



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8

Issue: IV

Month of publication: April 2020

DOI:

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Developing an Identification and Monitoring System in Ensuring Responsible Use of the Internet in Nigeria

Adu Michael. K¹, Akinwamide Sunday O², Idris-Tajudeen, Rashida³

^{1, 2, 3, 4}Department of Computer Science, The Federal Polytechnic, Ado-Ekiti.

Abstract: This paper proposes better method for a safe and responsible use of the internet by designing a system that can uniquely identify users and thereby enabling effective monitoring. The work puts forward a system that performs the role of Internet Service Providers (ISPs) and in addition registers every internet subscriber at first attempt to surfing the internet. A central database is maintained to keep detailed information of subscribers which must include one that identifies uniquely. The online access monitoring system functions as a tool that authenticates every subscriber and logs their activities on the internet. Illegal and fraudulent activities on the internet can be traced to perpetrators. Small scale Internet Service Provider was achievable with laptops having wireless data cards. A virtual router application was developed and configured to mimic a real life router device to suit the implementation needs. The issue of anonymity of internet users is eliminated.

Keywords: Internet, users, Internet Service Providers, centralized database, access monitoring

I. INTRODUCTION

The internet has emerged in the last decade as an extremely important conduit for information and communication. It has assisted and remained the major tool for active and effective participation in societal activities [6]. The internet has resources that have over time become an essential components of our daily social, educational and entrepreneurial activities. The internet is a limitless reservoir for all sort of elements that are place or kept in it without restriction. This has over the years encouraged activities of unscrupulous men who took advantage of their anonymity to inflict different sort of social, economical and psychological hardship on the people [2]. The goal of this research is to identify and provide links to trace and bring to book fraudsters on the internet via their identities and addresses thus enabling safe and responsible use of the internet in Nigeria. The figure below depicts the activities of a typical internet/online social networks fraudster/attacker .

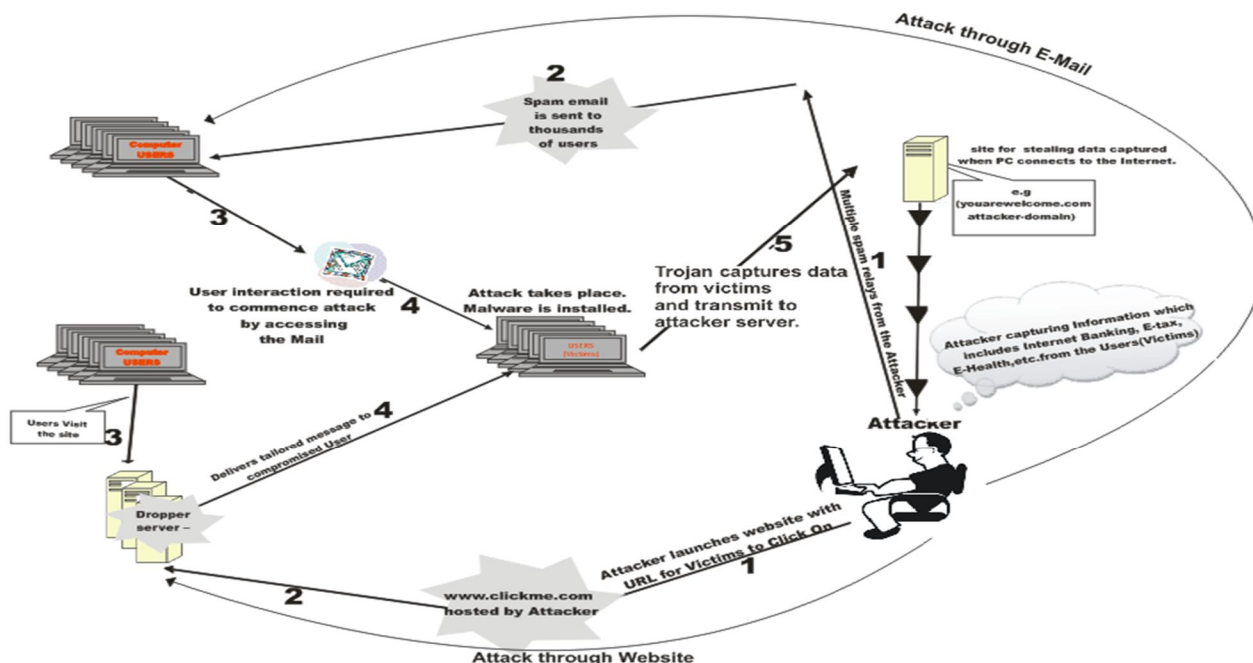


Figure 1. Activities of a typical internet/online social networks fraudster/attacker.

An attacker on the internet launches a website with Universal Resource Locator (URL) for victims to click on it. At this point, messages are dropped for the compromised users from a dropper server at the instance of the attacker [3]. Attack takes place in different forms, malware is installed on the users' systems, Trojan captures data from the victims and are transmitted to the attacker's server. The attacker consequently captures information details of the victims which include bank accounts details et cetera. Also, the attacker could send out multiple spam electronic mails to thousands of users [4]. Users interactions with the emails trigger attacks. Today, related crimes that are perpetrated with mobile phones in Nigeria are decimated and criminals are tracked by the law enforcement agencies as a result of centralized database for mobile phone subscribers. Many cases of fraudsters who call their victims pretending to be staff members of banks calling from customers' care desk, asking their victims to provide some of their account details to defraud them have been successfully investigated and culprits apprehended. The success recorded in this area is as a result of the existence of subscribers' database that make provision for information that can be traced to every individual. Also, no subscriber can access the mobile phone network without being registered. The success recorded in this regard could be extended to online social networks users on the internet using the same principle. Numerous security risks that exist on the internet/online social networks platforms include privacy violations, identity theft, and sexual harassment among others.

While most organizations and researchers have carried out work in the area of filtering software and using technology to address the challenges, others focus on social and educational strategies. However, application of commercial, proprietary-protected internet filtering software can unnecessarily and unconstitutionally restrict legitimate users from accessing appropriate material on the internet[5].

This work targets bringing out the identities of criminals for prosecution rather preventive measures being proposed by previous researchers. The authority should be able to bring to fore the activities of users with malicious activities in order to exercise any form of monitoring for safe and responsible use of the internet. It is therefore reasonable that any enduring method of preventing this crime must reveal the identity of the perpetrators. The need for a comprehensive technological approach to effectively monitor users activities without infringing into their fundamental right to information access and dissemination is the stake of this paper.

II. METHODOLOGY

Small scale ISPs are created using laptops with wireless data cards. 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 selected users to register with the ISP and have easy sign in on subsequent connections. 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 [1]. It can as well accept any form of biometric authentication such as finger print. After the signup, the user will now have a unique username and password chosen by him that he can now use for authentication before having access to the network 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. The database will have an admin panel where detailed information about all users' activities can be sorted for and accessed on demand.

A. Setting up the PC as an Internet Service Provider (ISP)

Almost every portable device can connect to the internet through a wireless network, using a personal computer as WiFi hotspot, this is very practical to implementing this research work. The work takes advantage of the multitude of Internet of Things (IoT) and established a connection of the personal computer to the internet. The Connectify Hotspot is used to create free WiFi hotspot. It is used to turn the Windows platform into a WiFi hotspot. The internet connection is shared with other devices such as smartphones, game consoles, et cetera. After the download and installation of the latest version of connectify Hotspot, it is given a name (SSID) and password. The 'Start Hotspot' button is pressed to share internet connection. This is the point at which any WiFi enabled device can connect to the Hot spot.

B. Store and Access logs of authenticated users

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. This software is cloned and remodified to suit the peculiarity of this project, which is to enable users information to be stored, and to access logs of authenticated users. Wireshark is a data-capturing program that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols.

III. RESULTS AND DISCUSSION

The results of Captured network data were browsed via a Graphical User Interface (GUI), or via the terminal (command line) version of the utility, TShark. Captured files were programmatically edited or converted via command-line switches to the "editcap" program. Data display were refined using a display filter and further formatted to a database (MYSQL).

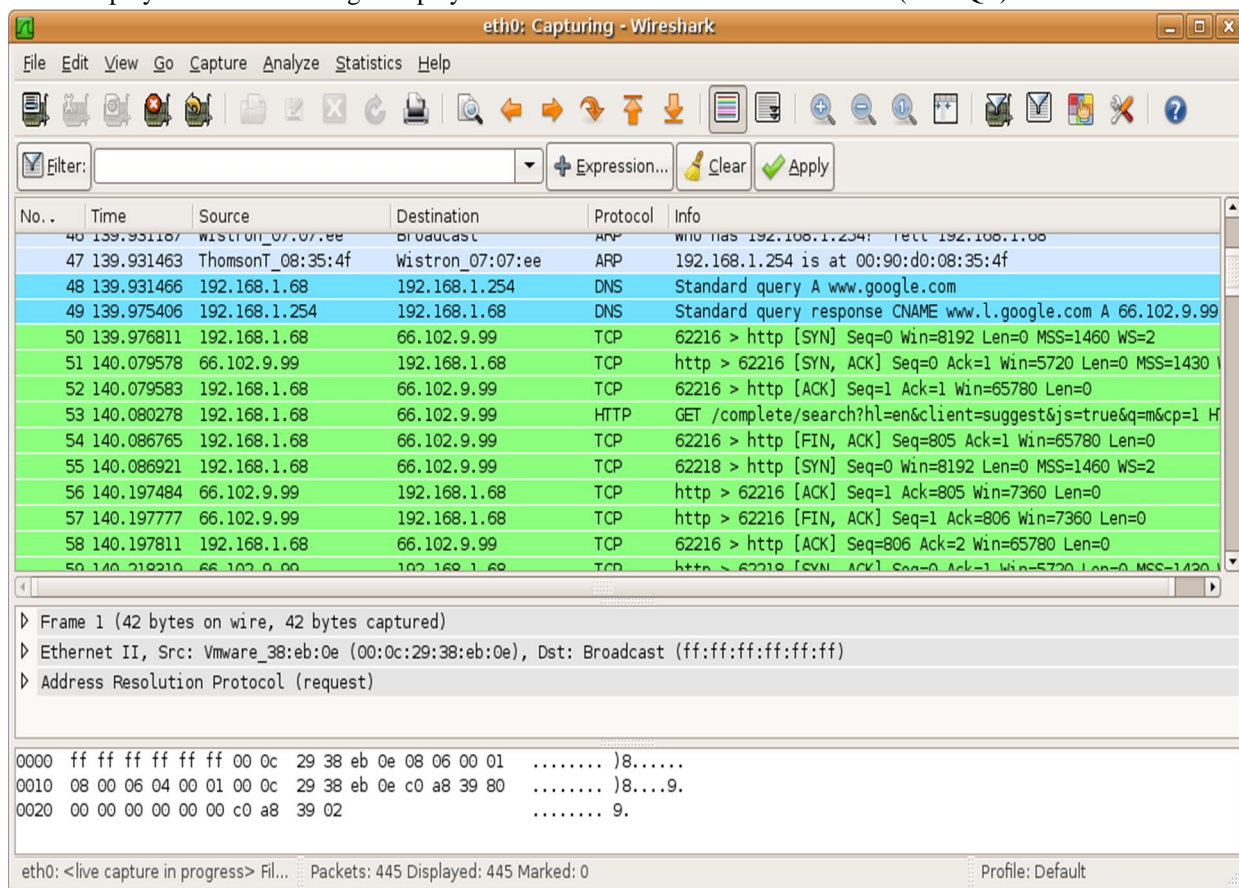
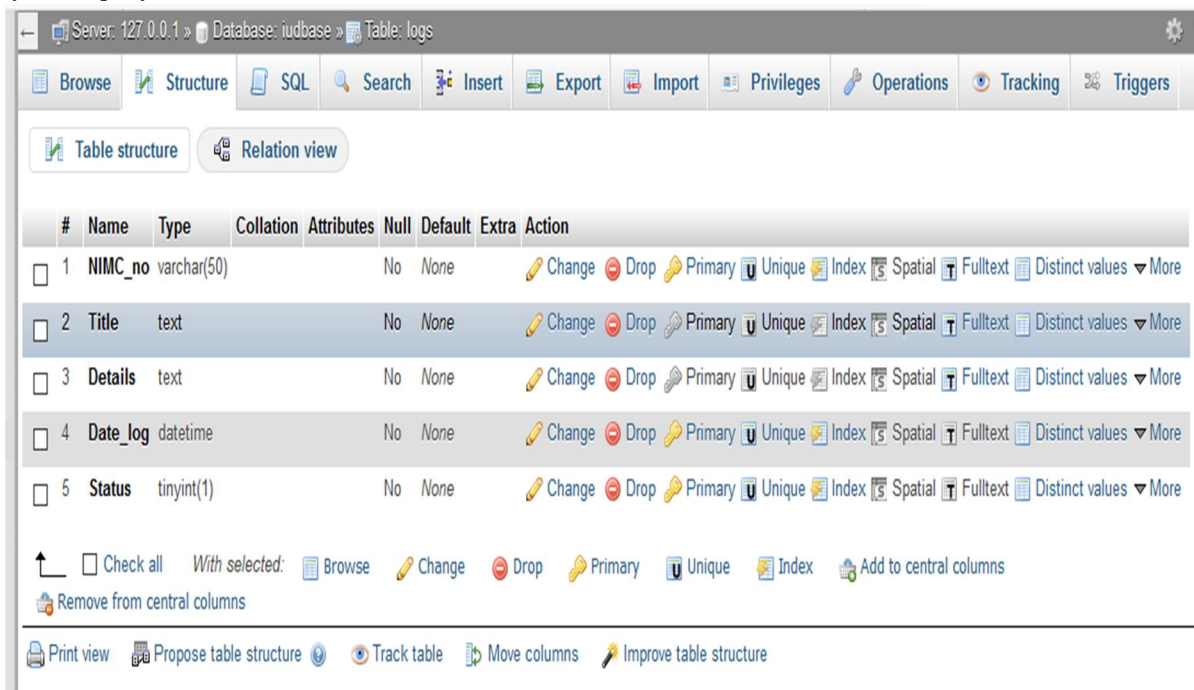


Figure 2. Display of Wireshark Software, a packet Analyser.

| # | Name | Type | Collation | Attributes | Null | Default | Extra | Action |
|---------|---------------------|-------------|-----------|------------|------|---------|-------|---------------------|
| 1 | NIMC_no | varchar(50) | | | No | None | | Change Drop Primary |
| 2 | Surname | varchar(50) | | | No | None | | Change Drop Primary |
| 3 | FirstName | varchar(50) | | | No | None | | Change Drop Primary |
| 4 | Middlename | varchar(50) | | | No | None | | Change Drop Primary |
| 5 | Date_of_birth | date | | | No | None | | Change Drop Primary |
| 6 | Gender | varchar(10) | | | No | None | | Change Drop Primary |
| 7 | Nationality | varchar(50) | | | No | None | | Change Drop Primary |
| 8 | State_of_origin | varchar(40) | | | No | None | | Change Drop Primary |
| 9 | LGA | varchar(40) | | | No | None | | Change Drop Primary |
| 10 | Home_town | varchar(50) | | | No | None | | Change Drop Primary |
| 11 | Mobile_no | int(11) | | | No | None | | Change Drop Primary |
| 12 | Desktop_mac_address | varchar(50) | | | No | None | | Change Drop Primary |
| 13 | Mobile_mac_address | varchar(50) | | | No | None | | Change Drop Primary |
| 14 | Finger | blob | | | No | None | | Change Drop Primary |
| 15 | passport | blob | | | No | None | | Change Drop Primary |
| 16 | location_tracker | varchar(50) | | | No | None | | Change Drop Primary |
| Console | date_created | date | | | No | None | | Change Drop Primary |

Table 1. Users registration table

The above table show the user registration form field with their respective data type allocated to each field. NIMC_no was used as a primary key to uniquely identified users record.



| # | Name | Type | Collation | Attributes | Null | Default | Extra | Action |
|---|----------|-------------|-----------|------------|------|---------|-------|--|
| 1 | NIMC_no | varchar(50) | | | No | None | | Change Drop Primary Unique Index Spatial Fulltext Distinct values More |
| 2 | Title | text | | | No | None | | Change Drop Primary Unique Index Spatial Fulltext Distinct values More |
| 3 | Details | text | | | No | None | | Change Drop Primary Unique Index Spatial Fulltext Distinct values More |
| 4 | Date_log | datetime | | | No | None | | Change Drop Primary Unique Index Spatial Fulltext Distinct values More |
| 5 | Status | tinyint(1) | | | No | None | | Change Drop Primary Unique Index Spatial Fulltext Distinct values More |

Table 2. Users logs table

The above table shows the users' log with respect to their activities. This table registered every activity perform by respective user using their NIMC_no as primary key.

Sort by key:

Options

| | NIMC_no | Surname | FirstName | Middlename | Date_of_birth | Gender | Nationality | State_of_origin | LGA | Home_town | Mobile_no | Desktop_mac_address |
|---|--------------|-----------|-----------|------------|---------------|--------|-------------|-----------------|-----------|-----------------|-----------|---------------------|
| <input type="checkbox"/> Edit Copy Delete | 10234989009 | Ogunsakin | Tayo | O. | 1983-10-12 | Male | Nigeria | Ekiti | Oye | Oye | 803459 | 01:209:03:z3:xx:12 |
| <input type="checkbox"/> Edit Copy Delete | 12087822009 | Victor | Moses | Olanipekun | 1997-03-09 | Male | Nigeria | Osun | Ede | Ede | 8901 | 209:aj:12:z3:2b:2b |
| <input type="checkbox"/> Edit Copy Delete | 12309867830 | Adewale | Tosin | O | 1980-10-24 | Male | Nigeria | Kwara | Ilorin | Ilorin | 903930 | 01:209:03:z3:2b:12 |
| <input type="checkbox"/> Edit Copy Delete | 128967823991 | Amos | Thomas | Kehinde | 1992-02-02 | Male | Nigeria | Edo | Akoko Edo | Ed Edo | 829032 | 01:209:03:2b:23 |
| <input type="checkbox"/> Edit Copy Delete | 23098909123 | Micheal | Kehinde | Amos | 1983-12-12 | Male | Nigeria | Ekiti | Ikere | ikere | 80901289 | 01:209:03:12:RK |
| <input type="checkbox"/> Edit Copy Delete | 23561109871 | Babatunde | Moses | K. | 1983-10-24 | Male | Nigeria | Ondo | Akure | Itaogbolu South | 803937 | 01:209:03:as:3b:14 |
| <input type="checkbox"/> Edit Copy Delete | 23908934112 | Amaka | Janet | | 1986-10-24 | Female | Nigeria | Osun | Ife | Ife South | 9038839 | 01:209:03:z3:00:13 |

Console

Table 3. Registration Table of users of the internet data

| Browse | Structure | SQL | Search | Insert | Export | Import | Privileges | |
|--|--------------|-----------------------|---|---------------------|--------|--------|------------|--|
| Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are not available. | | | | | | | | |
| Showing rows 0 - 2 (3 total, Query took 0.0006 seconds.) | | | | | | | | |
| SELECT * FROM `logs` | | | | | | | | |
| [Edit inline] | | | | | | | | |
| <input type="checkbox"/> Show all Number of rows: 25 Filter rows: Search this table | | | | | | | | |
| Options | IIMC_no | Title | Details | Date_log | Status | | | |
| | 0234989009 | Chatting on Whatsapp | Joseph: Hello, friend Amos: hi Joseph: ... | 2019-06-02 03:09:18 | 20 | | | |
| | 289678239912 | Google Search Engine | Pls how can i format my nokia E45 phone using manu... | 2019-01-15 03:08:11 | 20 | | | |
| | 3098909123 | Tempo digital culture | Usng tempo digital culture website Studying usi... | 2018-06-11 03:08:07 | 20 | | | |

Table 4. Log Table of Users' Activities

The table shows some users activity details. These can be retrieved for questioning if the need arises. The collected details of conversation can be accessed and where fraudulent activity is suspected, further action would be taken to unravel the acts and perpetrator would be brought to book.

The concern of this research is on tracking and monitoring internet users activities, thereby creating avenue to curb cybercrime and other fraudulent acts perpetrated via internet in Nigeria. The available data used for this research were collected from users who surf the internet using devices such as mobile phones, desktop computers and laptops. The mobile phone of any user could be tracked using location tracker (GPS) and Mac address for monitoring. Users identification could be established using the collected unique identification identities of the users such as Fingerprint, NIMC (National Identity Management Commission) number, issued by the Federal Government to identify every individual. These details are maintained in the database. The NIMC number is a primary key to hold each user's record uniquely.

IV. CONCLUSIONS

In the midst of growing number of cybercrime attacks, corporations and companies are looking for stricter and more stringent cyber security measures. With this work, 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 enables a system 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. Therefore the issue of anonymity of internet users is eradicated.

V. ACKNOWLEDGMENT

The authors wish to thank TetFund Nigeria for sponsoring this research work. The Directorate, Centre for Research, Innovation and Development of the Federal Polytechnic, Ado-Ekiti is highly appreciated for their cooperation and understanding. Many thanks to Mr. Chuma Nwema, Mr. Kingsley Uzundu and Ajewole Tope for their technical assistance.

REFERENCES

- [1] Adu M. K, Alese B.K. and Adewale O. S, "Mitigating Cybercrime and Online Social Networks Threats in Nigeria" in Proceedings of the World Congress on Engineering and Computer Science, Vol I, San Francisco, USA, ISBN: 978-988-19252-0-6, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) WCECS 2014.
- [2] Babu M., and Parishatb M.G. "What is Cybercrime" <http://www.ncpc.org/resources/files/pdf/internet-safety> , 2012.
- [3] Benevenuto, F. Rodrigues T., Almeida V., and Goncalves M. "Detection Spammers and Content Promoters in Online Video Social Networks", In proceedings of the 32nd International ACM SIGIR Conference on Research and Development in Information Retrieval, pages 620-627. ACM , 2009.
- [4] ContentWatch, "Social Networking Challenges Every Parent Should know" <http://www.netnanny.com>, 2013.
- [5] Acquisti A. and Gross R., "Imagined Communities Awareness, Information Sharing and Privacy on the Facebook" in 6th Workshop on Privacy Enhancing Technologies, 2006.
- [6] Brenner J. and Aaron S.. "Online Adults are Social Networking Site Users", <http://pewinternet.org/Reports/2013/social-networking-sites/Findings.aspx>, 2013



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)