Implementation of Network Security in University Libraries: An Overview

Daniel Chuks Oriogu,[1] Sussan Udoaku Ogbuiyi,[2] Ngozi Oluchukwu Odiaka,[1] and Olumide Johnson Akanmidu[3]

[1] Afe Babalola University, Ado-Ekiti, Ekiti State
[2] Babcock University Illisan-Remeo, Ogun State, Nigeria
[3] Federal University Lafia, Nasarawa State

Abstract

The reliability and integrity of university libraries on the Internet which serves as the "network of networks " should be highly guided and protected in order to avoid the ravage of institutional repositories. Network security is a systematic protection of the network against threats and vulnerabilities. It is a necessity to university libraries especially now, that most of them are being digitalized and resources hosted on the Web. The paper presents Internet use in university libraries, the role of network in information service provision in university libraries, network security and its adaptability to information services provision and defense mechanisms. Therefore, the paper suggests that, university libraries should endeavour to provide effective network defense mechanisms so that their resources and the technology supporting it, will not be exposed to threats.

Keywords: Internet use, Network, Network Security, University Libraries

Introduction

Network security is a major concern for university libraries especially now that most academic libraries all over the world are adopting ICT (Information and Communication Technologies) in the provision and management of their resources. Today the computer, hand-held mobile devices and the Internet has become the most popular types of ICTs widely used in academic libraries. Many studies now show that students and lecturers connect to the resources of University libraries through mobile devices, inside and outside the premises of the Library. Hidda (2011) asserts that use of these applications and the services over computer networks are rapidly increasing day by day and computer users are becoming more advanced and demanding new services, quality of services, and high availability. These demands however, require reliable computer networks. While enabling the reliable services to users, libraries need to avoid unauthorized access that would compromise the integrity and reliability of their collections online by implementing proper filtering mechanisms.

The Internet is a veritable treasure of information sources that has enabled libraries to perform their information services beyond the physical confines of their own collections which has greatly boosted the service delivery of libraries. Therefore, to ensure the safe use of the Internet in libraries, there should be necessary security mechanisms put in place to protect information resources against all types of threats. Thus, the increased use of Internet services in academic institutions has ushered in, the need for network security. Stallings (2003) said that the continuous growth in computer systems and networks has increased the dependence of both organisations and individuals on the information stored and communicated using these systems. This leads to a sharp awareness of the need to protect data and resources to disclosure, to guarantee the authenticity of data and messages, and protection of systems from network-based attacks. Alabady (2009) also agreed that due to the evolution of networking and the Internet, the threats to information and networks have risen dramatically. As DeeAnn and Scott (2006) maintain, libraries are becoming more involved in the security area, not only as users of networked resources, but also as repositories of protected or confidential data. It stands to reason therefore that, academic institutions should protect their networks from possible unauthorized intrusion and other attacks. This needs to be part of the daily routine of the institutional information technology (IT) unit as it is essential to safeguard institutional information assets. Therefore, this paper reviews the implementation of network security in university libraries.

Internet use in university libraries

Internet is an information source that is vital to academic performance of students in academic institutions and also enables the library to provide information resources beyond the limits of its physical collections and space so as to effectively facilitate teaching, learning and research development. Sinha (2012) asserts that Internet is a network of networks connecting thousands of smaller computer networks together so that other networks may share information present in one network. The Internet is acknowledged globally as a technology dominated mostly by young people, and particularly students who are more inclined to exploit Internet resources for education, social interactions and entertainment (Salako and Tiamiyu, 2007). In a research conducted on 883 school students in Lebanon, Hawi (2012) indicated that 84.2% students used the Internet for communication and email, 65.7% for information search and for research, and 51.8% for entertainment such as online games and music. Also, Tiemo, Bribebena and Nwosu (2011) noted that Internet has a lot of promises for educational achievements for young people but certain drawbacks such as fraud, currency counterfeiting, theft of intellectual property, pornography, recipes for crime, and infecting systems with virus are also associated with the Internet.

Nevertheless, the Internet has become a global source of information resources accessible at anytime by anyone from anywhere in the world. It has converted the whole world into a global information society. It has tremendously improved communication and interaction among scientific research communities and enabled access to a vast range of latest information in every field of knowledge. It acts as a powerful supplement to the traditional way of information access. It facilitates electronic and exchange of ideas and collaboration among the scholars all over the world (Devi and Singh, 2009).

The need for Internet in university libraries is most necessary for students' academic progress; as it has greatly facilitated access to and use of information resources for students to carry out their academic activities. Awoleye, Siyanbola and Oladapo (2008) assert that Internet is used for information development, enhances easy communication, improves academic performance, used as a research tool, provides solutions to assignments, gives information on entertainment and education, and a source of scholarship. Therefore, university libraries in Nigeria should ensure steady and available Internet services to its users in order to benefit tremendously in their academic activities. As Agboola (2000) recommended that:

> Nigerian University libraries must take advantage of modern communication and information technologies to open up their contents. All Nigerian University libraries should be fully automated and linked to the Internet. This will enable them to communicate easily with one another and to share their resources. It will also open up to them the resources of libraries located outside the country.

Similarly, Ajiboye and Telia (2007) are also of the view that "if quality in higher education is to be attained in Africa, a more radical and positive approach to the provision of Internet facilities in our tertiary institutions must be adopted".

However, Jagboro (2003) carried out a study of Internet usage in Nigerian universities where opinion of 73 respondents was sought for on specific uses of Internet, two-third of the respondents indicated that they used it for e-mail, to get research materials and also recorded that low level of utilization of the Internet was attributed to the low level of connectivity and the high cost of cybercafe facilities. Also Oriogu, Ogbuiyi, Chukwuemeke and Ogbuiyi (2015) carried out a study on the assessment of Internet use in Afe Babalola University and found out that majority of the respondents use the Internet for research, course assignment and learning more about a subject. Studies have shown that a lot of students are really using Internet for academic purposes in Nigeria (Audu, 2006; Salaam and Adegbore, 2010; Ayub, Hamid and Nawawi, 2014).

The role of network in information service provision in university libraries

The advent of Internet technology has immensely contributed to the access and use of information resource in the academic institutions where students and academic staff have really gained profitably in the services of the Internet which has invariably increased the output of research. The Internet service is highly dependent on the network which is a fundamental fink to library service provision. Therein, over dependence of academic libraries on Internet services needs to be protected because of the vulnerability of networks. According to Reitz (2004) network is a group of physical discrete computers interconnected to allow resources to be shared and data exchanged, usually by means of telecommunication links and client/server architecture. Thus, network is the combination of information technology based components designed for the communication of various forms of information, such as voice, data, text, image, etc to connect within and between organizations. Daya (2008) asserts that there are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as “Trojan horses,” planted in the routers. Herein, 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 fink to the internet. With the advent of personal computers, LANs, and the wide- open world of the Internet, the networks of today are more open. As e-business and Internet applications continue to grow, finding the balance between being isolated and being open will be critical (Alabady, 2009).Therefore, the reliability of academic libraries on the Internet which serves as the “network of networks” should be highly guided and protected to avoid wreck of institutional assets.

Network security and its adaptability to information services provision

Network security is a systematic protection of the network against threat and vulnerabilities. Network security refers to all hardware and software functions, characteristics, features, operational procedures, accountability measures, access controls, administrative and management policy required to provide an acceptable level of protection for hardware, software, and information in a network (Alabady, 2009). It is the most vital component in information security because it is responsible for securing all information passed through networked computers (Chen, Iyer, and Whisnant, 2002; Kim, 2004). Network security is a necessary means of achieving a secured information asset in an academic environment. Without adequate protection, many individuals, academic institutions, businesses, and governments are at risk of losing their assets as malware or malicious software attacks may result in unauthorized disclosure of information, denial of services, or system downtime. Dhepe and Akarte (2013) assert that the most common computer security threats are fraud and theft, errors and omissions, malicious code, and malicious hackers, employee sabotage, integrity threat, denial of service (DOS), disclosure threat, social engineering and phishing and memory space. Onwubiko and Lenaghan (2007) assert that in 2001, the Code Red incident exploited a buffer overflow in a library module of Microsoft Windows' Internet Information Server - this allowed it to infect hundreds of thousands of computers (Moore, Shannon, and Brown, 2002), causing millions of dollars of damage.

Libraries are becoming soft targets for hacking since its resources are now hosted on the web and the Internet is considered as a major source of malware infection. In some cases, even legitimate sites can be infected with malware that can be downloaded to connecting computers. According to SophosLabs (2011) more than 30,000 websites are infected every day and 80% of those infected sites are legitimate. Newby (2002) noted that modern OPACs include functionality to make the holdings information searchable via a Web interface. Here lies the substantial security risk: Unix systems have many potential security flaws, and many well-known flaws have easy exploits available to any potential intruder therefore, connecting a system with critical data to the Internet is a bad idea. On the Internet, tens of thousands of amateur (and professional) potential intruders may try to get access to the system.

Even if the OPAC software itself is thought to be relatively free of security problems - a risky assumption to make - the underlying Unix operating system is almost definitely not. Yet, this potential risk needs to be balanced by the desire to make OPAC services available to the outside world. Also Newby (2002) provided the following recommendations for a secured OPAC:

O Only services needed should be running on the OPAC computer(s). Specifically, all Unix services (such as email, FTP, login, telnet) that are not required for OPAC functions should be disabled.

o System logs must be kept, and analyzed regularly (daily or weekly) by staff. A logins record should be maintained; integrity checkers such as Tripwire should be used to spot illicit changes to the system software, and the system should be audited regularly for usernames, programs or data that are no longer used.

O Ideally, the OPAC should only communicate with authorized terminals. For example, computers located within library buildings. If outside (Internet) access is required, the ideal scenario is to have a duplicate of the holdings database (or other information, if needed) on a separate server. This way, if the duplicate server were compromised, the original data and services would be intact.

o Personnel must be specifically responsible for monitoring security updates from the OPAC vendor, as well as the underlying Unix system vendor.

o Regular attempts should be made to bypass OPAC security from both within the library (at computer stations) and outside the library via the Internet.

According to Sanchez (2010), the following are ten of the biggest network threats:

a. Viruses and Worms: A virus is a malicious computer program or programming code that replicates by infecting files, installed software or removable media. Whereas a worm is a programme or script that replicates itself and moves through a network, typically travelling by sending new copies of itself via email.
b. Trojan Horses: The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Some Trojans are designed to be more annoying than others and they can cause serious damage by deleting files and destroying information on your system.
c. Spam: Spam is any kind of unwanted online communication.
d. Phishing: Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

e. Packet Sniffers: Computer network administrators have used packet sniffers for years to monitor their networks and perform diagnostic tests or troubleshoot problems.
f. Maliciously Coded Websites: Malicious code is the term used to describe any code in any part of a software system that is intended to cause security breaches or damage to a system.
g. Password Attacks: Password attacks are the classic way to gain access to a computer system is to find out the password and log in.
h. Zombie Computers and Botnets: In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e:mail spam and launch denial of service attacks. Most owners of zombie computers are unaware that their system is being used in this way.

The rationales behind network security are to ensure confidentiality, maintain integrity, and assure availability. DeeAnn and Scott (2006) opine that:

> Managing network security in the library requires cooperation among computing areas to put into place policies, technology and technology practices that will reduce threats caused either intentionally or unintentionally by people using computing resources. This cooperation extends to federal, state and academic units. This is important since networks, like other utilities, cross jurisdictions making it possible to launch attacks from both inside and outside the organization. Within the university, the library must coordinate technology practices with other information technology units.

Therefore, university libraries have greater role to play in order to ensure that their intellectual assets are not invaded and compromised by hackers. Dowd and McHenry (1998) said that when developing a secure network, the following need to be considered:

a. Access - authorized users are provided the means to communicate to and from a particular network
b. Confidentiality - Information in the network remains private
c. Authentication - Ensure the users of the network are who they say they are
d. Integrity - Ensure the message has not been modified in transit
e. Non-repudiation - Ensure the user does not refute that he used the network

Nevertheless, university libraries as a matter of fact, should endeavour to provide effective network security, so that its resources and computer system will not be infuse by virus and also they should provide an effective monitoring policy and adopt an effective network architecture that will highly support its Internet services.

Defense mechanisms

University libraries have always embraced their call to share information, but they must also be cognizant of their responsibilities to protect information and the systems that information resides in order to maintain and ensure effective and reliable information services. As long as information users continue to access and transfer information across the Internet, threats will continue to be a major issue. The following are different defense and detection mechanisms developed to deal with these attacks.

a. **Cryptographic systems:** It involves the use of codes to transform information into unintelligible data. Cryptography is the ability to send information to the receiver in a way that prevents others who do not have business with the information from reading it. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium (Kessler, 2016). Also, Kessler (2016) discussed the three kinds of cryptographic functions as follows:

o Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
o Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
o Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

It is pertinent to note that, a message in its original form is known as **Plaintext.** The coded information is known as **ciphertext.** The process for producing ciphertext from plaintext is known as **encryption.** The reverse of encryption is called **decryption,** a. Firewall: It is a system designed to prevent unauthorized access. The essence of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. Therein, a firewall protects the internal network from external network. It can be implemented in both hardware and software, or a combination of both (Adeyinka, 2008). Stallings (2011) discuss the following parameters of firewall:

I. Service control: Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.

II. Direction control: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

III. User control: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPsec.

IV. Behaviour control: Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

b. Intrusion Detection Systems (IDS): “Intrusion detection systems (IDSs) are hardware or software systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems. IDS make use of audit trails and network packets to detect intrusions which stores information such as date and time of the event, type and origin of the event, objects accessed, modified, or deleted”. There are two types of IDSs analysis to detect attacks: Signature-based detection which looks for events that match a predefined pattern of events, called signatures, associated with a known attack (Bace and Mell, 2001). Signature-based detectors are effective in detecting common forms of attacks without generating an overwhelming number of false alarms. A limitation of signature-based detectors is that they can only detect those attacks they know about (Cavusoglu, Mishra, and Raghunathan, 2005). In order to maintain its functionality to combat new threats, it must have to be regularly updated with signatures of new attacks. Anomaly detection identifies unusual behaviour. However, its main purpose is to detect attacks that have not been previously recognized and catalogued. Unfortunately, anomaly detection often produces a large number of false alarms because normal patterns of users and system behavior can vary widely (Cavusoglu, Mishra, and Raghunathan, 2005).

Conclusion

The emergence of information and communication technology has created a new paradigm shift in service delivery in academic libraries. As most university libraries are totally or partially automated, and their resources are hosted on the web, there is the need to implement reliable technologies to secure network and computer systems from malicious hackers and codes. Nevertheless, university libraries should adopt an effective defense mechanism to protect their systems and network from vulnerable attach. It is therefore quite apparent that for university libraries to confidently transact on the Internet it must fully develop and maintain effective network security defense in order to facilitate smooth access and use of information resources. Librarians are thereby enj oined to avoid being soft targets for hacking by safeguarding collections online.

References

Adeyinka, O. *(2008).* Internet attack methods and Internet security technology. *Modeling and Simulation, AICMS 08. Second Asia International Conference,* pp.77-82. www.dl.acm.org Agboola, A.T. (2000). Five decades ofNigerian University libraries: a review. *Libri,* (50): 280-9. Ajiboye, J. & Telia, A. (2007). University undergraduate students' information seeking behaviour: implications for quality in higher education in Africa. *The Turkish Online Journal of Educational Technology — TOJET,* 6(1): 40-54 www.tojet.net

Alabady, S. (2009). Design and implementation of a network security model for cooperative network. *International Arab Journal ofe-Technology.* 1(2): 17- 19.

Awoleye, O.M., Siyanbola, W.O. & Oladapo, O.F. (2008). Adoption assessment of Internet usage amongst undergraduates in Nigeria universities: a case study approach. *Journal of Technology Management and Innovation,* 3(1): 84-89.

Audu, C.D. (2006). Internet availability and use by postgraduate students of University of Nigeria, Nsukka. *Global Review of Library and Information Sciences, (2):*34-43.

Ayub, A.F.M., Hamid, W.H. & Nawawi, M.H. (2014). Use of Internet for academic purposes among students in Malaysian institutions of higher education. *The Turkish Online Journal of Educational Technology.* 13 (1): 232-241. www.tojet.net

Bace, R. & Mell, R (2001). NIST special publication on intrusion detection systems. SP-800- 3 1 National Institute of Standards and Technology. ww.csrc.nist.gov.pub

Cavusoglu, H., Mishra, B. & Raghunathan, S. (2005)77ze *value of intrusion detection systems in information technology security architecture. Information Systems Research,* 16(1): 28—46.

Chen S., Iyer R. & Whisnant K. (2002). Evaluating the security threat of firewall data corruption caused by instruction transient errors," *In Proceedings of the 2002 International Conference on Dependable Systems and Network, Washington, D.C.* www.itsec.gov.cn Daya, B. (2008.) Network security: History, importance, and future. University of Florida, Department of Electrical and Computer Engineering. http://www.pdfdrive.net/network-security-history-importance-and-future-e 16301 .html Daraman, M. (1997). Importance of Internet to libraries. *HeartLand Journal of Library and Information Science,* 1(2): 12-19.

DeeAnn, A. and Scott, C. (2006) Computer network security and ARL Libraries. *Faculty Publications, UNL Libraries.* Paper 53.

http://digitalcommons.unl.edu/libraryscience/53 Devi, T.P. & Singh, Y.N. (2009). Internet users: a study of Manipur University Library. www.crl.du.ac.in/ical09/papers/

Dhepe, Y.V. & Akarte, S.P. (2013) Security issues facing computer users: An overview. International Journal of Computer Science and Applications, 6(2): 263 -267. www.researchpublications.org Dowd, P.W. & McHenry, J.T. (1998). Network security: it's time to take it seriously. *Computer,* 3 1 (9):24-28

Hawi, N.S. (2012). Internet addiction among adolescents in Lebanon. *Computers in Human Behavior,* (28): 1044-1053.

Hidda, M.G. (2011). Network-wide security analysis. A dissertation submitted in partial fulfillment for the degree of Doctor of Philosophy (Computer Science and Engineering), Faculty of Information Technology, Brno University of Technology. www.fit.vutbr.cz

Jagboro, K.O. (2003). A study of internet usage in Nigerian universities: Acase study of Obafemi Awolowo University, Ile-Ife, Nigeria. *First Monday,* 8(2-3).

http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fin/article/^Tesj'/e^

G. C. (2016) An overview of cryptography. http://www.garykessler.net/library/crypto.html Kim H. (2004) Design and implementation of a private and public key crypto processor and its application to a security system. *IEEE Transactions on Consumer Electronics,* 50 (1). www.ceng.metu.edu.tr

Moore, D., Shannon, C. & Brown, J. (2002) "Code-Red: a case study on the spread and victims of an Internet Worm", Proceedings *of the ACM/USENIX Internet Measurement Workshop France, November, 2002. https ://www. caida. rg/papers/2002/*

Newby, G.B. (2002) Information Security for Libraries. http://www.petascale.org/papers/library-security

Onwubiko, C. & Lenaghan, A. P. (2007) Managing security threats and vulnerabilities for small to medium enterprises. IEEE International Conference on Intelligence and Security Informatics.www.research-series.com/IEEE-ISI07/

Oriogu, C.D., Ogbuiyi, S.U., Chukwuemeka, A.O. and Ogbuiyi, D.C. (2015). Assessment of Internet use in the Provision of Information to Students in University Libraries in Nigeria: A Case study of Afe Babalola University Library, Ekiti State, Nigeria. *Advances Social Sciences Research Journal (ASSRJ), 2{* 1):211 - 218.

Reitz, J.M. (2004). *Dictionary of Library and Information science.* Westport: Greenwood Publishing Group.

Salaam, M.O. & Adegbore, A. M. (2010). Internet access and use by students of private universities in Ogun State, Nigeria. *Library Philosophy and Practice.* http://unllib.unl.edu/LPP/salaam-adegbore.htm

Salako, O.A., and Tiamiju, M.A. (2007). Use of search engines for research by postgraduate students of the University of Ibadan, Nigeria. *African Journal of Library, Archives and Information Science,* 7(2):103-115.

Sanchez, M. (2010). The 10 most security threats explained, www.blogs.cisco.com Sinha, M.K. (2012) Internet literacy skills and internet usage patterns to access e-resources by Assam University Library users: an evaluative study. International Research Journal of Library, *Information and Archival Studies,* 1(1): 10-26. http://www.interesjoumals.org/IRJLIAS

Sophos Lab (2011). Who ordered Spam? New trick in PDF malware uncovered.

https://nakedsecurity.sophos.com Stallings, W. (2011) *Network Security Essentials Applications and Standards,* 4th ed., New Jersey: Pearson Education, 376-377

Stallings, W. (2003) *Network Security Essentials Applications and Standards,* 2nd ed., New Jersey: Pearson Education, 6

Tiemo, P.A., Bribebena, E. & Nwosu, O. (2011) Internet usage and regulations in Niger Delta university libraries. *Chinese Librarianship.* http ://www.iclc.us/cliej/c 131 TBN.pdf.