Cyber Attack Mitigation: Detecting Malicious Activities in Network Traffic

Amanze B.C Ph.D
Department of Computer Science,
Imo State University, Owerri
amanzebethran@yahoo.com

Nlemadim Maureen Ihuoma
National Identity Management Commission Owerri,
Imo State.
maureennlemadim@yahoo.com

DOI: 10.56201/ijcsmt.v9.no3.2023.pg33.37

Abstract

The aim of this work is to detect malicious activities in network traffic. With the growth in data sharing through network, enterprise networks have become targets of attacks from Internet malware including node forgery or impersonation, worms, client-side infects (drive-by downloads) and phishing attacks. Malicious code and viruses can slip into the network and gain access to the computer systems connected to the network causing various sorts of issues. So this research work develops approaches to rapidly detect malicious network traffic including packets sent by port scanners and network worms. This was achieved by developing a system that will improve the cyber security for the e- platform. A system that monitors network user's activities and keeps track of events and user's activities history on the network was developed. The new system was built with robust security authentication using a hybrid technique (Digital Signature and Rivest-Shamir-Adleman (RSA) Algorithm) for securing the e- platform. The implementation of the hybrid technique on the e- platform was done using Php-MySQL and Java Script. Object-oriented analysis and design methodology was adopted in this work and it is a set of standards for system analysis and application design. The result from the new system was of immense benefit to network users as the system introduced a more secured communication channels for e-platforms thereby preventing loss of data. Also the cyber security system ensures that all critical data are encrypted and that only authorized users have access to data in its entirety.

Keywords: *Digital signature, Encryption, Decryption*

Introduction

With the proliferation of online retailers in Nigeria, technology adoption has gone a long way in powering company development and innovation in the country. Nigeria's use of technology is driving economic growth, but it is also subjecting the country to rapidly growing vulnerabilities. On-premises equipment is moving from an asset to liability as demand for remote working and public cloud services grow. However, shifting to the cloud has a cost: it increases the attack surface of every business. The many and well-publicized data storage service breaches have boosted cloud security awareness, but hackers fight hard to stay one step ahead of the game.

Due to the persistent and universal nature of the Internet's traffic sent to unused addresses, modern enterprise networks have become continuous targets of attacks from a large number of attacks from Internet malware including worms, self-propagating bots, spamming bots, clientside infects and phishing attacks. The widespread growth of networks has created remarkable possibilities and a big challenge for people and organizations. The uncontrolled growth of networks has also led to an increase number of intruders on the internet making everyone to be at risk of attacks. Therefore, a strong mechanism is a necessity to protect computer systems and organizations from intrusion.

According to a recent poll conducted by Sophos Group plc, a British security software and hardware company, 86 percent of Nigerian businesses was victims of cyber-attacks in the previous year. The second-highest proportion after India, and significantly higher than South Africa's 64 percent. This information was gathered from 65 Nigerian businesses that use public cloud-based services such as Azure, Oracle, AWS, Alibaba Cloud, and others to store data.

The significant flaw in Nigeria was a result of misconfiguration in the company's server as 64 percent of organizations were attacked through this method while the remaining 36 percent was through stolen credentials.

Maitanmi et al. (2013) defines cybercrime as a crime that is committed with the help of a computer through a communication channel or a transmission media called the cyberspace and global network called the Internet. Cybercrime has been increasing in complexity and financial costs since corporations, government and individual or society at large started utilizing computers in the course of doing business. Cybercrime includes hacking, fishing, credit card fraud, denial of service, software piracy, etc. (Maitanmi et al., 2013). So e-commerce security centers on the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. The essence of securing e-commerce platform is to ensures that business transactions are authenticated, access to resources are only available for registered or selected users, encryption of communication channels, and ensuring the privacy and effectiveness of transactions.

Humans are recognized to be the weakest link when it comes to cyber risk. One can all agree that the internet has been an essential aspect of our lives over the last decade as we have begun to live two lives: one physical and one online, where we reside as a digital entity. In this digital reality, one has several usernames, aliases, profile photos, and so on in various locations. In this virtual environment, we exchange information both purposefully and accidentally. When we ask ourselves how many websites we are registered on, we are unlikely to be able to provide an accurate figure. Being sociable has evolved from seeing people in person to using Dating Apps and being online on various social media platforms. In today's world, it appears that technology is growing at such a rapid rate that we must keep up with it especially those with a limited understanding of cyber risks and rules to follow when utilizing digital equipment. On the other hand, Cyber security professionals in most organizations should get abreast with the state-of-the-art technology when it comes to cyber-attacks as there has been a knowledge gap in this technology.

Taking everything into account, it is imminent that companies should imbibe in regular vulnerability management on their IT infrastructure considering the rate at which hackers take advantage of publicly available information relating to them and their customers as this helps in mitigating the rate at which those vulnerabilities fall to the wrong hand. So, in this research work an effective solution to the problem will be presented, which indicates possible ways of detecting malicious activities in network traffic and block those types of attacks in order to minimise their effects on network resources availability.

There are many e-commerce sites in Nigeria. Some of the top e-commerce sites are Jumia (https://www.jumia.com.ng), konga (https://www.konga.com), PayPorte (https://payporte.com), VConnect (https://www.vconnect.com), Kara (https://kara.com.ng), Jiji (https://jiji.ng), Printivo Store(https://printivo.com),Obiwezy(https://obiwezy.com),Ajebomarket (https://www.ajebomarket.com), Kusnap (https://kusnap.com), etc. Most of these e-commerce sites have provided platforms for Nigerians to shop online.

Jumia is one of the most popular e-commerce websites in Nigeria. The popularity of Jumia Nigeria has gone far beyond the shores of this continent and was rated by Amazon's Alexa as the most visited e-commerce website in Nigeria.

Konga, Nigeria's online Megastore was "borne out of the desire to deliver with speed and precision so that you would never have to worry about accessing your needs and wants at your convenience." It owns large warehouses stocked up with goods and strategically located in Key cities such as Lagos, the capital Abuja, and Port Harcourt to ensure swift and efficient delivery.

Konga also allows small businesses with varieties of products to sell and showcase on their website.

Cyber Crime and Cyber Security

The term cyber security is the collection of tools, security concepts, security safeguards, guidelines, policies, actions, training, best practices, risk management approaches, assurance and technologies that can be used to protect the cyber space and organization and user's assets (Ibikunle and Odunayo, 2013). Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber space. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment (Ibikunle and Odunayo, 2013). Cyber security is the body of rules put in place for the protection of the cyber space. But as we become more dependent on cyberspace, we undoubtedly face new risks. Cyber-crime refers to the series of organized crime attacking both cyber space and cyber security. Sophisticated cyber criminals and nation-states, among others, present risks to our economy and national security.

1. **Hacking:** Nigerian hackers are engaged in brainstorming sessions at trying to break security codes for e-commerce, e-payments and e-marketing product sites.
2. **Credit Card Fraud:** Credit card or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction or when withdrawing money using ATM card. The hackers can abuse this card by impersonating the credit card holder.
3. **Yahoo Attack:** It is characterized by using e-mail addresses obtained from the Internet access points using e-mail address harvesting applications (web spiders or e-mail extractor). These tools can automatically retrieve e-mail addresses from web pages. Nigerian fraud letters join the warning of impersonation scam with a variation of an advance fee technique in which an e-mail from Nigeria offers the recipient the chance to share a percentage of a huge amount of money that the author, a self-proclaimed government official, is trying to siphon out of the country (WBrenner, 2010)
4. **Software Piracy**: Piracy involves the unlawful reproduction and sharing of applications software, games, movies/videos and audios.

Cyber Security Assessment Tools and Methodologies

Cyber security assessment consists of methods and procedures used to assess the effectiveness of cyber security controls in a digital system. In particular, the assessment methods and procedures are used to determine if the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the asset owner. There are several different types of cyber security assessment (Cynthia et al. 2012).

1. Network scanning
2. Vulnerability scanning
3. Password cracking
4. Log review and analysis
5. File integrity checking
6. Malware detection
7. Penetration testing

References

Abrazhevich, D. (2014). Electronic payment systems: A user-centered perspective and interaction design. Eindhoven: TechnischeUniversiteit Eindhoven.

Alshanketi, F., Traore, I., &Awad, A. (2018). Multimodal mobile Keystroke dynamics biometrics combining fixed and variable passwords. WILE

Aishani, B. and Prabu, S. (2019) ATM PIN Authentication using Facial Recognition. School of Computer Science and Engineering Vellore Institute of Technology, Vellore, Tamil Nadu

Amurth, P. K. and Redddy, M. S. (2012). Implementation of ATM Security by Using Fingerprint Recognition and GSM. International Journal of Electronics Communication and

Computer Engineering, 3 (1), pp. 83-86.

Bours, H. B. (2019) Continuous authentication using biometric keystroke dynamics. In The Norwegian Information Security Conference (NISK) 2019

Burr, W. E., Dodson, D. F. Polk, and W. T. (2016) Electronic authentication guideline. In Recommendations of the National Institute of Standards and Technology, NIST SP 800-63, Version 1.0.2, April 2016

Boneh, D., Shoup, V. (2015) A Graduate Course in Applied Cryptography. Accessible at: https://crypto.stanford.edu/~dabo/cryptobook/draft_0_2.pdf.

Banyal, R.K.; Jain, P.; Jain, V.K. (2013) Multi-factor authentication framework for cloud computing. In Proceedings of the Fifth International Conference on Computational Intelligence, Modelling and Simulation (CIMSim), Seoul, Korea, 24–25 September 2013; pp. 105–11

Cynthia, K. V., Susan, W., and John, T. M. (2012) Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network Design at Nuclear Power Plants. Sandia National Laboratories P.O. Box 5800 Albuquerque, New Mexico 87185

Davaanaym, Y.S., Lee, H.J., Lee, S.G., , and Lim, H.T. (2019) A ping pong based one-time-passwords authentication system. In 2019 Fifth International Joint Conference (NCM ’09) on INC, IMS and IDC, pages 574–579. IEEE Computer Society, 2019