BOOK CHAPTER | Secured Communication

Cybercrime and Secured Data Communication

Sarumi, Jerry Abayomi (PhD)
Department of Computer Science
Lagos State Polytechnic
Ikorodu, Lagos, Nigeria.
Email: Jerrytechnologies@yahoo.co.uk
Phone: +2348023408122

Abstract

As the Internet came into widespread commercial use, the nature of computer crimes began to shift. These crimes, known as cybercrimes, generally; occur in the virtual community of the Internet or in cyberspace. Therefore, all innocent internet users should inculcate the habit of continuously updating their knowledge about the ever-changing nature of information technologies. This will enable them to be familiar with any form of internet fraud targeted at them. The same Information and Communication Technologies (ICT) that have contributed tremendously to the productivity of supply chain companies and governments alike, as well as to the global competitiveness of the European Union, expose modern societies to a range of cyber threats. In recent times, hackers have been engaging in different string concept on login fields and phishing in order to intrude cloud accounts and improving their brute-force technology on passwords. The consequences of cybercrime attacks are difficult to estimate, but it is evident that they may influence negatively both industries and our communities. This research proposed to carry out effective security guild on this loopholes and prospective challenges in cloud data storage.

Keywords: Encryption, Authentication Scheme, IT, Cybercrime, Supply chain security, cybersecurity

Introduction

Store data security issues has been a significant aspect that determined value of service provided by cloud service provider or weaknesses. Data should be put in safe place while maintain it integrity and completeness throughout retention period. There are both internal and external threats that affect the honesty of stored data in cloud storage. Lack of good security techniques for storing data into cloud server or inappropriate mechanism for execution of stored data in a large portion of cloud server can cause data integrity issue. The abuse rank and data breaches in cloud computing storage are among the greatest security challenges facing this technology specifically focusing on security challenges related to shared resources and on-demand nature of cloud computing.

Citation: Sarumi, J.A. (2022). Cybercrime and Secured Data Communication.
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

Research Purpose

The purpose of this paper is to develop possible threat scenarios to enhance the understanding about how terror or criminal organizations may take advantage of IT vulnerabilities of supply chains not only for financial revenue purposes, but also to put at stake the safety of our societies. Thereafter, it is discussed how practical support may be given by governments to private operators to mitigate such risks. Internet especially is an aspect of information technology that enables us to communicate with one another globally irrespective of the country and the continent within a twinkle of an eye. More and more, development strategies is based on the need for developing countries to embrace information technology both as a way to avoid further economic and social marginalization as well as to offer opportunities for both growth and diversification of their economies.

Apart from the destruction cyber-crime does to the economy, it also leads to the erosion of confidence in genuine Nigerian commercial credibility and today many western countries with France taking the lead have moved to deny Nigerian businessmen and women who are legitimate the rewards of e-commerce. France today requires web camera verification for most online business transactions from Nigeria (Longe and Chiemeke, 2018). The contribution of internet to the development of the nation; has been marred by the evolution of new waves of crime. The internet has become an environment where the most lucrative and safest crime thrives. Cybercrime has become a global threat from Europe to America, Africa to Asia and to the other parts of the world. Cybercrime has come as a surprise and a strange phenomenon that for now lives with us in Nigeria. With each passing day, we witness more and more alarming cases of cybercrimes in Nigeria, with each new case more shocking than the one before.

Various scholars have examined the term “perception. People perceive things in a way that accord to their beliefs, interests, motives, needs and learning. According to (Obono et al, 2018), cybercrime describes “those criminal acts either committed in cyberspace, such as various forms of identity theft and bank fraud, or acts that have a physical component and are simply facilitated by the use of internet-based tools”. Such acts commonly include distribution of fraudulent emails, and pornography on the internet. He further notes that cybercrimes are illegal activities perpetrated by one or more people using the cyberspace through the medium of networked computers, telephones and other information and communication technology equipment. There is hardly any crime committed in the world today that does not have cybercrimes undertone, because of high dependence on modern technology.

According to (Oketola et al, 2019) some young people use the web for information on current issues in health, education, politics, researches, sports, and for personal development as well as building skills. While others, misuse it for unconstructive activities. The growing danger from crimes committed against computers, or against information on Computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law, must be enforced and countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cybercrime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network.

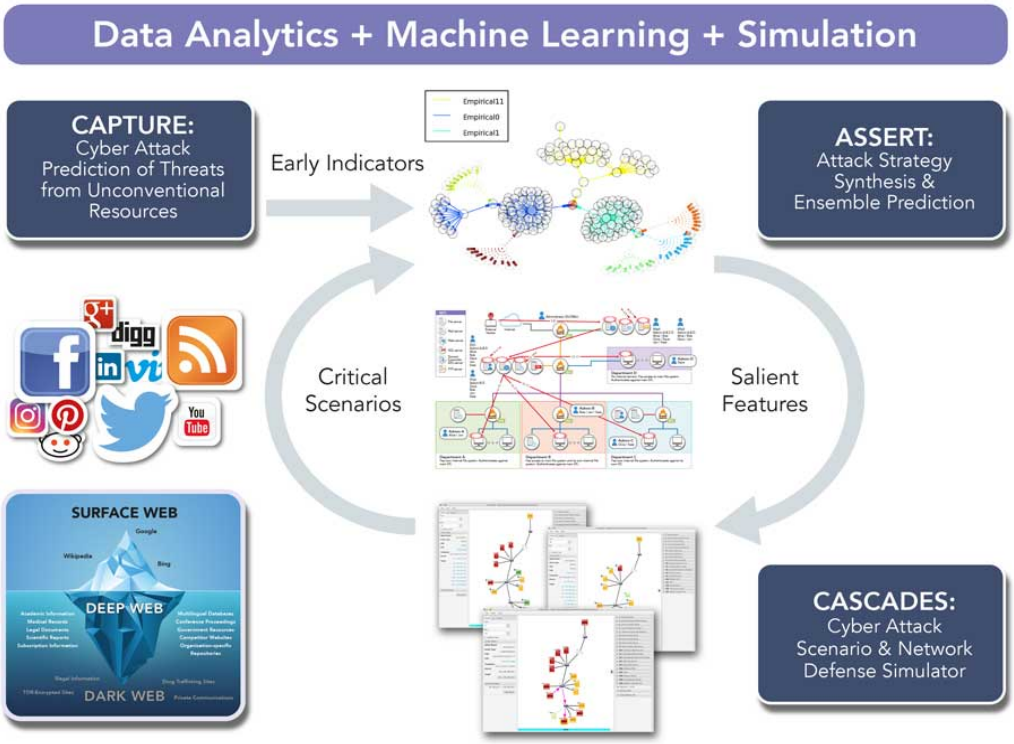

Fig. 1: Cyber Attack Threat Scenario
Source: https://researchfeatures.com/cybersecurity-threats-can-we-predict-them/

Research Observations

i. That the level of cybercrime in Nigeria is high.
ii. That the reasons for cybercrime in Nigeria include but not limited to poor cyber security; poverty, corruption in the system; high unemployment rate and lack of self-control.
iii. That the government can curb cybercrime in Nigeria by improving the economic condition of the masses; by reduction in the level of poverty; by reducing the level of corruption in the system; by creating more jobs for the youths; by value reorientation and by ensuring cyber security.
iv. That the there is a significant relationship between cybercrime and the economic development in Nigeria.
v. That there is a significant influence of cybercrime on Nigeria's foreign policy.

Consequently, during recent years, topics including cybercrime, cyber security, and cyber warfare have caught special attention and have been included in national security agendas of many countries around the world. In fact, every industry that Check Point tracked saw a significant increase in attacks last year.

Geographically, Africa was hardest hit by cyberattacks followed by APAC, Latin America, Europe and North America (in that order). Attack frequency increases year-over-year ranged from 13 percent on the low side in Africa to a whopping 68 percent increase in Europe.

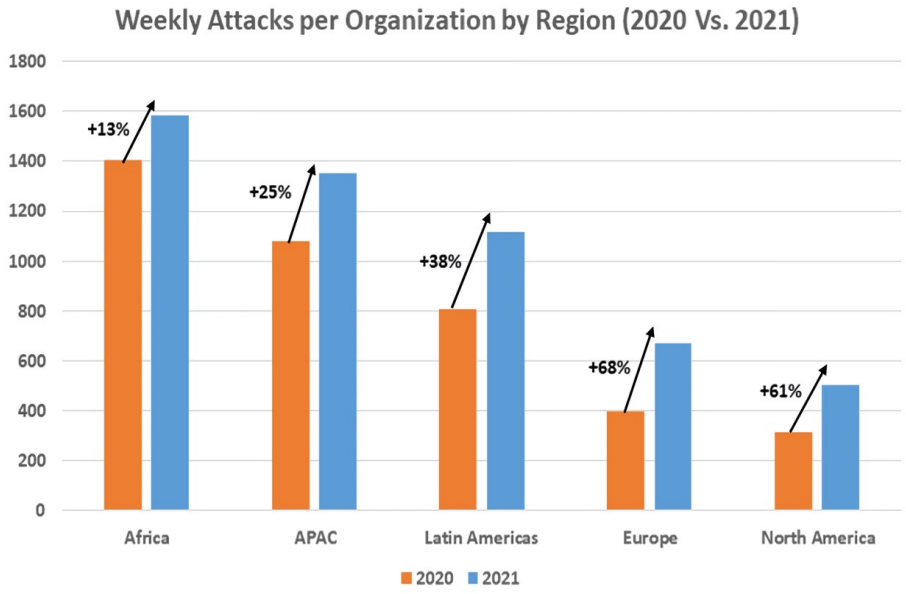

Fig. 1: Weekly Attacks Per organization By region (2020 vs 2021)
Source: https://www.cshub.com › attacks › news › 2021-records.

Check Point said all too often, organizations come under attack after failing to apply a patch for a known vulnerability. The security company recommends segmenting networks and putting strong firewall and ISP safeguards between them in order to keep infections from propagating across the entire network. It is also a good idea to educate employees to recognize telltale signs of potential threats and train them to report unusual findings to security teams immediately.

Due to lack of adequate security on data projection, data security and privacy has become a major issue in computing. Sending or sharing many, commercial and confidential data through the network are more vulnerable due to lack of proper encryption method. Achieving good security is always a talk of a good security method being in place. Sometimes it is not enough to maintain the secrecy of information, it is also necessary to keep the existence of the message secret. With the crucial growth of technology, data communications over the network are still vulnerable to attack because of the problem stated above. Therefore, there is need of better security method with better efficiency in order to increase the security.

Double Encryption is better to strengthen data security from unauthorized access when transmitted over the network. It is essential to ensure that only authorized access permitted and secured behavior is expected. Encryption in the computing employs a technique to secure data that will be stored. Hence, double layer encryption proposed to enhance security of data communication thus maintaining confidentiality of transmitted data.

The aim of this research is to propose a new era of key cryptography double layer encryption so that data; can be extremely secured, protected, and shared while in network environment. Double Layer Encryption methods, ensure security based on a popular cryptography algorithm RSA that is a relatively novel technique. The idea of double layer encryption will not only make full use of the great processing skill of computing but also can efficiently ensure data privacy and security.

While designing a two party cryptographic protocol one of two possible models is considered. These are

i. Semi honest model: when it is assumed that the protocol is cooperative and both parties follow the protocol properly in such a way that they help each other to compute fi (MA, MB), but curious parties may keep a record of all the information received during the execution and use it to make a later attack.
ii. Malicious model: where it assumed that parties might deviate from the protocol. In this case, during the interaction, each party acts non-cooperatively and has different choices which may determine the output of the protocol but the network supports various types of communications like one-to-many, many-to-one, one-to-one (peer) and many-to-many communications. The cases of many-to-many communications are essentially very important to study as all the cases are covered. Hence a detailed study of group communication done.

The many-to-many communication is like IP broadcast or multicast. Based on various applications the tailor made protocols, designed and presented in the literature. (Communication called group communication). As IP multicast comes to play a fundamental role in several emerging network applications such as online conferencing, distributed multiparty games, communication of stock quotes to brokers, etc. The security of group communications is a critical networking issue.

However, for this model of communication, the issues and problems of security are complex since group settings involve multiple participants who may join and/or leave dynamically. In order to secure group communications, security mechanisms such as authentication, access control, integrity verification and confidentiality are required. Group communication confidentiality requires that only group members could read multicast data even if the data broadcast to the entire network.

This key, generally called “group key” and the underlying management problem, called “group key management”. A group key management protocol must establish and distribute the group key while meeting the following requirements Group key secrecy: non-group members should not have access to any key that can decrypt any multicast data sent to the group. Key independence: a user who knows any proper subset of group keys cannot discover any other group key not included in the subset. Forward secrecy: members who left the group should not have access to any future key. This ensures that a member cannot decrypt data after he leaves the group.

References

1. Trustworthy Clouds, Privacy and Resilience for Internet-scale Critical Infrastructure (Tclouds), www.tclouds.eu (6 Dec. 2012).
2. National Threat Assessment 2008. Organised Crime (Zoetermeer, The Netherlands: KLPD–IPOL Department, Netherlands Police Agency, April 2009),www.csd.bg/fileadmin/user_upload/Countries/Netherlands/Dutch%20National%20%20threat%20assess ment%202008_tcm35-504488.pdf (17 April 2012).
3. Causes, Effects and the Way Out. *ARPN Journal of Science and Technology.*
4. Dr. Martins, J. Oni, (2013). *Cyber Crime in Nigeria: The Implication on our Economy and*.
5. Folashade B. Okeshola & Abimbola K. Adeta, (2013). The Nature, Causes and Consequences of Cybercrime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research Vol. 3 No. 9*
6. Jaishankar, K. (2010). The Future of Cyber Criminology: Challenges and
7. Opportunities. International Journal of Cyber Criminology 4, 26–31.
8. Kshetri, N. (2016). The Simple Economics of Cybercrime. IEE Security and Privacy.

9. Longe, O. B., & Chiemeke, S.C. (2008). Cybercrime and criminality in Nigeria - What roles are internet access points playing? European Journal of Social Sciences,6(4).
10. Melvin, A. O., Ayotunde, T. (2011). Spirituality in Cybercrime (Yahoo Yahoo) Activities among Youths in South West Nigeria. Youth Culture and Net Culture: Online Social Practices. https://www.irma-international.org/chapter/spirituality-cybercrime-yahoo-yahoo-activities/50709/