0 Data Analysis

Table 1: Mean and standard deviation showing the extent of network security and privacy awareness in medium scale business in Nigeria.

S/N	Items	N	Mean	SD	DEC
1	Company stores data electronically	105	3.70	.47	VH
2	Company employs hardware/software to prevent unauthorized access to electronically stored data	105	2.36	.49	L
3	Company maintain wired/ wireless network	105	3.40	.49	H
4	The network is encrypted	105	2.33	.49	L
5	The software/hardware that prevents unauthorized access in routinely updated	105	2.70	.47	H
6	Electronically stored data are backed up in external facility or process	105	1.40	.47	VL
7	Company periodically test the security controls in place to prevent unauthorized access to personal information or records	105	1.40	.49	VL
8	Company in the past few years has suffered any network attack	105	2.35	.49	L
9	Company has any official policy as regards customer data privacy.	105	1.50	.42	L
10	Company revise this policy to meet current issues of concern	105	2.32	.42	L
11	Company gives away (on request) customer information to third party (government, organization	105	2.33	.82	H

	or individual) without his/her consent.				
12	Our customers are aware of our data privacy policy	105	1.40	.47	VL
	Cluster mean	105	2.35	.36	L

H=high extent, VH = Very high extent, L=low extent. DEC= Decision.

IV. SUMMARY AND CONCLUSION

Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. Analysis showed that medium scale businesses in Nigeria store electronic data to a very high extent but lack the adequate hardware/software to prevent unauthorized access to electronically stored data.

However, many of these companies do not have official policy as regards customer data privacy. In cases where they exist, customers are not aware of such policies. This calls for serious attention. The fact that these companies have suffered minimum attacks on their networks in the past few years, as compared to their counterpart in the developed world, does not eliminate its possibility. This study therefore recommends that government and regulatory bodies should give serious attention to network security and privacy of medium scale businesses in Nigeria. Network security standards should be set for any organization setting up or providing a wireless network. These standards also should be updated to meet the current trend in security challenges. Government should also review existing data privacy laws and ensure that customers are aware of such laws before engaging in any transaction that involves giving aware their personal data to the third party.

REFERENCES

[1] Bhavya DayaNetwork Security: History, Importance, and Future University of Florida Department of Electrical and Computer Engineering. 2014

[2] Murthy, B. V., Vuppu P. and A. Vasavi Significances and Issues of Network Security *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 3, Issue 6, June 2014

[3] KPMG Data Loss Barometer 2012 (January 2013) (http://www.kpmg.com/EE/et/IssuesAndInsights/ArticlesPublications/Documents/Data-Loss-Barometer.pdf)

[4] Carnegie Mellon University, Governance of Enterprise Security: Cylab 2012 Report: How Boards & Senior Executives Are Managing Cyber Risks, J. Westby, Author, May 16, 2012. http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf

[5] Verizon 2013 Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/2013/

[6] J. Weisenthal and S. Ro, "AP Just Got Hacked And A Fake Tweet Caused The Stock Market To Tank," *Business Insider*, 23 Apr 2013. http://www.businessinsider.com/ap-tweeton- white-house-2013-4#ixzz2WJq7OhFk

[7] B. Browdie, "Card Processors Attacked in 45 Million Bank Heist Identified," American Banker, May 13, 2013. *http://www.americanbanker.com/issues/178_91/card-processorsattacked- in-45-million-dollar-bank-heist-identified-1059040-1.html?zkPrintable=1&nopagination=1*

[8] Reed D. November 21, 2003. Network Model to Information Security. Retrieved: Available at: *http://www.sans.org/reading_room/whitepapers/protocols/applying-osilayer-networkmodelinformation-security_1309*

[9] Jaiswal, M. (2014). IP Security architecture, application, associated database, and mode. *International Journal Of Research And Analytical Reviews (IJRAR)*, *1*(1), 446-453.

[10] ENISA, "Security Issues and Recommendations for Online Social Networks," Position Paper, Nov.2007; http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[11] Purna C. S. and Prafulla K. B., Methods of Network Security and Improving the Quality of Service – A Survey *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com India Volume 5, Issue 7, July 2015 ISSN: 2277 128X*

[12] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. *Second Asia International Conference*, vol., no., pp.77-82, 13-15 May 2008

[13] Marin, G.A., "Network security basics," *Security & Privacy*, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005.