A Holistic Mobile Security Framework for Nigeria

Fidelis C. Obodoeze, Francis A. Okoye, Calister N. Mba, Samuel C. Asogwa, Frank E. Ozioko

Abstract— Since the inception of mobile telecommunication in Nigeria in 2002 as Global System for mobile Telecommunication(GSM) and Code Division for Multiple Access(CDMA), there has been a meteoric rise in the number of subscribers as well as the security challenges affecting the mobile telecommunication platforms. Security challenges such as hackers' attacks to personal data and corporate networks leading to loss of privacy and funds, the threats of malicious programs such as virus, worms, Trojans, bombs, etc as a result of massive interconnectivity to the internet by the majority of the subscribers using mobile phones as well as synchronization of mobile equipment to Personal Computers(PCs) and corporate networks , and the rampant theft of mobile equipment have been identified to constitute the greatest security challenges. This paper examines these challenges and carefully deduced from them the current existing attack models or patterns in the Nigeria telecommunication industry in order to formulate counter solutions to them. This paper finally proposed a five-model corrective and preventive security framework that can tackle and mitigate these identified security challenges if implemented.

Index Terms— holistic mobile security, Nigeria, malicious program, CDMA, GSM, smart phone, SIM, IMEI, intranet, security-triad, attack models

I. INTRODUCTION

Nigeria with a teledensity of 0.73% in 2001 suddenly rose to 75.17% in August 2012 as a result of the emergence of Global System for Mobile Telecommunications (GSM) and Code Division for Multiple Access (CDMA) telecommunication platforms in 2002 brought about by the then Obasanjo administration in 2002 [1]. Since then there have not been any laid-down uniform mobile security framework to protect over 105 million active subscribers from all forms of security threats affecting the effective, smooth and safe mobile transactions and services. Ordinary users and corporate subscribers are threatened on daily basis by several security challenges such as privacy invasion, mobile phone theft, SIM card cloning, mobile epayment security threats, attacks from malicious programs such as virus, Trojans, spywares, worms and the worst of all being attacks from hackers who device all forms of social engineering tactics to beat unsuspecting subscribers in order to defraud them using their mobile application platforms. Since the inception and proliferation of mobile telecommunication in Nigeria, criminals such as hired assassins, armed robbers, kidnappers collect their victims' Subscriber Identification Module (SIM) card numbers (mobile or cell phone numbers) and use them to track their victims to kidnap, assassinate or rob them at gun points. This is very rampant in Nigeria since the rise of political assassinations, armed robbery and kidnapping for ransom. Fig. 1 shows the replica or prototype of SIM card used by most Nigerian mobile users in GSM and CDMA telecommunication platforms powered by telecommunication firms such as MTN, Airtel, Globacom, Etisalat, Starcomm etc.

Fig. 1. Subscriber Identification Module (SIM) smart card prototype used by most Nigeria mobile users

All the GSM and CDMA telecommunication firms in Nigeria have implemented the Nigeria Communication Commission (NCC)'s directive for all telecommunication firms to have their mobile subscribers' SIM cards registered and the biometric and personal data of the subscribers stored in a database. This is a good step in the right direction to abate incidences of robbers or kidnappers who use SIM card phone numbers to contact the victims' relatives for ransom. These stored data can be used later to apprehend and arrest the criminals.

The rise in the usage of smart phones and mobile devices such as Blackberry, Nokia, IPad, Iphones, etc. has exacerbated the mobile security challenge in Nigeria by rapidly contributing to the spread of epidemics such as worms, viruses, Trojans, logic bombs, etc over the internet and private corporate networks such as intranets [2]. In Nigeria, out of over 102 million current mobile subscribers, it was reported by [3] that 82 million subscribers access the internet or data services via their mobile devices as modem via their PCs; this contributes to the easy and fast spread of security epidemics. Also, it was identified that quite a large population of the subscribers use their mobile devices to access multimedia applications such as MMS, video, audio and conduct all kinds of ecommerce transactions and payment, especially now that epayment cashless policy is in place in Nigeria [4] ,[5]. All these applications throw up quite a considerable amount of security exposures and vulnerabilities to the users.

Another factor contributing

Revised Manuscript Received on February 06, 2013.

F.C. Obodoeze, Dept. of Computer Science, Renaissance University, Enugu, Nigeria.

Dr. F.A. Okoye , Dept. of Computer Engr., Enugu State University of Science & Technology (ESUT), Enugu, Nigeria,.

S.C. Asogwa, Dept. of Computer Science, Michael Okpara University of Agriculture, Umudike, Nigeria, (e-mail: sasogwa@gmail.com).

C.N. Mba, Dept. of Computer Engr., Caritas University, Enugu, Nigeria.

F.E. Ozioko, Dept. of Computer and Information Science, Enugu State University of Science & Technology (ESUT), Enugu, Nigeria.

to the spread of mobile security challenge in Nigeria is users' education; the majority of the users do not have basic security know-how to combat some of these menaces, therefore any security framework designed for Nigeria telecommunication industry must take this into consideration to ensure the successful implementation of the framework.

This paper will examine these security challenges affecting the safe and smooth usage of mobile devices and mobile applications and services in Nigeria. This paper will equally examine the current mobile security attack models to assist in designing effective countermeasure framework. Finally, this paper will propose and develop an enhanced and holistic security framework that will protect users' data, fund and privacy from hackers, prevent and protect mobile equipments from theft, protect corporate networks and data from all forms of espionage and attacks.

II. COMPUTER AND CYBER SECURITY DOMAINS

To tackle mobile security challenges in Nigeria, the computer and cyber security domains should be considered. Author in [6] classified the computer and cyber security domains into the following three categories:

- *Safety*
- *Attacks*
- *Privacy*

Safety deals with both the physical well-being and physical security of mobile platforms users (subscribers) and mobile equipment. Attacks deal on all types of security vulnerabilities and breaches that affect the smooth operation of mobile platforms and services. Privacy deals with the concerns on preservation and protection of confidentiality and integrity of mobile data and information from unauthorized users or hackers. This three security-triad in mobile telecommunication helps to provide a holistic security for both the mobile users and equipment. Fig.2 shows the three-triad security domains in computer and cyber security.

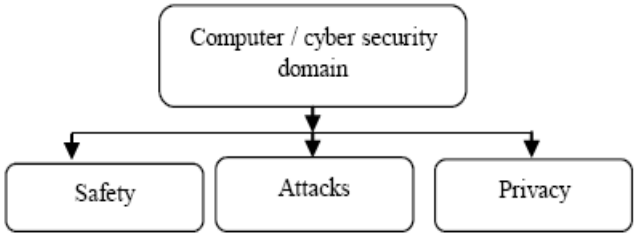

Fig. 2. Computer and Cyber-security domain [6]

III. CURRENT GSM SECURITY ARCHITECTURE

The current GSM security architecture upon which the current Nigerian telecommunication networks were built lacks the necessary features to curtail most of the mobile security insurgencies in Nigeria. At the time the GSM security framework was built, the level of sophistication of mobile security challenges now were not envisaged. Moreover, most of the GSM security algorithms have been proved to be defective in securing the recent GSM applications. Therefore, new mobile security framework is needed to tackle holistically the myriads of security challenges affecting the telecommunication industry.

IV. SECURITY CHALLENGES AFFECTING MOBILE PLATFORMS AND USERS IN NIGERIA

We have identified and classified the major mobile security challenges affecting mobile users in Nigeria as physical, data and operational security challenges. Physical security challenges affect the safety and well-being of the mobile equipment (mobile phone and SIM card) as well as other telecommunication equipment. These involve protection of mobile equipment physically from being stolen, vandalized by criminals or hackers. Data security for the mobile platforms make sure that sensitive and critical data and information contained or transmitted by the mobile equipment and platforms are not intercepted in transit by hackers either to eavesdrop on the data or modify them or use the data to defraud or molest the victims. Operational security challenge involves the security challenge or attacks affecting the operational capacity of the mobile platforms or services that depend on the mobile platforms.

The following security challenges were identified to be the major issues affecting the smooth and safe running of mobile platforms in Nigeria:

- Passive eavesdropping on voice or data (SMS, MMS) on mobile platforms.
- Privacy invasion or attack by hackers or thieves who stole mobile phones from their victims.
- Loss of confidentiality and integrity of enterprise data as a result of attack on their corporate network by hackers via mobile telecommunication platforms.
- Loss of privacy of banking data (pin number and passwords) by consumers who use mobile devices to conduct banking/financial transactions.
- Attacks by hackers who use misleading social engineering schemes and mobile telecommunication platforms to defraud their unsuspecting victims of their hard-earned funds.
- Attacks from malicious program such as virus, worms, Trojans as a result of rampant spread from smart phones to PC, smart phones to other phones, phones to phones, smart phones to corporate networks etc.
- Theft of mobile phones and other mobile devices by armed robbers or thieves who resale these stolen mobile devices.
- Bombing and destruction of telecommunication base stations by terrorists especially in the northern part of Nigeria.
- Loss of mobile devices by their owners to unwilling persons who refuse to turn them over to the original owners with the intention of either selling or using the mobile device(s) in any of the telecommunication networks in the country

Out of these mobile security challenges identified on the course of the research, threats posed by hackers seem to be the biggest challenge in Nigeria. The second most challenging security challenge affecting mobile users in Nigeria is the frequent or rampant losses of mobile equipment by their original owners to thieves either robbed at gun points or the owners carelessly looses the mobile phones while in transit.

V. NIGERIA MOBILE SECURITY ATTACK MODELS

We have identified in this research about five (5) mobile security attack models or patterns in Nigeria. They are as follows:

1. Smart phones to smart phones/other mobile devices (with malicious programs) attack model,
2. Mobile device to telecomm base station (with man-in-the-middle) attack model
3. Smart phones to PC (with malicious programs) attack model, i.e. hot synced attack model,
4. Smart phones to internet/mobile network (with malicious programs) attack model,
5. Smart phones to corporate WLAN Intranet (with malicious programs/hackers) attack model, and finally
6. Physical attack model.

As contained in Fig. 3, a mobile subscriber with a smart phone or any other mobile device can transmit malicious codes or programs such as virus, worms, Trojans etc. while trying to exchange file (s) with the receiver using interfaces such as Bluetooth, USB cable, infra-rays etc. Figure 4 depicts what happens when a mobile subscriber is trying to send voice, SMS, MMS to the receiver at the other end passing through the telecommunication link or base station; an attacker (man-in-the middle) which can either be passive or active can tap into the communication link of the victim with sole intention of passive eavesdropping or active modification of the message in transit. In Fig. 5, malicious programs can be transferred to a PC from smart or mobile phone or visa-visa by a subscriber who tries to transfer a file from any direction using interfaces such as USB port, Bluetooth, infra-rays etc. The attack by the malicious program in both ways is referred to as hot sync. As we pointed out earlier on, majority of mobile subscribers in Nigeria use their mobile devices as modem to connect to the internet for data services. By so doing as depicted in Figure 6 malicious programs or malwares can be downloaded straight from the internet into the mobile devices, the same contaminated mobile device can contribute in posing problem to the telecommunication network the subscriber is connected to. The most challenging aspect of security threat, as depicted in Fig. 7, comes from when mobile subscribers who use smart phones like Blackberry, IPad etc connect to the corporate intranet network while at the same time connects to the major source of malicious programs, the internet. Once the smart phone is contaminated with malicious programs, the same can be transferred to the corporate intranet network and if steps are not taken to tackle this challenge, the malicious program can start to send important highly confidential information or documents belonging to the company to the hackers who planted the malicious program on the internet. Physical attack model describes the security challenge facing Nigerian mobile subscribers in the areas of stealing of mobile phones at gun-point, bombing of mobile station base stations and telecommunication equipment by terrorists in the northern parts of the country.

Understanding thoroughly these identified attack patterns or models will help unravel the enormous mobile security challenge in Nigeria and in designing a suitable security framework that will solve the myriads of security problem affecting the telecommunication industry. Figs. 3 to 7 depict these mobile security attack models.

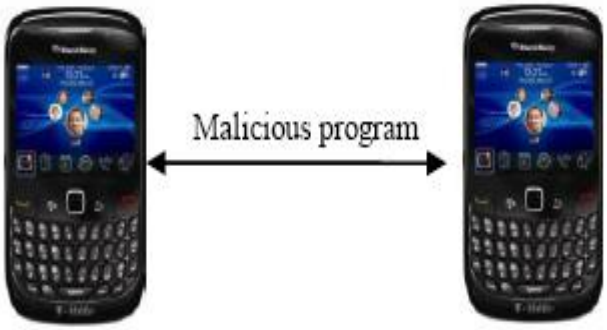

Fig. 3. Phone to smart phone/other mobile devices (with malicious program) attack model

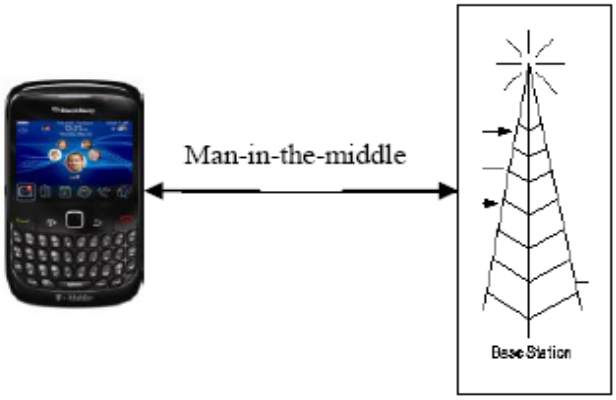

Fig. 4. Subscriber with Smart phone to telecommunication network (with man-in-the-middle) attack model

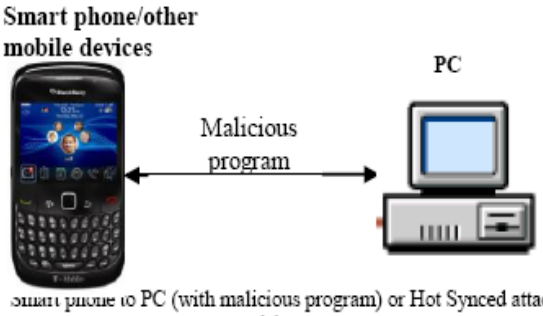

Fig. 5. Smart phone to PC (with malicious program) or Hot Synced attack model

Fig. 6. Smart phone to internet/telecomm network (with malicious program) attack model

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

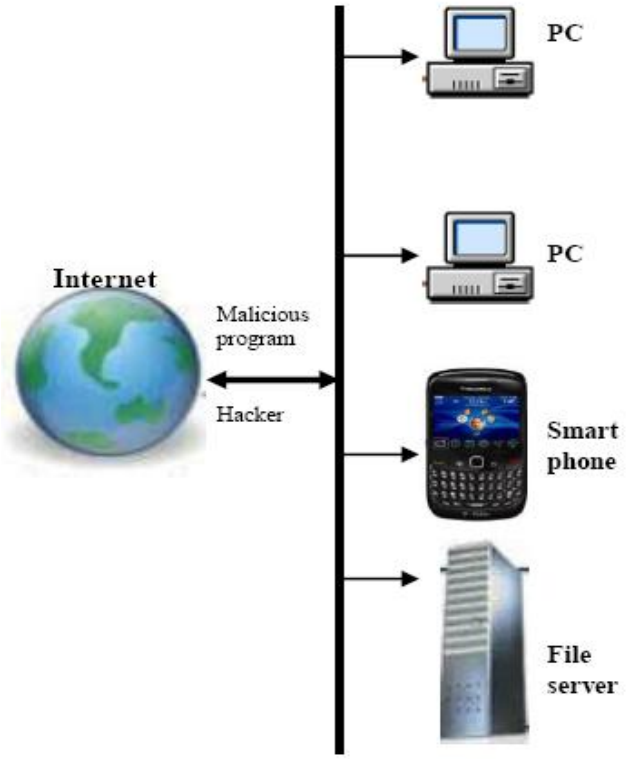

Fig. 7. Smart phone to corporate WLAN intranet (with malicious program) attack model

VI. THE PROPOSED SECURITY FRAMEWORK

In this section, we describe the proposed holistic mobile security framework that can mitigate and tackle the mobile security challenges highlighted in the paper. It covers the three-security triad of safety, attacks and privacy as well as physical, data and operational security. Before any security framework is to be developed to tackle successfully security challenges confronting a country, the security challenges themselves in the country must be studied and analyzed. Also the security attack models or patterns must be studies and understood. The security challenges affecting mobile users and platforms in Nigeria enumerated in section IV of this paper were thoroughly studied before developing this framework. Also the attack models or patterns in section V of this paper were studied before arriving at the proposed security framework.

A. Security Framework against attack on GSM data confidentiality and integrity

Attack on the privacy of mobile subscribers stem from the second attack model in Fig.5 where GSM data- voice, SMS, MMS etc. can be intercepted, eavesdropped or modified by the man-in-the-middle (hacker). By so doing the confidentiality and integrity of the mobile data can be compromised. According to [7], the use of encryption and decryption cryptographic process can be used to protect or secure GSM or mobile data – voice, SMS and MMS including epayment mobile data. To ensure that the GSM SMS data remains confidential, a password-based cipher was used to encrypt the SMS message's content. For SMS data to be secure or protected during an end-to-end communication session there is need for confidentiality and integrity of the message. Authentication can be achieved by simply looking at the message itself, which includes the sender's phone number. Encrypting the message with a password-cipher, as stated earlier, provides confidentiality while a message digest was used to ensure integrity of the GSM SMS data. Fig. 1 shows clearly the encryption and decryption methodology that can be used to protect mobile users' data engaged in an end-to-end communication session.

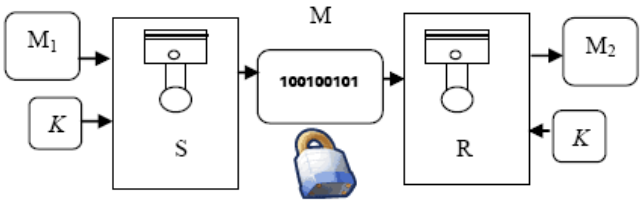

Fig. 8: End-to-end encryption and decryption of SMS data[6]

As depicted in Fig.8, using a key K_1, sender S encrypts message M_1 and sends M. The recipient R receives message and using the key, K_1, decrypts it into M_2. Provided they share the same password (private key), so that $K_1=K_2$, and no errors happen during transmission, R will recover the message so that $M_1=M_2$. Public key can also be used for secure mobile communication sessions involving more than two persons and only the genuine recipients can get the secret key and used it to communicate securely. Highly confidential or mission-critical mobile data needs to be protected using encryption and decryption cryptographic transformations protect the data from hackers or malicious codes.

B. Security Framework against attack on corporate networks

Smart phones are always connected to corporate intranets and extranets by company staff and partners and sometimes some important business information or data can be stored there even after work. A hacker whether within or from outside can connect to intranet network or portal of a company as legitimate user or uses brute-force to guess the valid logins and then login legitimately or uses malicious programs as backdoor to retrieve very confidential company data and information and afterwards turn them over to rivalry companies or even try to defraud the company using the obtained data or information. The following measures can be used to protect corporate networks from hackers and malicious codes either from within or outside:

1. Protect corporate networks using network protective devices such as firewalls from external hackers.
2. Demilitarized zones (DMZ) server to protect networks from external hackers in public networks. Fig. 9 shows a private network (intranet) protected against hackers and malicious programs using DMZ Web Servers.
3. Authentication and Authorization mechanisms and user access control mechanisms can be used to deter fraudulent employees (hackers within).
4. Use of Ant-virus and Anti-spyware programs can help in stopping the activities of hackers using malicious programs as backdoors.
5. Use of log files or audit trails can be developed and maintained to monitor the activities of internal staff of an organization to prevent or stop insider attack.

6. Company's data should be stored and secured in physically protected servers and data centers and must not be contracted or sourced out to an external service provider.
7. Tunneling and Virtualization can also be used to protect private networks from attacks from hackers. Details can be found here [8].

Fig.10 shows the connection architecture for a company wireless LAN (WLAN) intranet network with *firewall security* blocking malicious program from the internet (uploaded by hackers) from entering into the company intranet. The firewall can be a piece of hardware equipment or software.

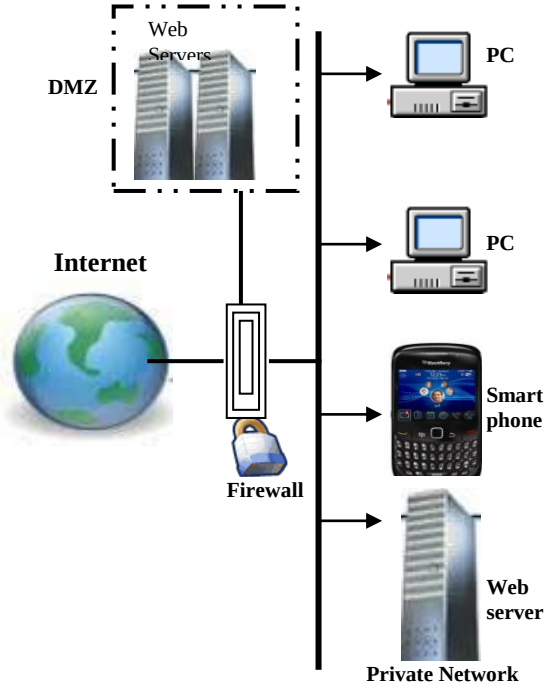

Fig. 9. A typical DMZ securing private network against hackers

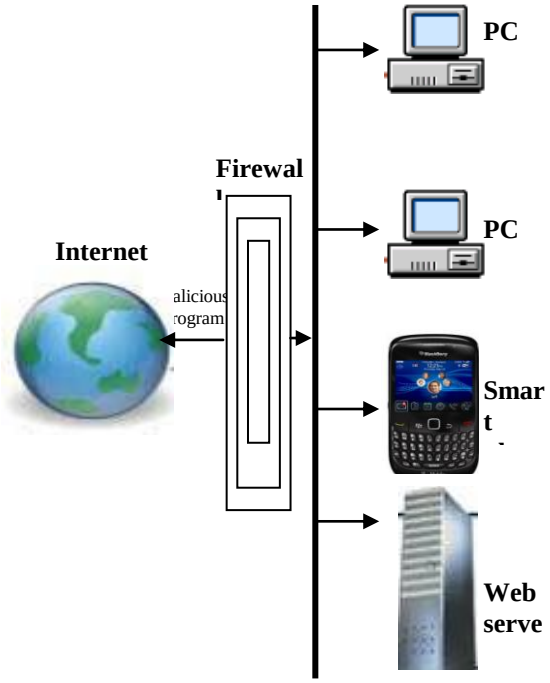

Fig. 10. Firewall security protection against hacker's attack to a corporate intranet

C. Security Framework against loss of mobile equipment or phones and bombing of mobile base stations

In Nigeria, since the inception of GSM and CDMA platforms in 2002, the telecommunication platforms (especially the GSM) have not bothered to implement IMEI (international mobile equipment identification) use to deter stolen mobile equipment from being used in the same mobile network within the country. The telecommunication watch-dog, the Nigerian Communication Commission (NCC) has not deemed it necessary to enforce compliance to this important security objective to protect millions of mobile subscribers from frequent looses of their mobile equipment. For the high incidences of loss of mobile equipment such as mobile phones, smart phones and other mobile devices to thieves and robbers preemptive measures such as discouraging the sale or use of stolen mobile equipment within the telecommunication networks of the country will help reduce incidences of theft of mobile equipment since a stolen mobile phone cannot be sold or used in the country the motives for stealing them are automatically eliminated.

Another factor that can help deter frequent stealing of mobile phones is for the mobile phone users to implement the use of security lock code inbuilt in most mobile phones to lock the mobile equipment so that once they are lost the thieves cannot find them useful in any way either to sell or use them. Installed mobile base stations by the telecommunication companies such as MTN, Airtel, Globacom, Etisalat, Starcomm etc. can be further protected if physical security mechanisms such as IP spy cameras, Close Circuit Television (CCTV) cameras can be installed in each other to capture biometric identifies of the terrorists as well as alert nearby patrol vehicles of the Joint military taskforce (JTF).

D. Security Framework against attacks from malicious programs

Most of the malicious codes or programs originated or are downloaded from the internet. Attacks from malicious programs such as virus, Trojans, spywares, worms, logic bombs, etc. pose the third highest challenge to mobile users in Nigeria. The spread of malicious programs is on the increase majorly due to the fact that most mobile subscribers use their mobile devices are modem to connect to the internet. In Nigeria, the telecommunication films serve as Internet Service Provide (ISPs) without any facility to protect the subscribers against attack from malicious programs and spywares. Some of the malicious programs are actually installed by hackers online in a bid to gain access to victim's PC or corporate network using some *backdoors* or as *zombies* to launch illegal attack against other targeted PCs or networks.

To protect user's mobile phones, PCs and corporate network against attacks from malicious codes or programs, we recommend the following measures:

1. Install current Anti-virus and spyware software on mobile phones, PCs and server of corporate networks and have them updated on daily basis in order to neutralize malicious programs and spywares.
2. Install Firewall program or hardware on PCs and corporate network to drop requests to and from

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

hackers using malicious programs as tools.

3. Users should avoid visiting some websites with security rating from some Anti-virus virus to avoid contracting the malicious programs from the internet. Email anti-virus programs should also be installed to make sure that dangerous hackers' malicious codes are not downloaded into the mobile phones or PCs.
4. Users should always back up their data on mobile devices, PCs and corporate networks to recover easily once there is attack.

E. Security Framework against attacks from hackers and malicious programs as a result of subscribers ignorance

Ignorance is a very serious challenge affecting majority of the mobile subscribers or users in Nigeria. Most of the subscribers have not obtained basic security or safety tips or education on how to circumvent most of the mobile security attacks and vulnerabilities. For instance many users do not know that they have to disconnect or switch off their mobile and smart phones' Bluetooth connectivity once they are through with the usage. Malicious program can exploit this vulnerability and wreck havoc on the user's mobile equipment, PC and/or network later on. Also because of ignorance on security issues, most of the mobile subscribers fall vulnerability to the social engineering antics of hackers and cyber criminals who capitalize on their ignorance to collect vital banking or credit information which they use to later empty their victims' bank deposits. These cyber criminals use bulk SMS telecommunication platforms to send social engineering deceptive messages to mobile users via their mobile phones to reveal their debit/credit bank details. Educating the mobile subscribers nationwide using popular mass media platforms such as radio, TV, internet, and even SMS, by both the NCC and telecommunication firms can help curb this menace by hackers and cyber criminals in the country.

VII. CONCLUSION AND FUTURE WORK

Millions of users and subscribers use mobile platforms for one form of service or the other on daily basis in Nigeria since 2002 when mobile telecommunication services started in Nigeria but there has not been a unified holistic security framework to protect mobile users and equipment from attacks, protect their privacy and their mobile data as well as ensure that critical mobile data are protected from hackers who misuse them to defraud or harm the subscribers illegally.

This paper identified and presented all the major security challenges affecting the successful and safe operations of mobile platforms by subscribers in their day-to-day businesses.

Major security challenges such as invasion of privacy of mobile data of subscribers, attacks by hackers and malicious codes on personal equipment and corporate networks, theft and destruction of mobile equipment, affecting the successful and safe operations of mobile platforms and services by users and subscribers in Nigeria in their day-to-day businesses were highlighted.

Corrective and preventive security frameworks that will ensure safe and successful implementation of mobile services and operations in Nigeria were presented in this paper. The suggested five (5) security frameworks in the paper are as follows:

1. Security framework against attacks on GSM or mobile data's confidentiality and integrity by hackers or man-in-the-middle;
2. Security framework against attacks on corporate networks by hackers and malicious codes;
3. Security framework against frequent loss of mobile equipment or mobile phones to forestall or discourage the sale and reintroduction of lost or stolen mobile equipment in Nigeria telecommunication networks;
4. Security framework against attacks by malicious codes or programs from the internet; and finally,
5. Security framework against attacks by hackers and malicious programs as a result of lack of security and technical education and knowledge by the mobile users or subscribers.

We sincerely hope and believe that these security frameworks presented in this paper will help protect the millions of mobile users and subscribers in Nigeria when implemented.

Our future work is to design and develop commercially viable mobile solutions that can protect mobile users and corporate networks against some of the identified mobile security challenges.

REFERENCES

1. National Mirror, "Telecoms: Nigeria's Teledensity hits 75.17%" , Retrieved on December 28, 2012 from http://nationalmirroronline.net/new/business/telecoms-nigerias-teledensity-hits-75-17/.
2. Trendo Micro, "The rise of smart phones and the usage on the Internet: The security issues and solutions", Retrieved on December 18, 2012 from http://www.trendmicro.com/us/enterprise/product-security/mobile-security/index.html.
3. NCC, "Subscribers Data", Retrieved on December, 26, 2012 from http://www.ncc.gov.ng//index.php?option=com_content&view=article&id=125&Itemid=73.
4. F. C. Obodoeze, F.A. Okoye, S.C. Asogwa, C. N. Mba and F.E. Ozioko, "Enhanced Modified Security Framework for Nigeria Cashless Epayment System", International Journal of Advanced Computer Science and Applications (IJACSA), New York, USA, vol. 3, no.11, 2012, pp.189-196.
5. Mynaij.com, "Cashless Banking: Cyber Criminals Now Focus on Nigeria". Retrieved on 8th August, 2012 from http://news.naij.com/cashless_epayment_in_Nigeria/.
6. T. Strang, "Lecture, Topic: "Programming Mobile Devices, Security Aspects", WS2007/2008, University of Innsbruck. pp. 15,18,19,20.
7. F.C. Obodoeze, "Cyber Security for GSM Data Protection.", Master thesis submitted to Department of Electronic and ComputerEngineering, Nnamdi Azikiwe University Awka, Nigeria., pp.84, November 2010.
8. E. Dulaney, "CompTIA Security+ Study Guide Fourth Edition", Sybex US.A., pp. 29-33.

AUHTORS PROFILE

Engr. Fidelis C. Obodoeze is a lecturer at Renaissance University Enugu, Department of Computer Science. He is currently pursuing his PhD programme in the Department of Electronic and Computer Engineering Nnamdi Azikiwe University Awka, Nigeria. He had his Masters Degree in Control Systems and Computer Engineering at Nnamdi Azikiwe University in 2010 and B.Sc Degree in Computer Engineering at Obafemi Awolowo University Ile-Ife in 2000. He had authored and co-authored several research papers at reputable local and international journals.

Dr. Francis A. Okoye is a lecturer and former Head, Department of Computer Science and Engineering Enugu State University of Science and technology (ESUT), Nigeria. He had his Ph.D in Computer Science in 2008 at Ebonyi State University Abakaliki, Nigeria.
He obtained his MSc. and BEng. in Computer Science and Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 2001 and 1996 respectively.

Mr. Samuel Chibuzor Asogwa is a Ph.D research scholar in the Department of Computer Science Nnamdi Azikiwe University Awka, Nigeria. He is currently lecturing at the Department of Computer Science Michael Okpara University of Agriculture Umudike, Nigeria. He had his Masters (MSc.) in Computer Science at Ebonyi State University Abakaliki, Nigeria in 2011 and Bachelor of Technology (BTech.) in Computer Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 1999. He was the former Acting Head of Department of Computer Science, Renaissance University, Enugu, Nigeria.

Engr. Calister Nnenna Mba is a Lecturer and former Acting Head, Department of Computer Engineering, Caritas University Enugu, Nigeria. She is currently pursuing her Ph.D programme in Computer Science at Nnamdi Azikiwe University Awka, Nigeria. She had her MSc. Computer Science at University of Nigeria Nsukka (UNN) in 2009, Nigeria and B.Eng in Computer Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 2004.

Engr. Frank Ekene Ozioko is the Director of ICT office Enugu State University of Science and Technology (ESUT) and Lecturer Department of Computer and Information Science, ESUT, Nigeria. He had several years of experience in university ICT administration and engineering as well as in teaching and research