-

Script Based Exploits On Financial Systems Vulnerabilities and Its Impact On Banking Information Systems

Longe, O.B (PhD) & Bolaji, A.A.
Department of Computer Science & Mathematics
Adeleke University
Ede, State of Osun, Nigeria
longeolumide@fulbrightmail.org, badefola@gmail.com

ABSTRACT

Using the Nigerian Banking Services sector as a premise, we investigated script-based attacks on financial systems. Attacks scenarios were presented and possible mitigating actions recommended.

Keywords: Script based exploits, financial systems, vulnerabilities, impact, banking, Nigeria.

1. INTRODUCTION

Given the rapid rate of change on the role of emerging information systems and real-time services embraced by electronic-driven business and financial organizations, minor or incremental improvements in security can be undermined by organizational entropy. This is true, owing to the global use and adoption of different operating systems such as Microsoft Windows client and server operating systems software technologies. A myriad of critical system vulnerabilities associated with these systems puts valuable information assets used by financial institutions at potential risk.

The problem is however compounded as the banking sector continuously embrace the integration of enterprise wide collaborative tools known as Enterprise 2.0 and convergent technologies that use vulnerable Internet transport protocols to carry classified enterprise data across endpoints has brought new threats to the traditional set of organizational security controls.

1.1 Financial System Vulnerabilities

Vulnerability is a gap, error, or weakness in how a system is designed, used, and protected. When vulnerability is exploited, it can result in giving unauthorized access, escalation of privileges, denial-of-service to the asset, or other outcomes (Joseph and Aamir, 2013). According to (Canadian Centre for Intelligence and Security Studies, 2013), vulnerabilities of the financial system consist of both formal and informal institutions. Financial system vulnerabilities lead to many dangerous events that can also lead to global crisis, for example, terrorists are able to engage in money-laundering to finance terrorism because of vulnerabilities in the financial system from one country to the other (CCISS, 2013).

Financial markets are usually characterized by information that is asymmetric in nature; this is a situation where one party to a transaction has more information than the other party. For instance, potential borrowers usually know more about the risks and returns of a project than the lenders. This problem leads to what can be referred to as moral hazard (where borrowers behave differently once they have acquired a loan) and adverse selection (where most borrowers are of the risky type), causing financial markets to fail to allocate resources efficiently. Asymmetric information increases the possibilities of people exploiting the financial systems; more precisely, lack of information may prevent banks from distinguishing legal from illegal proceeds, and they may unknowingly participate in money-laundering as a result (CCISS, 2013).

-

Walsh, (2003) states that, an effective security plan or program to prevent financial system vulnerabilities must be based on a clear understanding of the actual risks the system faces; this will form the basic precept of protection to the banking information systems

The value of a security program depends as much upon the relevance of resources as upon their high quality. It is necessary to understand the problem first; then the solutions could be considered. It is important to understand how to calculate risk associated with vulnerabilities found, so that a decision can be made on how to react (Shakeel and Tedi, 2011).

2. VULNERABILITY CHALLENGES IN FINANCIAL SYSTEMS

In order to define the security problem involves in a financial system, an accurate assessment of three factors has to be carried out, and these factors are:

- **(i)** The nature of threats or risks affecting the financial system
- **(ii)** The probability of those threats becoming actual loss events
- **(iii)** The effect on the financial system or on the enterprise responsible for the financial system if the loss occurs.

Each of them can be called loss event profile, loss event probability or frequency, and loss event criticality respectively (Walsh, 2003).

There are three main classes of vulnerability by which the distinction can be made for the types of flaws (local and remote). These classes are generally divided into design, implementation, and operational category (Joseph and Aamir, 2013).

Design vulnerabilities

These are discovered due to the weaknesses found in the software specifications.

Implementation vulnerabilities

The technical security glitches found in the code of a system.

Operational vulnerabilities

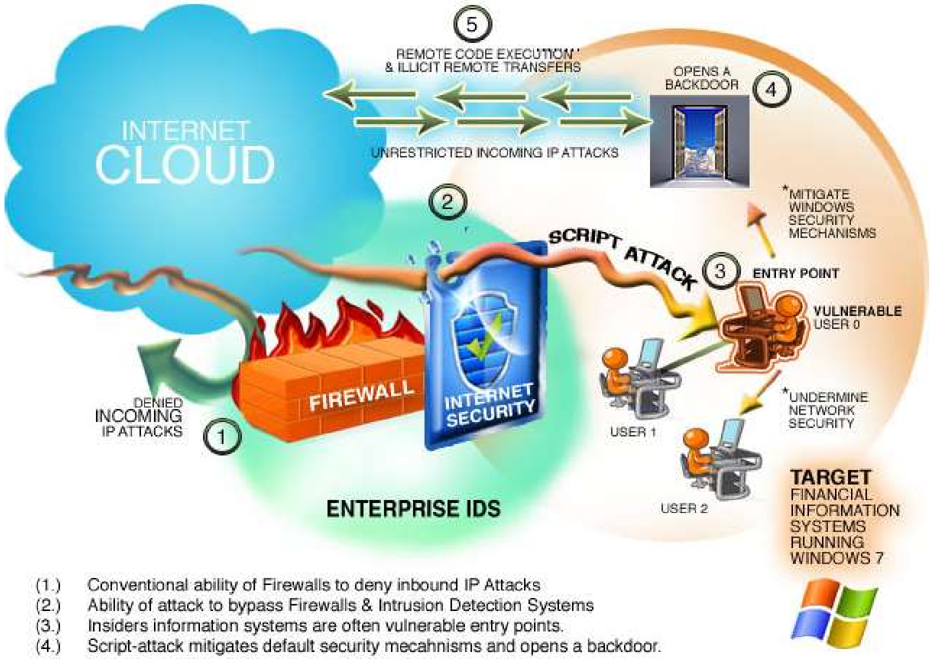
Those which may arise due to improper configuration and deployment of a system in a specific environment.

.

3. SCRIPT BASED VULNERABILITY SCENARIO

The use of the Internet grows together with the number of attacks which attempt to use it for nefarious purposes. One of the financial system vulnerability which has been commonly exploited is known as cross-site scripting (XSS). This class of vulnerabilities attack occurs when an attacker injects malicious code into a web application in an attempt to gain access to unauthorized information (Obi, 2007). In such instances, the victim is unaware that their information is being transferred from a site that he/she trusts to another site controlled by the attacker. A script based vulnerability that enables a potential attacker to demean windows proprietary security mechanisms and execute malicious arbitrary code on Microsoft Windows 7 Operating Systems and all versions, which are predominantly used for electronic commerce (E-commerce) and electronic business (E-business) initiatives involving both the Internet and institutions that rely on these services to effect routine business operations constitutes the focal point to be addressed in this work. An example of a script based scenario is as shown in figure 1

-


5
REMOTE CODE EXECUTION
& ILLICIT REMOTE TRANSFERS
OPENS A BACKDOOR
4
INTERNET
CLOUD
UNRESTRICTED INCOMING IP ATTACKS
2
*MITIGATE WINDOWS SECURITY MECHANISMS
SCRIPT ATTACK
3
ENTRY POINT
VULNERABLE USER 0
FIREWALL
INTERNET SECURITY
DENIED INCOMING IP ATTACKS
1
*UNDERMINE NETWORK SECURITY
USER 1
USER 2
ENTERPRISE IDS
TARGET
FINANCIAL INFORMATION SYSTEMS RUNNING WINDOWS 7

(1.) Conventional ability of Firewalls to deny inbound IP Attacks
(2.) Ability of attack to bypass Firewalls & Intrusion Detection Systems
(3.) Insiders information systems are often vulnerable entry points.
(4.) Script-attack mitigates default security mecahnisms and opens a backdoor.
(5.) Backdoors allows illicit remote activities on a target workstation.

Figure 1: A script-attack scenario

The targeted Banking financial system in the scenario is a Windows 7 operating system based. The script-based vulnerability attacks have their source in the cloud. A firewall blocks incoming attacks in a normal network setting, but script based attack can bypass the firewalls and the enterprise intrusion detection systems because of the method used by the code based attacks. The script attack goes from the first vulnerable user- user0 to other users1 and 2 which are not usually on guard as they were not expecting any form of attack from the user0. The success of the script attack will normally open the backdoor for the IP attacks that is normally blocked by the enterprise intrusion detection system and the firewall.

4. VULNERABILITIES FROM EXISTING PROTECTION MECHANISMS

The alarming thing about most subtle but powerful attacks on financial systems using scripts are based on the fact that malicious hackers relies on the significance of the ability of ‘arbitrary code to be executed without being detected by an **antivirus**, **firewall** or **anti-spyware** program installed on the workstation. The dependence on these mechanisms for protection is therefore rendered useless in script attack scenario. Most organizations are unaware of such forms of attacks and have lost huge sums of financial instruments occasioned by such vulnerabilities. According to NTT Communications (2012), broader vulnerability to attacks has been further heightened by the explosive growth in mobile phones, tablets, and other devices. These advances have taken the Internet off the desktop and allow practically unlimited online access to increasing numbers of users and more target opportunities for script-based attackers (NTT Communications, 2012). Some projections envision Internet-connected mobile devices hitting the 10-billion mark in coming years. This expanded connectivity opens the door further to script-based attacks, especially since many mobile device users tend not to regard these devices as portable computers. Such users are less likely to be aware of or concerned about possible script-based attacks (NTT Communications, 2012). Exploitability and payload construction advices the final step of writing proof-of-concept (PoC) code for a vulnerable element of an application (Lee, Tedi and Shakeel, 2014).

-

The proof of concept has established that total dependency on third-party antivirus programs, default windows security mechanism does not guarantee a healthy computing environment for e-commerce driven business organizations and financial institutions. Unfortunately in Nigeria, third party protective schemes are the order of the day. The possibilities for attacks are not only shocking and alarming but they can cripple the entire nascent information-driven financial infrastructure. Exploits on the vulnerability of the financial system has made a very strong impact in the banking information systems in Nigeria and the expression of this dissatisfaction is not unconnected with reports that the banking industry incurred huge losses of about N159 billion through cybercrime between 2000 and 2013. The inability of the National Assembly to pass the Nigeria Cybercrime Act into law is also identified as a major drawback in curtailing cybercrime in the banking information system of Nigeria (Okonji, 2014).

5. CONCLUSION

Since external threats are more easily perceived than internal threats, surveys and studies continue to show that the majority of security problems are internal. With all of this as context, the need for a new security paradigm is clear. Financial applications constitutes the lifeblood of many organizations and a growing piece of the world economy, a well-timed attack such as ‘customers credential theft’, or ‘denial-of-service’ permitted by this attack can cause a great deal of damage, by bringing down servers that control sensitive machinery or other functions, these attacks could also present a real physical threat to life and limb. An attacker could cause the service denial by flooding a system with bogus traffic, or even purposely causing the server to crash if an insider has knowingly or unknowingly demean the security mechanism of a financial information system.

In this paper, attempts have been made to establish the following:

1. Vulnerabilities are intrinsic to third party protective mechanisms such as antimalware, antivirus and firewalls
2. Several means of possible entry points are permissible on Microsoft operating systems and other operating systems currently employed by most financial institutions in Nigeria.
3. There are different attack scenario which includes the inability of internet security programs installed on a Microsoft Windows workstation, Network IDS, as well as default security mechanism such as Data Execution Prevention DEP and windows native firewall to detect when an ‘employee’ or malicious insider downloads a legit program obfuscated with a malformed script that can enable an attacker to remotely execute malicious code on the target workstation in a financial institution.
4. There are novel script invasion detection mechanism that can be used as a robust tool to address the problem of system manipulation and other malicious attacks on financial systems infrastructure.

REFERENCES

1. CCISS, 2013. Terrorism Financing and Financial System Vulnerabilities: Issues and Challenges. Canadian Centre for Intelligence and Security Studies, ITAC Trends in Terrorism Series, Carleton University.
2. Walsh James, 2003. Asset Protection and Security Management Handbook. POA Publishing LLC, Auerbach Publications, New York.
3. Obi Orjih, 2007. Type 2 Cross-site Scripting: An Attack Demonstration [Online]. Available from http://www.cse.wustl.edu/~jain/cse571-07/ftp/xsscript/ {Accessed: 22/09/14}.
4. NTT Communications, 2012. Successfully Combating DDoS Attacks. An NTT Communication White Paper, USA.
5. Shakeel Ali and Tedi Heriyanto, 2011. BackTrack 4: Assuring Security by Penetration Testing Packt Publishing Ltd, UK.
6. Joseph Muniz and Aamir Lakhani, 2013. Web Penetration Testing with Kali Linux. Packt Publishing Ltd, UK.
7. Lee Allen, Tedi Heriyanto, Shakeel Ali, 2014. Kali Linux – Assuring Security by Penetration Testing. Packt Publishing Ltd, UK.
8. Okonji Emma, 2014. Nigeria: Absence of Cybercrime Law Worries Information Security Society [Online]. Available from http://allafrica.com/stories/201407311214.html {Accessed: 22/09/14}.