International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:9, 2014

Curbing Cybercrime by Application of Internet Users' Identification System (IUIS) in Nigeria

K. Alese Boniface, K. Adu Michael

***Abstract*—**Cybercrime is now becoming a big challenge in Nigeria apart from the traditional crime. Inability to identify perpetrators is one of the reasons for the growing menace. This paper proposes a design for monitoring internet users' activities in order to curbing cybercrime. It requires redefining the operations of Internet Service Providers (ISPs) which will now mandate users to be authenticated before accessing the internet. In implementing this work which can be adapted to a larger scale, a virtual router application is developed and configured to mimic a real router device. A sign-up portal is developed to allow users to register with the ISP. The portal asks for identification information which will include bio-data and government issued identification data like National Identity Card number, et cetera. A unique username and password are chosen by the user to enable access to the internet which will be used to reference him to an Internet Protocol Address (IP Address) of any system he uses on the internet and thereby associating him to any criminal act related to that IP address at that particular time. Questions such as "What happen when another user knows the password and uses it to commit crime?" and other pertinent issues are addressed.

***Keywords*—**Cybercrime, Sign-up Portal, Internet Service Provider (ISP), Internet Protocol Address (IP address).

I. Introduction

CYBERCRIME can be defined as a crime committed or facilitated via the Internet. It is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe [4]. Cybercrime incorporates anything from downloading illegal music files to stealing millions of dollars from online bank accounts. It also includes non-money offenses, such as creating viruses on other computers or posting confidential business information on the Internet. Knowing the facts, trends, and growth is critical to crime prevention efforts and protecting personal data in public and private sectors. This also helps in the creation of tools and strategies to combat cyber criminals. By virtue of the tools being used today to commit cybercrimes, criminals are now more anonymous and thereby difficult to identify. The history of cybercrime is short compared with traditional crimes. The first published report of cyber crime occurred in the 1960s, when computers were large mainframe systems. Since main frame were not connected with other ones and only few people could access them, the cybercrime were always "insider" cybercrimes. Actually, in the 1960s and 1970s, the cybercrime which was "Computer crime", was different from the cybercrime of today, because of no internet [1]. In following decades, the increasing of computer network and personal computers transformed "Computer crime" into real cybercrime. Since internet was invented, people began to exchange information based on networks of computers, also keep data in computer rather than paper. There are principally three main categories of cybercrime [2].

A. Target Cybercrime

This is a category of crime in which computer systems are the target of the offence. In this category, there are also classes of target cybercrimes, including hacking, malware and Distributed Denial of Service (DDos) attack. DDoS Attack as an example is an attack carried out by special software/some codes on some target computers on the internet. These software or codes are usually written by skilled programmers usually referred to as a hacker. DDoS attacks are achieved when continuous packets are being sent unto some target server until the bandwidth limit is achieved; this will therefore make that server in-accessible (as its allocated bandwidth has been exhausted). Actually, target cybercrime is the most professional crime on cyberspace. The defense of target cybercrime always has time lag, since we always take actions to patch an exploit after a novel method is revealed. In others words, the active defense is difficult.

B. Tool Cybercrime

In this category, a computer is used as a tool in committing the offense. It includes crime against property such as theft, fraud, extortion and against persons, including physical harm. The common form of this category is "*Social Engineering*" [5]. This is a process in which the cyber criminal communicate with prospective victims pretending to be who he is not in order to force the victims to disclose their valuable information which the criminal will then use to perpetrate his criminal acts. Using social engineering, a cyber criminal may pretend to work in his unsuspecting victim bank and that there is a problem with his (the victim's) bank account and therefore the victim should provide account information such as: Account Number, Credit/Debit card information Access Codes. If a victim should fall for this trick, then this cyber-criminal (Scammer) will use this information in other to claim whatever the victim has in his bank account. Another method

B. K. Alese is an Associate Professor with the Computer Science Department and Acting Dean, Students' Affairs, the Federal university of Technology, Akure, Nigeria (phone: +2348034540465; e-mail: bkalese@futa.edu.ng).

M. K. Adu is a Senior Lecturer with the Computer Science Department, the Federal Polytechnic, Ado Ekiti, Nigeria (phone: +2348066714060; e-mail: memokadu@yahoo.co.uk).

of social engineering could involve the scammer pretending to be a relative or friend of unsuspecting victims.

C. Computer Incidental

These are crimes where a computer system plays a minor role in committing the offense. In this category, the challenges for collecting the evidence are presented, which include evidentiary challenge and digital privacy. An example is "Phishing"; - This is achieved when the cyber criminal set up a clone of a website which people frequently visit to supply valuable information about themselves, for example: Paypal.com, an online payment system where, a hacker might set up a PayPal look-alike website and hence direct unsuspecting Paypal.com users to this fake website. If a user fails to identify that the site is not the real Paypal.com address and proceeds to supply his information, his username and passwords will be sent to a file on the hacker's server which then later will be used to access his victim's Paypal.com account at will.

In all, cybercrime is a new type of crime, compared with traditional crimes, but the harm caused by the former is not less than the latter.

II. Cyber Crime Prevention Strategies

Cyber criminals are not different from traditional criminals in a way because they both want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner when armed with a little technical advice and common sense. Many cybercrime attacks can be avoided. Similar to target hardening for a residence or a business (e.g., lights, locks, and alarms), the more difficult it is for a cyber criminal to successfully attack a target, the more likely he or she is to leave it alone and move on to an easier target.

Previous research works have identified the following as the basic ways that cybercrime can be prevented [4].

- Keep computer system up-to-date
- Secure configuration of the system
- Choose a strong password and protect it
- Keep firewall turned on
- Install or update antivirus software
- Protect personal information
- Read the fine print on website privacy policies

III. Cyber Crime Prevention by Unique User Authentication Method

The motivation for this research work in curbing cyber crime is borne out of the fact that any attempt at preventing cyber crime must identify the tool being used by the criminals, which is the internet. However, it seems no critical work has been done to review the identity of criminals rather preventive measures are being proposed by researchers. The criminals too are working hard if not harder to beat every preventive hurdle on their way. It is therefore reasonable that any enduring method of preventing this crime must reveal the identity of the perpetrators. The more anonymous they are, the more difficult to prevent [3]. Regardless of whichever way the crime is committed, the criminal has unique identity that can also be associated with the machine on which the crime is being performed. The goal of this research is to identify how to trace these identities and addresses to their owners. However, this may be an almost unachievable task as the internet itself does not reside on a particular machine and Internet users have access to various tools with which they can hide their identity on the internet. These tools includes; Proxies, tunnels, VPN (Virtual Private Network) and Virtual machine which an internet user may employ in order to hide any trace of his activities on the internet. Despite all these challenges, the best method/approach to curbing cyber crimes is to initiate control from the time and the source of internet service connectivity. This is proposed in this work. This source is usually the Internet Service Providers (ISPs) that provide internet services to their subscribers in different forms.

IV. Proposed Invention

This system requires that Internet Service Providers (ISPs) to register every internet subscriber at first attempt to surfing the internet. Once it is done by any ISP, registration is no longer necessary when trying to use the internet through another ISP. The information collected about any individual is hosted in a centralized database maintained by the National Communication Commission (NCC) in a cloud. Collecting information that truly validates an individual involves; Collecting subscribers Bio-data (e.g. Full name, Age, etc), Full address of residence, biometric Information (e.g. Fingerprint), National Identity Card Number and a Passport Photograph.

V. System Implementation

To implement this work, a ***small scale ISP*** is created using a laptop with wireless data card. A ***Virtual Router*** application is developed and configured to mimic a real life router device and to suit the project implementation needs. A signup portal is also created to allow internet users to register with the ISP and have easy sign in on subsequent connections, "this is preferable instead of asking the user to go through many processes before browsing which could be frustrating". The signup asks users for unique identification information which will include the users' bio data and government issued identification number like National Identity card, voters card et cetera. It can as well accept any form of biometric authentication such as finger print. After the signup, the a user will now have a unique username and password "chosen by him" that he can now use for authentication before having access to the internet which will be used to reference him with an IP address that his system is using thereby attaching him to any criminal report related to his record and the IP address at any point in time at the National Communication Commission (NCC) cloud which is the central database for all ISPs. The database will have an admin panel where detailed information about all users' activities can be sorted for and accessed on demand.

VI. Fundamental Issues

There are some fundamental issues that might agitate the minds concerning this proposed invention at curbing cyber crime in Nigeria. These issues are practically technical, and how to address them is discussed as follows;

What happen if a criminal minded individual get access to another person's password and username? In order to handle this, first and foremost users are expected to keep their username and password safe. Also, the system has an additional security level that sends a random generated pin - code to the mobile device, email, face book, twitter, in fact anything that can receive message that the user added while signing up. So after entering username and password, one will be asked to enter the security number received before he can be logged in fully for internet access.

What happen if a user phone is down and cannot surf the internet, cannot check mail, face book and so on? Again, this intelligent system makes provision for user to select where he wants the security pin code to be sent and afterwards gives him a link to a *'dynamic login page'* that is linked and allowed to the mail or social network gateway. Once a correct username and password of the gateway is entered, the internet access will be given and the user's information logged.

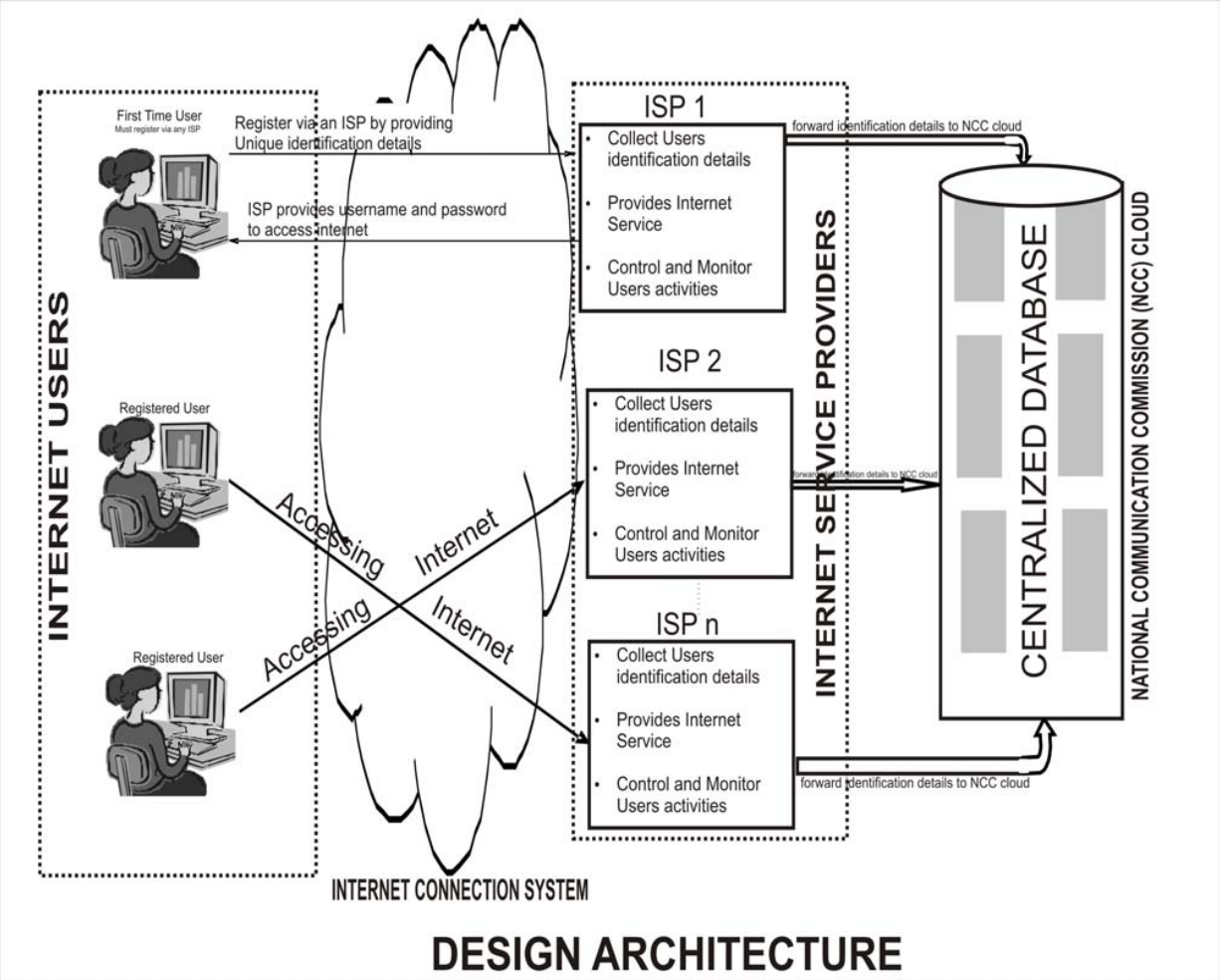

Fig. 1 Design Architecture of the System Implementation Process

VII. Conclusion

Cyber security has emerged as one of the hottest growing sectors over the last few years. As enterprises, government agencies, banks and companies continue to be plagued by cyber attacks, online security has become a major concern for all. Hackers have gained access to data of almost 1.6 million accounts from different websites globally. In response to the breach, Face book has already advised its users to activate login approvals and login notifications in their security settings. However, the recent breach has not only put current cyber security solutions under scanner, but has exposed their ineffectiveness in solving the problem. It is believed that strict vigilance from all sectors is the need of the hour. Efforts to improve coordination within the private sector are also important. Additionally, training and education on security matters are equally significant to developing a preventive

mechanism against cyber attacks. Amid the growing number of cyber attacks, corporations and companies are looking for stricter and more stringent cyber security measures to plug the loopholes in the system. Most significantly, spending on developing cyber security solutions is expected to continue to rise. In this Paper, a comprehensive invention to preventing cybercrime is proposed having carefully identified the main reason for inability to curb cyber crime as the anonymity of the criminals. That is, no proper means of tracking the perpetrators via any known record. This work is done with a view to attracting the attention of academics and researchers for advancement study of the principles and open up new challenges that will bring about effective and efficient method of cyber crime prevention.

REFERENCES

[1] Gulcu C, Tsudik, G, 'Mixing email with babel'. IEEE Conf. network and Distributed System Security, USA,1996, pp. 2-16.
[2] Jefferson, D.H, "Cybercrimes" National Crime Prevention Council http://www.ncpc.org/resources/files/pdf/internet-safety, 2012.
[3] Danezis G, 'Better anonymous communications' PhD thesis, University of Cambridge, 2004.
[4] Babu M, Parishath M.G, "What is Cybercrime" http://www.ncpc.org/resources/files/pdf/internet-safety , 2012.
[5] Wang Z, Stavrou A, "Exploiting Smart-Phone USB Connectivity for Fun and Profit," In the proceedings of the 26th Annual Computer Security Application Conference (ACSAC), December 2010, pp.357-366.