
MOBILE DEVICE – A TOOL TO FIGHT INSECURITY IN DEVELOPING COUNTRIES

Oju, Onuoha¹, Etim, Emmanuel Okon² & Ogbonna, Iheoma A.³

Department of Computer Science,
Abia State Polytechnic, Aba

¹ojupro@gmail.com

²Iniobongabasiama45@yohoo. Com

³Job4ogbonna@yahoo.com

Abstract

This piece of work was motivated by the inability of governments to utilize the enormous potential endowed in mobile devices in combating insecurity. Basically mobile devices provide a phenomenal service that can lead the enhancement of high multimedia services such as video, text, images and audio files. This paper discusses the use of mobile device to combat insecurity in developing nations, where applications will be used in order to achieve the aims. Insecurity is one of the biggest problems that a lot of countries are suffering from. It will be observed that a good deployment of mobile technology and information and communication technology will be sine qua non for governments and security agencies in the areas of fighting insurgency/terrorism, militancy, kidnapping, armed robbery and other crimes that are disrupting the peaceful coexistence of our society and therefore, chat a better path for progressive nations.

Keywords: Mobile Device, Insecurity, GSM, ICT & Application.

INTRODUCTION

Since the beginning of the 21st century, there has been an explosive increase in the demand for tether-less connectivity. In the opinion of Licklider and Taylor (1968), in a few years, men will be able to communicate more effectively through machine than face to face. The mobile phone and other mobile devices is an embodiment of that revelation. The mobile phone and other mobile devices is an embodiment of that revelation. Mobile phones, cell phones, Personal digital assistants (PDA), smart phones and other types of digital phones with a broad range of functions are referred to in this paper as “mobile phones”.

Mobile phones in recent years have become ubiquitous. Children and young adults have them. Out of a global population of 6.8 billion people, there are 3.3 billion mobile phone users (Scott Davis, 2008). The driving force for this explosion is based on the Need for Mobility – user mobility: users communicate anytime, anywhere, with anyone, and device portability: devices can be connected anytime, anywhere, with anyone, and device portability: devices can be connected anytime anywhere to the network. Most users of mobile phones are unaware of the potentials and methods endowed therein, which can be used to combat crime. Information and Communication Technology is one of the platforms that cannot be ignored. ICT is a driving force on these mobile devices especially when it comes to insecurity where by a lot of instruments can be deployed to tackle, improve vigilance of all the organizational activities. There is a saying that security is every ones concern? Basically, ICT can be a great tool in detection and identification of citizens, their interaction and communication, movement, education and so on. The increasing rate of unemployment, illiteracy, poverty and corruption are the issues that contribute immensely to the rising level of insecurity in a developing nation. In many developing countries, there seems to be a direct proportionality between the issues mentioned above and the compulsory increase in the level of violent crimes like armed robbery, kidnapping, child trafficking, rape, militancy and even terrorism.

The inclusion of mobile devices in the fight against these vices that is increasing taking over most developing nations will certainly assist the security agencies in controlling or even eliminating these crimes. This research will therefore encourage these agencies and provide better society through its finding and recommendations.

MOBILE PHONE APPLICATIONS SECURITY

Mobile phones capable of running download third-party applications, also known as smartphones, are now pervasive. The popularity of individual smartphone operating systems, such as Android, BlackBerry OS, and iOS (formerly iPhone OS), is strongly influenced by the applications made available to users through on-phone “application stores” A cottage industry for smartphone applications has emerged, supplying tens of thousands of applications, seemingly overnight. However, the speed at which these applications have emerged leaves into question the diligence and efficacy of developers and the resulting application code. Great harm may result from malicious or faulty smartphone applications, not only to the device and user, but also to the relatively fragile cellular networks to which smartphones are attached.

Our research focuses on the security of smartphone applications. We have studied smartphone application security from various perspectives, which has resulted in multiple projects. Our overall research goals focus on the design of new technologies to protect the end user, application providers, content providers, and cellular network providers.

The smartphone marketplace has evolved significantly and swiftly during the last few years. In particular, the number and variety of third-party applications available to smartphone users has grown almost exponentially. These applications are frequently of negligible cost (often free) and undergo limited (if any) quality assurance or security verification. Unfortunately, security features in existing smartphone operating systems are insufficient to protect users against malicious or poorly designed applications.

The TaintDroid system is designed to track and identifies smartphone privacy risks created by downloaded applications. TaintDroid uses dynamic taint analysis to track privacy sensitive information from their source (eg.) GPS hardware, microphone, phone identifier storage, etc. to the point at which it leaves the phone through a wireless network interface. To perform this analysis in real time on existing smartphone hardware, TaintDroid uses several careful optimizations, trading tracking granularity for performance.

ENHANCNG SECURITY DEVICES

Close Circuit Television (CCTV)

CCTV plays a significant role in protecting the public and assisting the police in the investigation of crime. The UK is one of the most watched countries in the world McCahill & Norris, 2003). It is estimated that there are five million CCTV cameras in use today, and this number is likely to rise in the future (Gill, 2006). Even though the exact number of CCTV systems deployed in the Uk is unclear, the extent of CCTV coverage and the government's funding of new systems have increase dramatically over the last decade, yet there is little substantive research evidence to show that CCTV works.

Social perceptions and attitudes towards security have changed, and over time society has become increasingly security conscious. This change has also been a result of the mass media coverage on crime. People have changed their views as a result of terrorism, gun crime, child abductions, etc. And have adopted a more proactive role in ensuring their safely. One way this has been achieved is through investment in CCTV systems. Security is now considered essential for the protection in CCTV systems. Security is now considered essential for the protection of both people (eg. within businesses and for the general public) and their property. There is need for CCTV to be deployed.

Online Vehicle Registration

Vehicle Registration in Nigeria began over 100 years ago and the records have been essentially manual which in turn has not help to raise the efficiency of general automotive services in recent years. Today, computer has been discovered as a very efficient instrument, which has played a very significant role in adequate management of information. However, computerization has helped in many areas of life and due to vehicle owners, the thought of computerization of this operation becomes of great important in order to wipe out the manual data processing system from which many problem have originated. One of the main objectives of this research paper is to come up with an online registration for vehicle a more reliable and better medium where road network schemes are found in Singapore and Malaysia.

Electronic road control is one of the main schemes established by Singapore government to control road traffic where only licensed and registered vehicles are allowed in the road (Authority, 2016). Vehicles movement is controlled due to the installation of gantries which

determined and sensor the movement of each vehicle that pass by for the day. With the help of this system the government also introduces the electronic road pricing scheme. ERP is an Electronic Road Pricing.

System used in managing road. Based on a pay-as-you-use principle, motorists are charged when they use priced roads.

Some benefits of ERP system are:

Minimizes traffic volume.

Record of each vehicle passed for the day.

Optimizes usage of the road network.

No human error.

ERP is reliable and fully automated system operates 24 hours.

Its central computer system ensures gantries are always working properly.

SIM Registration

A SIM, Subscriber Identity Module, is the removable circuit board found in a modern cellular phone. It carries the network identity information and is a type of smart card which can also be found on payment cards (EMV), ID cards and so on. A smart card is basically a small computer, providing a safe and controlled execution environment (Edsbacker, 2010). When the GSM standard was proposed there was an obvious need for a strong user/network authorization. This meant a telephone number was to be closely tied to a subscriber account in the operator's network and at the same time making it very hard for someone to copy the information (since this might enable calls on someday else's account).

One way to solve this would mean putting the phone number, necessary encryption keys and the like inside the physical phone itself. This was method used in older American CDMA one-based networks. However, it meant that the user got one phone number for each physical phone, making replacement a big problem. In order to avoid this in the GSM networks, the authentication and user identity functionality was placed on a removable smart card. This smart card type was called a Subscriber Identity Module (SIM). The smart card command set as defined by the ISO standard was extended to make it possible for the SIM to perform user interaction. Examples of such commands are the ability to display text on the phone's display, get user input and sending/receiving SMS. Some developing country like Nigeria and other nations embarked on a nationwide SIM Card Registration Project to help tackle insecurity. This was necessitated by the fact that in 2008, security agencies approached the Commission in to assist them in resolving crimes perpetrated through the use of telephones in which criminal elements could not be identified with the number of the phones that they use.

The objectives of SIM Registration exercise were:

To assist security agencies in resolving crime and by extension to enhance the security of the state.

To help monitor suspected person on the calls they answer.

To enable operators to have a predictable profile about the users on their networks.

To enable the Commission to effectively implement other value added services like Number Portability among others.

GPS Driver's License

A GPS Tracking unit is a device that uses the Global Positional System to determine the precise location of a vehicle, person, or other asset to which it is attached and to record the position of the asset at regular intervals. The recorded location data can be stored within the tracking unit, or may be transmitted to a central location database, or internet-connected computer, using a cellular (GPRS), radio, or satellite modem embedded in the unit. This allows the asset's location to be displayed against a map backdrop either in real-time or when analyzing the track later, using customized software. A GPS tracking system uses the GNSS (Global Navigation Satellite System) network. This network incorporates a range of satellites that use microwave signals which are transmitted to GPS devices to give information on location, vehicle speed, time and direction. So, a GPS tracking system can potentially give both real-time and historic navigation data on any kind of journey. A GPS tracking system can work in various ways. From a commercial perspective, GPS devices are generally used to record the position of objects e.g vehicles as they make their journeys. Some system will store the data within the GPS tracking system itself (Known as passive tracking) some send the information to a centralized database or system via a modem within the GPS system unit on a regular basis (Known as active tracking).

GPS tracking System is one of the most rapidly growing technologies around the world. Most developed countries have focused on the GPS technologies in resolving some of their inherent security problems. According to Michael and McNamee (2006), Global Positional System (GPS) is increasingly being adopted by private and public enterprise to track and monitor humans for location based services (LBS). A location-based service (LBS) is information or entertainment service, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device. LBS can be used in a variety of contexts, such as health, indoor object search, entertainment, work, personal life, etc. LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking.

Explosive Device Detectors

Nowadays a lot of attention is being paid to the development of methods and instrumentation for the detection of explosive devices. Initially explosives have already killed thousands of people and injured several tens of thousands worldwide not only Nigeria, Infrastructural facilities, like railway stations, airports, undergrounded railways, security offices, electricity, water supply, etc. are preferred targets involving up to thousands of people. Assuming, the methods will be found to early detect explosives by means of sensors. New forms of bomb attacks are more sophisticated, more dangerous, using remote control of Improvised Explosive Devices (IED); initiation by mobile phones permits terrorists to initiate a bomb immediately. Therefore, detection systems with a reliable detection efficiency used in broad range of IEDs are an important problem. An IED is an improvised explosive charge, equipped with a non-standard (home-made) or a professional detonator. But, an Improvised Explosive (IE) may be any chemical or mixture capable of an explosive reaction. IED detection techniques can be divided into two groups: bulk detection of explosives, and trace

detection of explosives. In bulk detection, a macroscopic mass of explosive material is detected directly, usually by viewing images made by X-ray scanners or similar equipment. In trace detection, the explosive is detected by chemical identification of microscopic residues of the explosive compound. These residues can be applied in either or both of two forms; vapor and particulate.

TELECOMMUNICATION REGULATORS AND NATIONAL SECURITY

Telecommunications constitutes an important sector for any modern society. It is an essential infrastructure, which stimulates the development of other sectors such as commerce, industry, agriculture, education, health, banking, defense, transportation, and social interaction. “With the implementation of the National Telecommunications Policy, Nigeria’s telecoms industry has undergone significant development in the last 15years” (Tosin, 2015). According to International Telecommunication Union, the number of people connected to the internet is 24 million. This figure is low when compared to countries with up to 150 million users. Although the Nigerian Communication Commission (NCC) has embarked on different regulatory framework and initiatives aimed at increasing internet access in the country, there is no synergy with the security agencies on ways to handle the security challenges that will accompany such increase. Tosin also was of the opinion that the NCC also requires that every single active mobile telephone number has the owner’s biometric data registered. The SIM card registration exercise has running since the past two years to build a database of telephone subscribers as well as assist in crime monitoring and control. NCC should have the means of tracking those sophisticated mobile devices that not connected to the services provides in Nigeria.

CONCLUSION

In this work, we have attempted to advance the course security and mobile devices in developing nations by examine various options that can make it succeed. With the adoption of the mentioned ICT applications, a significant surveillance can be obtained where a lot of activities can be monitored and controlled. In the end it is hoped that there will be harmonized security arrangement, where all the activities and functions specific agencies are pooled together under one umbrella aimed at having timely access to security information by everyone living in these developing nations using mobile devices. Such arrangement will help governments to fight insurgency/terrorism, militancy, kidnapping, armed robbery reduce cost of governance and chat a better path for a progressive nation.

RECOMMENDATIONS

For any government and National Security agencies to restore security they must rise to their responsibilities and take back control of their Cyberspaces and the transmissions that go on here and there. As the user-base and the technology keeps evolving where more sophisticated and enhanced devices keep emerging, it becomes only imperative and inductive that the National Security forces implement technology or ICT applications proactively in order to manage the new trend of events and data transmission nationwide. The security should be nationwide not only implementing it is areas affected by crimes. Moreover, the authors recommend and emphasize the fact that the responsibility of National Security lies also in the hands of the citizens and not the security agencies alone. National security is all about people, and the people must also duly contribute their part as they all strive to restore peace and security to their nation. Every suspicious transmission, movement, communication within the circle of reach of every citizen be reported to the nearest and appropriate authorities for

prompt action to be taken. The citizens have to be ready to comply and also have in mind that security is every bodies business.

The National Identity Management Commission and the Nigerian Communication Commission should be able to provide the security agencies with databases that are biometrically assembled. These data include photographs, fingerprints, and geo and bio data of citizens as a way of officially documenting Nigerians. Other forms of digital data capturing include GSM subscriber's registration, the issuance of passports and driver's licenses.

REFERENCES

- Authority, L.T. (2016, March 10). Local Transport Authority. Retrieved March 10th, 2016, from Local Transport: <http://www.Ita.gov.sg/content/Itaweb/en/roads-and-motoring/managing-traffic-and-congestion/electronicroad-pricing-erp.html>.
- Biham, E. & Dunkelman, O. (2000). Cryptanalysis of the A5/1 GSM Stream Cipher. In B. Roy & E. kamoto (Eds.) Progress in Cryptology-INDOCRYPT 2000, Springer, India. ISBN: 354041525.
- Blurton, C. (1999). New directions of ICT- Use in education. In World Communication and Information Report 1999-2000 (On-line). Available: <http://www.unesco.org.education/educprog/lwf/edict.pdf>.
- Davis, S. (2008). Mastering rails: Rails and the mobile web. Retrieved from <http://ibm.com/deveperworks/java/library/j-grails06178/>
- Edsbacker, P. (2010-06-12) An introduction to SIM card application development. Sweden: Edsbacker, Peter.
- Gill, R. (2006), Theory and Practice of Leadership, London: Sage Publications Interview: Recharad Armitage.
- Licklides, J.C.R., & Taylor, R.S. (1968). The computer as a communications device, Science and Technology, 76,21-31.
- Mccahill, M & Norris, C. (2003, Estimating the Extent, Sophistication and Legality of CCTV in London; in M. Gill (ed.) CCTV, Perpetuity Press.
- Obi, V.C. (2005): Information Communication Technology Skills Needed by Business Education Teachers from Effective Instruction in the Secondary Schools in Enugu State. The Journal of World Council for Curriculum and Instruction, Nigeria Chapter 4, (2), 99-106.
- Tosin Akinjobi (2015); NCC and Nigeria's Biometric Database; Daily Independent, Nigerian Newspaper. March 14, 2015; [Http://Linkis.Com/Htwwa](http://Linkis.Com/Htwwa).