Anatomy of Script Based Exploit On Financial Systems Vulnerabilities and Its Impact on Banking Information Systems in Nigeria – A Revisit

[1]Longe, O.B., [2]Ibitowa, F. & [3]Oluwatunde, S.J
[1]Department of Cyber Security, Caleb University, Imota, Lagos State, Nigeria
Department of Computer Science, The Polytechnic, Ibadan, Ibadan, Nigeria
Computer Science Programme. Caleb Business School, Lagos, Nigeria
E-mail: longeolumide@fulbrightmail.org, ibitowafolashade@yahoo.com; oluwatundesola@yahoo.com
Phone: +2348035902385

ABSTRACT

We revisited a previous effort on script-based exploits on financial systems vulnerabilities. The impact on banking information systems were x-rayed and possible attack scenario were presented. We propose a future research that will demonstrate the vulnerabilities intrinsic to third party protective mechanisms such as antimalware, antivurus and firewalls and the demonstration of our novel script invasion detection mechanism as a robust tool to address the problem of system manipulation and other malicious attacks on financial systems infrastructure.

Keywords: Scripts, Banking Information Systems, Vulnerabilities, Exploits, interoperability and Security

iSTEAMS Conference Proceedings Paper Citation Format
Longe, O.B., Ibitowa, F. & Oluwatunde, S.J (2018): Anatomy of Script Based Exploit On Financial Systems Vulnerabilities and Its Impact on Banking Information Systems in Nigeria – A Revisit. Proceedings of the 14th iSTEAMS International Multidisciplinary Conference, AlHikmah University, Ilorin, Nigeria, Vol. 14, Pp 145-148

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 (Microsoft Developer Network Library 2018). A myriad of critical system vulnerabilities associated with these systems puts valuable information assets used by financial institutions at potential risk (Adigun et al. 2014).

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 (Toby 2017).

2. SCRIPT BASED VULNERABILITY SCENARIO

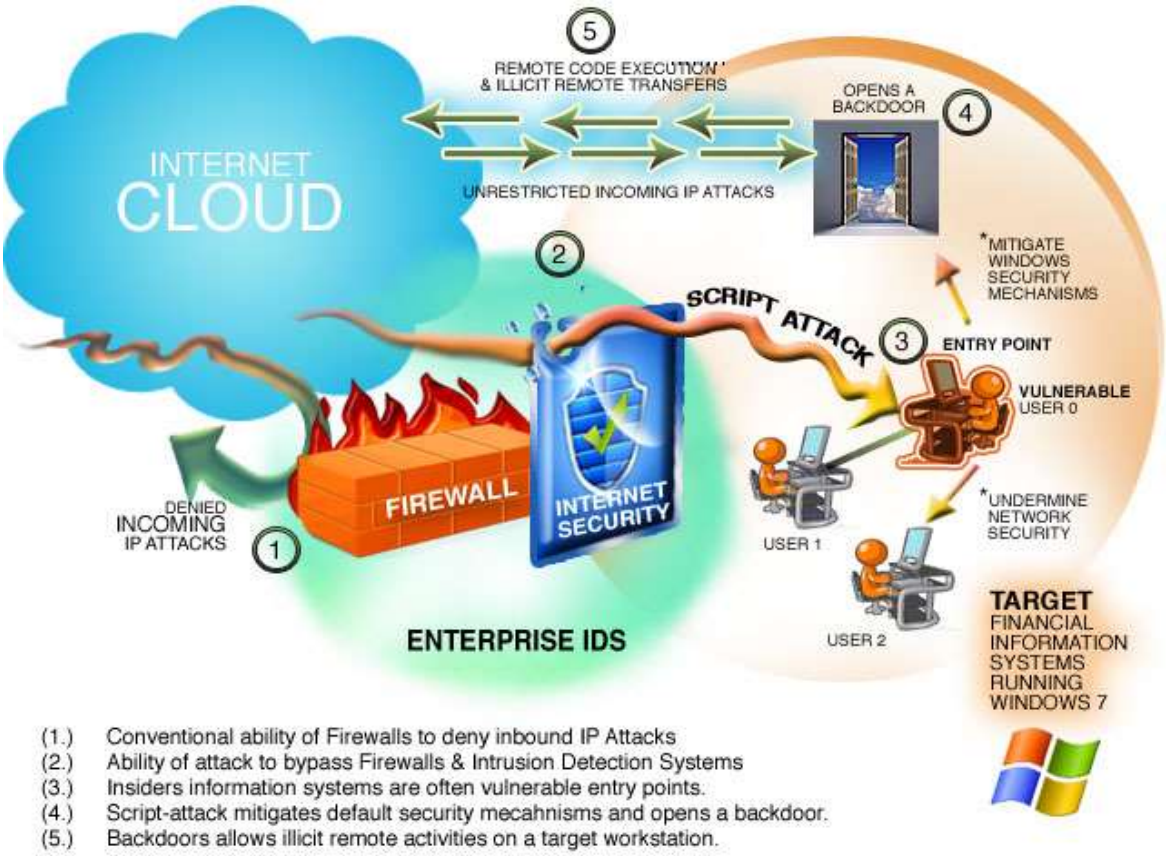
A script based vulnerability that enables a potential attacker to demean windows proprietary security mechanisms and execute malicious arbitrary code on Microsoft Windows 7 Operating Systems and all versions, which are predominantly used for electronic commerce (E-commerce) and electronic business (E-business) 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 workshop (Bo Han, et al 2012)

3. CAUSE FOR ALARM

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 are therefore rendered useless is script attack scenario. Most organizations are unaware of such forms of attacks and have lost huge sums of financial instruments occasioned by such vulnerabilities (Danny, 2018).

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 (Adigun et al., 2014).

4. SCRIPT-ATTACK SCENARIO



5. TRAINING MODE

Since external threats are more easily perceived than internal threats, surveys and studies continue to show that the majority of security problems are internal (Nena & Juliana, 2018),. With all of this as context, the need for a new security paradigm is clear (Uzal et al., 2013). 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 (Guneet, 2015). 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 (Elsevier, 2016).

6. FUTURE RESEARCH DIRECTION

Future work will do the following:

1. We will demonstrate the vulnerabilities intrinsic to third party protective mechanisms such as antimalware, antivurus and firewalls (Hossein & Lawrie, 2014).
2. We will show that there are several means of possible entry points permissible on Microsoft OS and other operating systems currently employed by most financial institutions in Nigeria (Microsoft Developer Network Library 2018).
3. We will demonstrate using different attack scenario, 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. [(Hossein & Lawrie, 2014, (ipswitch Community, 2018)].
4. We will demonstrate the use of our novel script invasion detection mechanism as a robust tool to address the problem of system manipulation and other malicious attacks on financial systems infrastructure (Pritika, 2015).

WORKS REFERENCED/CONSULTED

1. Adigun, A.A, Longe, O.B & Bolaji, A.A (2014), "Script Based Exploits On Financial Systems Vulnerabilities and Its Impact On Banking Information Systems", Department of Computer Science & Mathematics, Adeleke University, State of Osun, Nigeria. Computing, Information Systems, Development, Development Informatics & Allied Research Journal. Electronic version: https://static.secure.website/wscfus/8466857/2398607/v5n3p9-cisdiar-journal.pdf
2. Ayeni, B.K., Sahalu, J.B. & Adeyanju, K.R. (2018), "Detecting Cross-Site Scripting in Web Applications Using Fuzzy Inference System", Department of Computer Science, Faculty of Science, Almadu Bello University, Zaria, Nigeria. Journal of Computer Networks and Communications, Volume 2018. Electronic version: https://www.hindawi.com/journals/jcnc/2018/8159548
3. Bo, H., Quing, W., Fajiang, Y., & Xianda, Z. (2012), "A Vulnerability Attack Graph Generation Method Based On Scripts", International Conference on Information Computing and Applications, Pp. 45 – 50. https://link.springer.com/chapter/10.1007%2F978-3-642-34062-8_6
4. CCISS (2013), "Terrorism Financial and Financial System Vulnerabilities: Issues and Challenges, Canadian Centre for Intelligence and Security Studies, ITAC Trends in Terrorism Series, Carleton University.
5. Danny,P. (2018), "What is malware? Everything you need to know about viruses, trojans and malicious software", Electronic version: https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/
6. Elsevier (2016), " Featured in this issue: Distributed denial of service attacks – holding back the flood", Network Security Journal, March 2016.
7. Guneet, K.P. (2015), "Cyber Business Security Threats and Solutions", Maharaja Agrasen Institute of Technology, GGSIPU, CMAI Association of India
8. Hossein, S. & Lawrie, B. (2014), "Operating System Security", Computer Security Principles and Practical, Electrical Engineering and Computer Science.
9. IPSwitch Community (2018), "Understanding Data Execution Prevention in Windows". Electronic version: https://community.ipswitch.com/s/article/Understanding-Data-Execution-Prevention-in-Windows-1307565976900
10. Keenan, S, C. (2015), "Financial Institution Advantage and the Optimization of Information Processing", SAS Institute Inc., Carry, North Caroline, USA. Electronic version: https://support.sas.com/content/dam/SAS/support/en/books/financial-institution-advantage/68050_excerpt.pdf
11. Lee, A., Tedi, H. & Shakeel, A. (2014), "Kali Linux-Assuring Security by Penetration Testing, Packt Publishing Ltd., UK.
12. Microsoft Developer Network Library (2018), " Windows Client Operating System Protocols Documentation", Electronic version: https://msdn.microsoft.com/en-us/library/gg134033.aspx
13. Muniz, J. & Lakhani, A. (2013), "Web Penetration Testing with Kali Linux, Packt Publishing Ltd., UK.

14. Nena, G. & Juliana de, G. (2018), "Insider vs. Outsider Data Security Threats: What's the Greater Risk?", Digital Guardian. Electronic version: https://digitalguardian.com/blog/insider-outsider-data-security-threats
15. Okonji, E, (2014), "Nigeria: Absence 0f Cybercrime Law Worries Information Security Society". Electronic version: http://allfrica.com/stories/201407311214.html
16. Pritika, M. (2015), "Controlling Attacks and Intrusions on Internet Banking using Intrusion Detection System in Banks", Department of Computer Science, Khalsa College for Women, Amritsar. International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2015 https://pdfs.semanticscholar.org/67e5/e9ac0ff2e5025099c0d9caf96c4d17bcc55d.pdf
17. Reserved Bank of India (2017), "Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds", Department of Banking Supervision, Central Office, Mumbai. Electronic version: https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf
18. Ruowen, W., Peng, N., Tao, X., & Quan, C. (2013), "Meta Symploit: Day-One Defense Against Script-based Attack with Security-Enhanced Symbolic Analysis", Department of Computer Science, North Carolina State University, Raleigh, NC, USA. Electronic version: https://pdfs.semanticscholar.org/bc60/dfc6162c603dd622d83054643d9fda890505.pdf
19. Toby, F. (2017), "The Reserve Bank, Cyber Security and the Regulatory Framework", A speech delivered to the Future of Financial Service (10th Annual) Conference in Auckland. Electronic version: https://www.rbnz.govt.nz/research-and- publications/speeches/2017/speech-2017-07-19
20. World Economic Forum (2017), "Insight Report: The Global Risks Report 2017 12th Edition.
21. Uzal, R., Riesco, D., Montejano, G. & Debnath, N, (2013), "Trust in Cyberspace: New Information Security Paradigm", Department of Computer Science, Winona State University, USA.