COMPUTER BASE NETWORK SECURITY AND FIREWALLS IN BANKING SYSTEM

1. Dr. H. A Eneh
Lecturer

2. C.C Nnaji
Researcher

3. L.O Odo
Researcher

Abstract

Computer based network are connected system on a network sharing same resources with a firewalls preventing unauthorized access to confidential information thereby enhancing the security architecture. Information security in the banking sector is heavily controlled as banks store and manage their clients' private information. Information security has always been the responsibility of the information technology (IT) department in financial institution. Banks have become a component of the internet and daily lives. It is a real task to protect these bank procedures, systems from the attackers and minimize the security threats. With this Cyber-attacks increasing day by day, and this is the challenge facing by countries and organizations like banking where data is critical. These banks should be built networks using secure strategies to protect their components. However, the performance of the network is affected by applying security rules. Network security is an essential priority for protecting applications, data, and network resources. Applying resource isolation rules are very important to prevent any possible attack. This isolation can be achieved by applying the DMZ (Demilitarized Zone) design. A DMZ extremely enhances the security of a network. In this paper perimeter network security framework is proposed to the protection and minimize the cybersecurity issue that exists in Libyan banks effectively. The computer based network security and firewalls in banking system requires an intensive security protection in firewalls in banking system thereby providing privacy and integrity on private information's of customers using the method DMZ.

KEYWORDS: COMPUTER BASED, FIREWALLS, NETWORK SECURITY.

1.0 **INTRODUCTION**

Computer based systems are personnel computer interconnected within a network connect using any network connection topology eg bus, mesh, star etc. The systems on network share common resource. The conflict on computer base system on network is the comprisable vulnerable nature of the connection method. The privacy, security and integrity of systems on network is the actual context of this paper work. The vulnerability of the system on network in financial institutions causes a lot of damage to confidential document thereby both customer and bank owner are the point of huge losses. Intensification of bank systems security is the initial priority of the banking management. To avoid unauthorized access to confidential data in the banking system/server a firewalls in banking system is built.

The advancement in technology in the Nigerian Banking sector cannot be done without the use of computers, networks and internet and hence the need to protect the organization's computer and network from unwanted users and malicious attacks becomes very important. Cybercrime and other unintended use which makes it easy to steal a kobo from millions of bank accounts than traditional or conventional bank robbery is becoming predominant despite the positive impact of the advancement in information and communication technology has on the society. [4] Technology has progressed so much that it would be of no surprise if your computers are hacked and you are completely unaware of the reasons for it. Any organization should monitor its system for potential unauthorized access and several kinds of attacks, in other to safeguard sensitive information. [5].

Banking sector in its delicateness is a trust-based institution, that requires an absolute trust from her customers, upon this the banking sector should take security issues as a special concern to continually earn the trust of their customers, The need to tighten-up security and proper management channels that could give opportunities for fraud and malicious attacks such as: breach of privacy of customer data, distributed denial of service attacks, and technological letdowns created on electronic banking platforms becomes expedient.

The most fundamental computer based system in an organization pertains to the processing of business transactions. A transaction processing system can be defined as a computer based system that captures, classifies, stores, maintains, updates and retrieves transaction data for record keeping and for input to other types of CBIS. Transaction Processing Systems are aimed at improving the routine business activities on which all organizations depend. A transaction is any event or activity that affects the whole organization. Placing orders, billing customers, hiring of employees and depositing cheques are some of the common transactions. The types of transactions that occur vary from organization to organization.

Throughout the evolution of computer networks and the Internet, there is one thing that can beat the speed of this evolution: the speed of the evolution of security risks threats and attacks. To understand the reasons behind the development of security, it is necessary to look back at the history of networks and security together. The first successful attempt to build a network in which data can travel from one end of the country to the other was initiated by the Defense Research Projects Agency (DARPA) in 1969. Initially four organizations from around the USA were selected to participate in this project. The University of California Los Angeles (UCLA), the University of California at Santa Barbara, the University of Utah and the Stanford Research Institute (SRI) were the four organizations among which a network was established. This network was called Advanced Research Projects Agency (ARPANET), which later became the Internet we know today. After those four organizations, other academic institutions, defense-related companies and governmental organizations joined the network. (Leiner, Cerf, et al., 2003)

A firewall is a legal barrier preventing the transference of inside information and the performance of financial transactions between commercial and investment banks. Restrictions placed on collaborations between banks and brokerage firms under the Glass-Steagall Act of 1933 acted as a form of firewall. One purpose of a firewall is to ensure banks do not use regular depositors' money to fund highly speculative activities that could put the bank and depositors at risk. The firewall in banking is a barrier to prevent

2.0 LITERATURE REVIEW

In this section discuss the related literatures which have provided solutions in an organizational or technical approach. Angelakopoulos and Mihiotis (2011) studied the challenges of e-banking for the banking sector in Greece, during the e-commerce era and the study shown that the low response rate from customers and the implementation of security and data protection mechanisms are the main problems faced by banks. Shuaieb (2013) suggested an analysis of the factors affecting Internet banking adoption in Libya. The author highlighted the challenges facing the spread of electronic banking in Libya, such as, the weakness of security systems achieved in the field of electronic commerce and the lack of an appropriate environment for electronic commerce.

Folorunso et al. (2016) introduced an online questionnaire to assess the computer and network security strategies for Nigerian Banks as a case study, the samples are limited to computer security experts and information technology department staff in banks. The security strategy that they are asking is regarding passwords, antivirus, firewalls, encryption, IDS, and IPS. Also, the study investigates if the Nigerian banks have experienced any form of attacks on their systems. The security strategy of the Internet-based services, which require more security strategy such as DMZ, is not mentioned in the study.

The study findings that Nigerian banks are using effective computer and network strategies after, implementing almost all security strategies and they rarely experience malicious attacks of any form. Tytarenko (2017) proposed study to design the first line of defense enterprises based on the selection of the best security controls. A NIST SP 800-53, revision 4 uses as a primary reference for selecting the best security controls. The author selected thirteen of controls to build the first line of defense. However, some important controls did not appear in the study result, which they are necessary to build the first line of defense. Dart et al. (2018) studied the Science DMZ architecture, configuration, cybersecurity and performance. They used supercomputing centers and research laboratories to highlight the effectiveness of the science DMZ model. They concluded that Science DMZ model enhance collaboration, accelerating scientific discovery.

Rababah et al. (2018) used OPNET simulator to assess the effect of DMZ on network performance. The author used three scenarios, first without DMZ and Firewall, second with Firewall and third with DMZ. The results show that DMZ solves many critical performance problems, also they found that DMZ is not only to improve network security, but it is also to improve network performance.

3.0 Comparative Study on Banking Systems and Security

The integrated banking system (Core Banking System) preferred to other CBS software? Core Banking Systems gives room from the implementation most or all security strategies on them and this could be found on any of the following Integrated Banking System application: AX, Finnacle, SAP, T24, Microsoft CRM, Phoenix, and Flexcube. As result of the resident security strategies on the core banking system this goes to show that a relationship exists between computer security strategies implemented by banks and the Integrated Banking System. Thus, there is a great impact from the Integrated Banking Systems on computer security strategies implemented in the banking sector. This displayed that Flexcube polled highest followed by some respondents who did not write the name of the integrated banking system used by their banks, while Finnacle polled one of the least results. So the need to review why Flexcube would be preferred becomes important. The following are some of the features the Oracle Flexcube possess:

1. Capability to process large transaction volumes, with high value of availability all day.
2. A channel support of multiple delivery, which including branches, point-of-sale terminals, ATMs, mobile devices, call centers, and internet banking
3. A Web-based user interface resident on XML with context-sensitive help
4. Role-based access and application are covered by Security management.
5. Exception processing which is automated and online validations.
6. Combination deployment which could either be centralized or decentralized.
7. Existing systems are easily integrated using Enterprise Edition technology, flexible Java Platform.

Helps with collateral, and nonperforming assets which are Operational risk management controls.

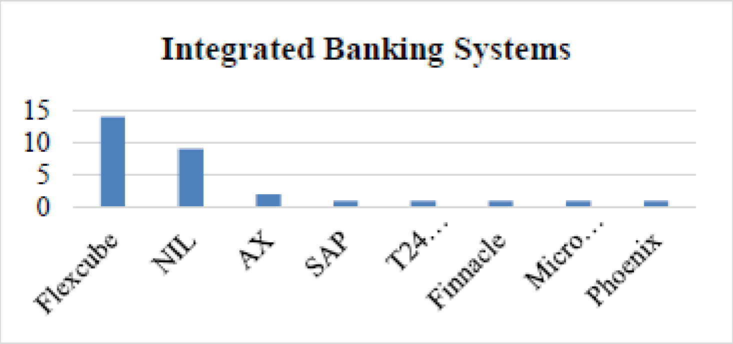

Figure 3.0 Integrated banking systems [source: Ogunwobi, et al (2016)]

Public Demilitarized Zone (DMZ) - Private Network Layout

In addition to the implementation of the Defense in Depth concept, Arconatti (2002) proposes the implementation of "Tiered Networks". This is to ensure that the most important data will be stored in the most secure segment of the network. The "Tiered Networks" approach divides the network architecture into three main segments: Public, Demilitarized Zone (DMZ), and Private. The Public-DMZ-Private setup is widely applied in many networks (Rosamond, 2004). Public is the global Internet, on which enterprise security staff do not have any control. Private is the enterprise network, where access from the Internet is prohibited. DMZ is a network segment, which serves as a buffer zone between the public and private network segments. The servers for users outside the enterprise are located in the DMZ. Access to the DMZ is not prohibited but limited to some ports. Since there is no complete solution for the security of the Internet, there should be a separation between the company's network and the Internet. That is why the public and private parts must exist in every network. Since there are some services that should be publicly accessible such as e-mail and web, the servers of these services must be located in between the Internet and the organization's network, which is the DMZ. Arconatti (2002) defines the segments of the approach with different terms:

1. The Internet tier consists of the global Internet. The enterprise security policy does not control every device on the Internet, but does enforce requirement upon these devices accessing the enterprise network.
2. The Extranet tier consists of a protected extension of the corporate Intranet. This extension is often protected by a demilitarized zone (DMZ). In some cases, the DMZ is the extranet tier.
3. The Intranet tier consists of the private enterprise network" Arconatti, (2002)

In order to provide better security, some additions can be applied to the basic public-DMZ-private layout. Instead of using one DMZ, more than one DMZ can be created, and application servers can be grouped and located in those zones. By creating more than one DMZ, access control can be applied more efficiently. For example, in a complex network, three DMZs may be created: management DMZ, database DMZ and external DMZ. The management servers of security devices are located in the management DMZ, while the database servers are located in the database DMZ, and other application servers are located in the external DMZ. In this layout, additional security may be applied to database servers and access to the database DMZ can be restricted to only application servers.

Complexity Problem and Management Difficulties

Networks grow as new security products, which have their own management consoles, screens, and logs to be handled by the security administrator, are added. These different devices have different locations in the network layout. Most of them are produced by different companies and are intended to be managed in a decentralized fashion. Thus, decentralized management and log handling is the default setting in many organizations. As a result, the correlations between the logs of these different systems cannot be easily checked, and the relations between them cannot be discovered easily. Sources, destinations, reasons, methods and consequences of possible intrusions cannot be detected as expected, thus the assumed benefits of the security products may not be realized. Managing system security in an enterprise is becoming more and more complicated, since security administrators are inundated with a very high number of logs coming from different security devices such as firewalls, intrusion detection / prevention systems, anti-virus systems, routers, switches and other peripherals. All these various devices have their own management consoles, interfaces and way of presenting the logs. They all require administrators to spend time on managing the device and analyzing the logs of the device, which is a factor that may degrade the efficiency of the administrators.

However, incident handling and security management, which are the main assignments of a security administrator, requires the review of all the logs in a regular and timely fashion and quick response in order to prevent any kind of hostile network intrusion attempt, and recover from an incident as soon as possible. Although enhanced central management devices and software are available today, they are expensive and still require a great deal of human interaction. Hyland and Sandhu (1998) discussed that every method of security management requires human presence to some degree at every security device along with manual handling and evaluation of the security logs. Nevertheless, remote monitoring and centralized management with correlation and aggregation capabilities are seen as viable solutions for network security management.

Even though these correlation and aggregation capabilities are useful, those systems are far from providing a full solution. The problem is due to several reasons such as the lack of universal standards for log generation, inadequate correlation capabilities of the software compared to the human brain, along with the price of the software.

Design a Secure Network Software Facilities

The main goal of designing secure networks is to manage the risks as effectively as possible, rather than eliminating all the threats Bertagnolio, (2001). Security administrators ask six questions about the incidents: Why, Who, What, Where, Why and How. A secure network, in principle, should be designed to provide the administrators the answers to these questions. A secure system must have all the watching, monitoring and logging capabilities Abramson, (2001). In one of its articles, the Microsoft tech-net web site identifies 10 immutable laws of security administration Microsoft, (2007). One of the laws of security administration is listed as 'the most secure network is a well-administered one'. This sentence indicates the importance of the configurations of the network. Actually most successful attacks are not executed by exploiting a flaw in the software, but by taking advantage of the misconfigurations in the network. Another important law of security administration is about the complexity of the network. It states that 'the difficulty of defending a network is directly proportional to its complexity'. Keeping it simple, documenting every configuration change, updating security policies are all good components of successful security management.

Defense-in-Depth

The concept of Defense-in-Depth is a layered approach to network security. The basic definition of Defense-in-Depth is “not putting all the eggs in one basket” Miles, (2004). This simple analogy refers to not putting all the emphasis on a single defense mechanism for the protection of a network, but relying on several different security measures in a layered approach. There is no single product in the security products market, which can completely protect networks from all the different types of threats. Applying security countermeasures in multiple layers improves the overall strength of the security. In this approach, if a security precaution fails, there is another level of protection that can prevent the attack. Defense-in-Depth is a widely used practice for building secure networks. In this strategy, the plan is to install different security software in such a way that those installations would provide challenges for attackers. These different security software may overlap with each other, but there should not be any gaps between the layers. An intruder has to navigate through all the measures to find the target. With all these levels of security measures and careful monitoring, the probability of launching an attack without leaving any trace decreases. Different security precautions at each level mean different technologies and diverse methods of protection to be overcome by the attacker. Scott Rasmussen (2002) discusses the issue as “The more layers, to a degree, the stronger the security and the more diversity the more comprehensive the protection”.

4.0 Discussion and Conclusion

The computer based network security and firewalls in banking system (CNSFBS) presented in this paper, overcomes most of the shortcomings of the old decentralized way of handling the security of a network. Public Demilitarized Zone (DMZ) - Private Network Layout is the context method suggested firewall for banking system interfaces with other security for proper and strong network security, which display the performance indicators of all the security devices in the organization’s network.

With its useful features and advantages, CNSFBS helps system security firewalls in banking to handle their task conveniently, and provides a better way of presenting the security issues to upper management. The advantages of CNSFBS are better convenience, reduced time for monitoring, centralized presentation of the logs, user-friendly interface, better way of troubleshooting, modular and scalable design, and centralized storage of the reports. These advantages are explained in detail in the following sections. After the implementation of the CNSFBS, network handle became significantly easier. Administrators who are on duty after work hours monitor the performance of the system in a more convenient way. The thresholds are determined through the system and based on those parameters, the on duty personnel are given specific instructions to act. These precautions prevent false alarms that had to be dealt with. CNSFBS also made network monitoring easier during the work hours. The upper management and administrators can see the real-time status of the network, the status of the services and the disk spaces when they check the web pages of the system.

Reference

Ogunwobi, Z. O., Folorunso, S. O. and Alebiosu, O. B. (2016): Evaluation of Computer and Network Security Strategies: A Case study of Nigerian Banks; CoRI’16, Sept 7–9, 2016, Ibadan, Nigeria.
[4] Wada F., Longe O. and Danquah (2012), actions speaks louder than words – understanding cybercriminals behaviour using criminological theories. *Journal of internet banking and commerce,* April, vol. 17, no 1
[5] Courtney H. (2014), Importance of network security for business organization, *avalan wireless blog,* May 7

Angelakopoulos, G. and Mihiotis, A., 2011. E-banking: challenges and opportunities in the Greek banking sector. Electronic Commerce Research, 11(3), pp.297-319.

Ogunwobi, Z.O., Folorunso, S.O. and Alebiosu, O., (2016). Evaluation of Computer and Network Security Strategies: A Case Study of Nigerian Banks. In OcRI (pp. 85-90).

Tytarenko, O., 2017. Selection of the best security controls for rapid development of enterprise-level cyber security. Naval Postgraduate School Monterey United States.

Dart, E., Rotman, L., Tierney, B., Hester, M. and Zurawski, J., 2014. The science dmz: A Network design pattern for data-intensive science. Scientific Programming, 22(2), pp.173-185.

Rababah, B., Zhou, S. and Bader, M., 2018. Evaluation the Performance of DMZ. Assoc. Mod. Educ. Comput. Sci, pp.0-13.

Arconati, N. (2002). One Approach to Enterprise Security Management. SANS Institute Security Reading Room, Retrieved April 13, 2007, from http://www.sans.org/ reading_room/

Hyland, P.C., & Sandhu, R. (1998). Management of Network Security Applications. In: Proceedings of the 21st NIST-NCSC National Information Systems Security Conference, Arlington, Virginia.

Bertagnolio, L. (2001) Security on the Network: What You Need to Know. SCMagazine, Feburary.

Abramson, C. (2001). A Return to Legacy Security. SANS Institute Security Reading Room, Retrieved April 03, 2007, from http://www.sans.org/reading_room/

Microsoft Inc. (2007). Ten Immutable Laws of Security Administration. Retrieved March 15, 2007, from http://www.microsoft.com/technet/archive/community/columns/security/ essays/10salaws.mspx?mfr=true.

Miles, T. (2004). Paradigm Shift. Applied Principles of Defense-in-Depth: A Parents Perspective. SANS Institute Security Reading Room, Retrieved April 13, 2007, from http://www.sans.org/reading_room/

Rasmussen, S. (2002). Centralized Network Security Management: Combining Defense in Depth with Manageable Security. SANS Institute Security Reading Room, Retrieved April 15, 2007, from http://www.sans.org/ reading_room/