Analysis of methods and techniques used for Intrusion detections in mobile devices

Olorunfemi Tope Roseline

Department of Electrical and Electronic Engineering Science, University of Johannesburg, Auckland Park Kingsway Campus, 2006, South Africa

toppyrose6@gmail.com

Nwulu Nnamdi

Department of Electrical and Electronic Engineering Science, University of Johannesburg, Auckland Park Kingsway Campus, 2006, South Africa

nnwulu@uj.ac.za

Abstract

The rapid evolution in the use of smart mobile devices has greatly enhanced the lives of humans and their ability to disseminate and store information. These smart devices have revolutionized our personal life, work life and businesses with vast amount of Information stored on these devices. However, this poses a great threat of unauthorized access to the confidential information stored on these devices. Hence, there is the need for Intrusion Detection System (IDS) in smart mobile devices. An Intrusion Detection System can be deployed in mobile devices to detect attacks that might want to cause damage to the device, or steal the user's resources and suggest appropriate remedies measures to be taken. This paper presents a review of the state of the art pertaining to intrusion detection in mobile phones and analyses recent methods and techniques used for this task.

Keywords: Intrusion Detection system, Internet, Information Technology, Mobile phones and Security.

1.0 Introduction

Mobile phones are portable devices which can be carried from one place to another. These devices are now being used on the go to perform official and business dealings such as bank transactions, purchasing and selling. All these

activities leave users confidential information's stored on the mobile phones. This information must be safeguarded from falling into wrong hands, loss theft etc. Malicious content is another major issue that mobile phone users contend with. Malicious contents are unwanted/unsubscribed content that get delivered to mobile phones. These unwanted contents use a phishing attack to trick users by sending fake/deceitful SMS's. when these fake SMSs are sent to users and they open them. The malicious SMS redirects the phone to malicious websites where malware, such as virus and Trojan are downloaded to the device. All these mishaps get themselves into the device, multiply and steal the user's sensitive information by transferring it to a remote server where they make use of it. The malware causes Denial of Service (DoS) in mobile devices which may lead to crashing of the device completely if care is not taken [1]. The goal of this paper is to make sure that Confidentiality, Integrity and Authentication (CIA) of these devices is not compromised. The remaining sections of this paper are as follows; Section 2 presents the literature review on mobile threats and vulnerabilities, section 3 presents literature review on IDS techniques, section 4 gives some recommendations and section 5 gives the conclusions.

1.1 Features of mobile devices

Mobile phones are handy and are easily susceptible to attacks. Some of the features of these devices which make them vulnerable to attacks are highlighted:

i. **Mobility**: mobile phones are durable and can be taken from one place to another. This exposes the devices to the danger of getting stolen or lost.
ii. **Strong connectivity**: mobile devices have the capability to connect to each other or to other devices over a network.
iii. **Strong personalization**: as an individual device, it is not commonly shared among multiple users hence it is meant for personal use and personal information is stored on it.
iv. **Technology convergence**: Several hi-tech features are embedded in the Smartphones, such as gaming, video conferencing, chatting and use of the social media etc [2].

2.0 Literature review of mobile threats and vulnerabilities

In a wired set-up, there are set of protections, safe guards, rules and regulations, which prevents intruders and makes the communication secure through devices like firewalls, secured gateway etc. - unlike the mobile set-up with several decentralized and dynamic nodes, which connect the frequency with the device. However, these make the networks more vulnerable to various forms of attacks. It is, therefore, pertinent to know these security vulnerabilities and the defensive mechanisms to guide against them using mobile phones. Reference [3] highlighted some threats and vulnerabilities which the attackers can exploit to gain unlawful access. These can be grouped into two broad headings: **mobile threats** and **mobile vulnerabilities**. Mobile threats can be further divided into four sub-headings namely: Physical threats, Application- based threats, Network-based threats and Web-based threats while mobile vulnerabilities and has three sub-divisions: root kit, worm and Trojan horse vulnerabilities respectively. Physical threat is the major concern faced by the mobile device users today. Since the device is portable and can be carried from one

place to another, this in turn exposes the device to the danger of theft [4]. Theft of mobile devices or it's loss is a major threat to mobile device users because the device can be resold in the market and personal data will be lost/ gone which can threaten the user's private/ sensitive information.

According to [5] there are four basic application based mobile threats:

(1) Trojan threat: this is a major mobile malware threat which utilizes techniques of social engineering by downloading itself on mobile phones without the user's approval. It makes changes to one's phone by sending unsolicited SMS, increase phone tariff and allow attackers to have full access to the system by exploiting its vulnerabilities.

(2) Privacy threat: this is a kind of threat which maliciously reveals the International Mobile Equipment Identity (IMEI) Number and device location information of mobile phones: This can lead to attack on the mobile phones which violates user's privacy. Other types of privacy leakage include: Phone numbers, Call logs and SMS logs [6].

(3) Adware applications: These sets of applications creeps into the phones surreptitiously and install itself without the user's permission. They are very difficult to identify or get rid of from the system. The purpose of these applications is to show unwanted advertisement to users. it also serves as a perilous spyware that watches the activities of the user's and steal private information's such as call logs, email, SMS"s, photos, etc.

(4) Session Initiation Protocol (SIP) Threats: "Session initiation protocol" is a connection procedure for producing signals and controlling multimedia message connections such as video and voice calls. The main use of SIP is for internet calls and instant messaging over internet protocol (IP) networks. Vulnerabilities in SIP is a major window for attackers to exploits mobile devices, which can pave the way for attackers to launch attacks against the devices by listening to confidential voice communications and as well lunch denial of service attack against the mobile devices which sometimes crashes the devices [7].

In [8], the web-based mobile threats: were detailed. Web-based mobile threats: are threats which occurs when a user attempts to access the internet using a web browser. This gives an opportunity for unauthorised exploitation of the mobile device. Example is phishing trick threat: phishing is a way of getting useful and valuable private or business data from the user, while presenting itself as genuine links. The purpose is to steal valuable information or try to gain access to users log in details.

A very common web based mobile threat is the "drive by downloads" which is a phenomenon whereby a user visits malicious website and automatically downloads malicious applications on the device causing it to be ineffective. This can be minimized by users being careful of the type of website they surf. Users should also avoid clicking unsolicited links and downloads. There is also another web based threat termed "browser exploit threat" which is threat that takes advantage of the flaws in the mobile phone browser application when accessing music files, flash share, Pdf files, etc. All these get attacked when surfing on a malicious browser.

Mobile vulnerability is a breach in security system of a mobile device, due to flaws or weaknesses by the developers during the development stages of the device. The vulnerabilities include the following: Root kit vulnerability which

affects the operating system of the device by installing malicious applications on the device. Another vulnerability is Worm vulnerability which is a malicious code that duplicates itself on the mobile device. is through the network. Worms are deadly as they breach the defence of the mobile device. The final vulnerability is Trojan horse vulnerability which inflicts the device with malicious applications such as worm to steal valuable data which it does through phishing [9].

3.0 Literature review on IDS techniques in mobile phones

The mobile phone has taken the centre stage in communicating and transacting in this dispensation. Thus, lots of confidential information is stored on the device. Therefore, there is need for an intrusion detection system so that the people and the device can be safe. IDS can detect unwanted or any abnormality on a smart mobile phone. This can be done either through any of the available mobile Apps in stores or through spam filtering techniques. In [10], an online-security system was developed to detect calls from mobile lines already classified as being fraudulent. The work was based on an "artificial-neural network with Radial Basis Function (RBF)". The RBF model can recognize patterns and perform classification. Thus, historical and recent information about the activities and the usage of the mobile phone were collated in training the RBF model. The information from mobile users collated include: location of the call, time of call and the network used, days of the weeks, international or local calls, etc. This collated information was saved in a database and used to screen incoming calls to determine if it's genuine or not. The security solution was also used for both security systems against cellular-phone cloning and to identify imposters and perpetrators. The system works in such a way that if a user is calling, it will be checked against the saved log files in the database created from the various features of the phone and checked whether it correlates with what they have in the saved file. If it corresponds, the call goes through if not it is denied. Then both the genuine user and the service provider would be notified immediately. This has helped the telecommunication company in reducing their losses; and, the mobile phone user; since it reduces the cost of making calls.

Power consumption in hand-held devices is very critical to the usage of the devices. If there is no power, there would be no computing for the device. The normal life expectancy of a mobile-phone battery is at least 30 days. If there are less than this – then it gives signals that the device maybe under one or more attacks. Therefore, battery power is very essential in mobile devices. This aspect needs to be researched, to detect any attacks draining the power of the battery; and, to protect the devices. However, in [11] their paper designed a system called "Host-Intrusion Detection Engine (HIDE)". This ensures that the power behaviour in a mobile phone is checked to detect possible intrusion. This was done by taking into consideration the irregularities of the power consumption in the device. This is done by measuring the consumption of the power over a period (T) and energy (E) to determine whether the device is under an attack. The system also provides an early alarm, to detect any attacks - before irreparable damage is caused to the device; and it also protects the battery lifecycle.

Mobile-phone users need to get a good security system to be free of from malicious programs. Mobile malware, such as Trojan, virus and worms are on the rampage, to steal user sensitive information stored on the phone. This will be achieved by sending SMSs to users which contains malicious links. The SMS will suggest to user site to visit. Consequently, [12] have come up with a model which can be used to detect Trojan malware in mobile devices. They used a misuse-detection system, based on a behavior checker. Misuse detection is very efficient and fast at detecting the malicious behaviours of known attacks. Since a mobile phone has only limited features, it was easy to compile the database of behaviours known attacks. Furthermore, it can detect malicious applications which tend to send SMSs - without notifying the mobile-phone users; while the behaviour checker monitors the activities of the applications that run in the system.

The proposed solution works in such a way that whenever an application wants to use any of the messaging features, it needs to establish a session with the message server. A detector application will now observe all the sessions and monitor all the messaging events in the session. If it correlates with the known attack, it is suspended; and it notifies the user, as follows: "*ACTIVATE_MONITOR_RESPONSE_SUSPEND LIST"* The app was tested on a Nokia mobile phone with a Symbian operating system; and it works as expected. The number of mobile-phone users has increased drastically in recent years - due to the features that now come with them. The amount of information stored on these devices is considerable; and the security can no longer be compromised. Therefore, the single authentication and validation is no longer adequate for mobile-phone security. Hence, [13] established a "host based IDS system, based on a statistical model and Biometrics" in order to detect fraud and abnormal activities on mobile phones. The system algorithm was developed with multiple sensors installed on the device to monitor user altitudes and keep tabs of the records of the day-to-day activities. The system consists of two layers. The first layer is to give a warning to the user that an abnormal behaviour is suspected. It is then necessary that the user re-authenticates itself, to be able to continue with the device. The second layer consists of an alarm-triggering sensor. If the user ignored the first warning, the alarm will be triggered, thereby notifying the user that another authentication is required for further authentication; and this time it must be biometric, to continue with the use of the device. The model was developed and tested and it works as expected which improves the security of the mobile phones.

The Smartphones being produced these days comes with advanced processors, operating systems; and they can perform work that a computer can do successfully. This makes the phones vulnerable to various attacks and malicious software applications, such as a virus, Trojan and worms. Against this background, the study conducted in [14] uses cloud computing services for intrusion detection and recovery process. The cloud service was deployed with a mobile-host agent, known as lightweight, which was installed in the form of an application on the android-mobile device. The system uses a proxy, which duplicates the exact nature of the device; and it is stored in the cloud. It also duplicates all the traffic between the mobile device and the internet; and it then sends them to the cloud environment for an in-depth inspection to be carried out. The cloud-computing service takes input from the mobile device, and performs the detection and identification of any malicious abnormal behaviour over the network. It also serves as the access control for the mobile device, as well as any applications and the services in the device. The lightweight does the recovery where necessary. The architecture has four basic components, which are: the emulator, which copies the exact

residence of the mobile device in the cloud, the memory scanners: these scan the device for resident attacks, to act against it. The system was called the anomaly detection: and it calls the detection of an anomaly very fast. Therefore, it is applied solely as the system calling device. The antivirus software: this runs in the emulator to detect the abnormal malicious signatures, such as Trojan, viruses and worms. The system was tested on android mobile phone and proved to be good in detecting malicious applications; and it also serves as recovery process whenever required.

Mobile phones are usually open to attack and the threat especially that of theft when left unattended in public places. In protecting these devices, the focus should not be only on the information and data in the mobile phone, but also the mobile phone itself. The use of a conventional password and drawing patterns are no longer enough to secure the mobile devices these days. Therefore, there is a need for more comprehensive security solutions. The use of biometrics has also been deployed in several approaches, such as voice, face and fingerprint. Unfortunately, these biometrics alone are not good enough to secure the device. Thus, [15] proposed a biometric approached combined with the biometric charger, which serves as the device dongle. The mobile phone and the mobile-phone charger will be utilized as capacitive fingerprint readers. The system proposed that when a mobile phone is bought, it should be programmed with the user finger-print and the mobile-phone charger. It was recommended that it is only be the mobile phone manufacturer that can do the re-programming, if required. “The fingerprints then become the encrypted key, which the two devices need to use for synchronization. The battery is recommended to be in-built and should not be detachable from the phone, such that if separated from the device, the mobile phone becomes useless; because both devices and fingerprints need to synchronize before it can work. If this solution is deployed; the theft of intrusion of mobile phones would be discouraged.

Mobile phones with Bluetooth-enabled feature expose the devices to great risk. The sensitive information on the mobile phone can easily be stolen - if there are no proper security mechanisms in place for such mobile phones. Consequently, [16] developed a system called “Bluetooth Logging Agent” (BLA), to detect malicious and unauthorized access in wireless network through Bluetooth features. This works with another system called “Bluetooth mobile-module logging” which houses the databases built; and it uses verification and authentication rules to verify all the communications between the mobile phones and the remote devices. When a communication is initiated, an alarm will notify the mobile phone users that there is an intruder. If the user needs to connect, it will be accepted else will be rejected. The system was tested on mobile phones and it was discovered that it improves the authentication of the Bluetooth-enabled device security.

The work done in [17] is titled “A bio-signal based framework with Electroencephalography (EEG) with Statistical analysis, Hidden Markov Model (HMM) and Support Vector Machine (SVM)” to detect unauthorized access in mobile phones. Since the EEG technology is a novel technology that is used in medicine to diagnose patients’ brain disorders and migraine. However, the human brain waves correspond to the physiology and behavioural facts in relation to an individual. It has now been used in the field of security to detect unauthorized users. The research was carried out by developing an “authentication system for mobile devices” using “Electroencephalography (EEG)”. The EEG was developed with wireless connectivity through the means of Bluetooth with the “Headset-Hidden Markov Model

(HMM) and the Support-Vector Machine (SVM)". In the experimental set up, signals of fifty (50) different users with their brain waves were taken; twenty (20) were of genuine users and thirty (30) of unauthorized users for testing. when an individual is drawing pattern to unlock their mobile phones, signals of users are simultaneously taken to classify a genuine user from forgers. The brain signals were also captured using EEG android APIs Smartphones connected to the "EEG headset by using Bluetooth technology". Consequently, the system experimented with three security standard bio-metric, namely: "Half Total Error Rate (HTER), Receiver Operating Characteristics (ROC) and Detention Error Trade-off (DET)". When a forger is trying to get unauthorized access to the user's mobile device by drawing the user pattern, which the forger must have stolen from the user. The EEG receives the forger's brain waves and compares it with that of the genuine user. If it matches, it's gets authenticated; otherwise access is denied. The work was tested on mobile devices and result proved competent.

This table captures some of the literature already reviewed above just to give a clear picture and further clarification on the IDS method used, the type of intrusion they detect and the year of publication.

Table 2.1

S/N	Name of Authors	Intrusion Detection System Used	Threats detected in Mobile Phones	Year of Publication
1	Muhammed and Abdulhamit	Host – based and AMOXID	Threat of privacy infringement	2010
2	Azzedine and Mirela	Neural – networks and pattern recognition	Fraud	2002
3	Grant *et al*	Battery- Based IDS and Host Intrusion Detection Engine	Attacks on battery	2004
4	Yap and Ewe			2005

		Misuse detection on behaviour checker	Malware application (Trojan)	
5	Michalopoulos and Clarke	Host – based, statistical model and Biometrics	Fraud on mobile phones	2006
6	Rohit and Thangakumar	Cloud based computing and recovery system for Android	Misbehaviours in network	2012
7	Donny et.al	Biometrics and Dongle technology	Theft of mobile device	2013
8	Kishor et. al	Bluetooth logging agent	unauthorized access through wireless Bluetooth	2015
9	Pradeep et.al	Electroencephalography (EEG) with "Hidden Markov Model (HMM) and Support Vector Machine (SVM)"	Unauthorized access into the mobile phone	2017

4.0 Recommendations to smart mobile phone users

There are some bad approaches in which users engaged in when surfing the internet. These could lead to security and privacy problem. These also in turn has impact on the Personal Information Identity (PII) of users, and has posed lots of problems to the mobile phone users. These are captured as follows: Firstly, among all are unsafe data storage: The personal information and data, such as credit card numbers, emails correspondence, SMS messages and more that are stored on the mobile device are unsafe. The sensitive information on the device gets into wrong hands if the device is lost or stolen. Therefore, it is advisable not to store private and important data on these devices.

Secondly, avoid long session loggings management: Session login management becomes imperative in both mobile devices and PCs, especially when surfing websites over the internet. However, long-session login is very dangerous and should be discouraged. hijackers can use such vulnerabilities to login to one mobile device and steal valuable information. As such, session-login management should be brief; and when it's taking longer, the session should be terminated automatically.

Thirdly, there is also what we call several logins: several logins should do with users using one universal password for several accounts. This is a practice such as using same password for social networking accounts, emails, bank transfer etc. These accounts can easily be hacked into if the one and only password is eavesdropped into by attackers. As such, this should be discouraged among mobile-device users.

And lastly, weak validation: Conventional passwords are the most commonly used among users. This is not good enough to secure the mobile devices. Alongside password; there must be other high-level security combined with normal password just as proposed [6] to use "face recognition for mobile-device authentication".

5.0 Conclusion

From literature, we could conclude that a lot has been done in the field of intrusion detection in smart mobile phones. However, there are still much gap to be filled. As researchers are finding solutions to problems the more sophisticated the attackers are going deep into finding their way round and to counter the solutions. Therefore, the research and solutions must be on-going. Nevertheless, it is important to abide by the simple rules and regulations when using the internet. Also, it can be deduced from the literature reviewed most intrusions countered is privacy infringement, which is very key in breaching the CIA of the smart mobile devices.

References

1. Jian, P., Kim, R. and Helen, A. "User profiling in intrusion detection" Information Technology and Mathematical Sciences, University of South Australia, Australian Department of Information Systems and Cyber Security, University of Texas San Antonio, USA School of Computer Science, China. (2016).

2. Sujithra, M., Padmavathi, G. and Sathya, N. “A cryptographic Approach by Outsourcing Mobile data to cloud” Department of Computer Technology and Applications, Coimbatore Institute of Technology, Coimbatore, India (2015).
3. Shabtai, L., Teneboim, D., Mimran, L., Rokach, B. and Shaoira, Y. “Mobile Malware detection through analysis of deviations in application network behavior” Department of Information Systems Engineering, Ben-Gurion University of the Negev, Beer Sheva, Israel (2014).
4. Arun, R., Parth, H., Hui, Z, Jinyoung, H., Chang, L. and Chen-Nee, C. “Uncovering the footprint of malicious traffic in wireless-mobile networks” Journal of Computer Communications. Pages 95-107 (2016).
5. Nisha, P., Shantanu, S. and Awadhesh, K. “A survey on 5G: The next generation of mobile communication” Department of Computer Science, Ben-Gurion University of the Negev, Israel and Department of Computer Engineering, National Institute of Technology, Kurukshetra, India. (2016).
6. Esteban, V. and Daniel, G. “Face recognition for authentication on mobile device” Galician Research and Development Centre in Advanced Telecommunication, Spain. (2016).
7. Muhamed, H. and Abdulamit, S. “Intrusion Detection on Smartphones”. Official Android documentation: http://source.android.com/tech/security/index.html (2010) accessed online on 18th April 2018.
8. Chi Heon, K., Chun Kee, C., Yunhee, C., HyunJeong, S. Jiwon W., Sung-Mi, K. and Hyuk-Joon, L. “The usefulness of a mobile device-based system for patient-reported clinic”. The spine Journal. Pages 843-850 (2016).
9. Taejin, H., Sunghwan, K., Namwon, A., Jargalsaikhan, N., Chiwook, J., Jongwon, K. and Hyuk, L. “Suspicious traffic sampling for intrusion detection in software-defined networks.” School of Information and Communications, Gwangju Institute of Science and Technology, Gwangju, Republic of Korea (2015).
10. Azzedine Boukerche “Behavior-Based Intrusion Detection in Mobile Phone Systems”. Journal of Parallel and Distributed Computing. Pages 1776-1490 (2002).
11. Grant, A., Nathaniel, J. and Davis, I. “Battery-Based Intrusion Detection”. Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University (2004).
12. Sung, H., and Hong, T. “A Mobile Phone Malicious Software Detection Model using misuse detection on Behavior Checker”. Faculty of Information Technology, Multimedia University, Malaysia (2005).
13. Michalopoulos, D.S and Clarke, N.L. “Intrusion Detection System for Mobile Devices”. Network Research Group, University of Plymouth, Plymouth, United Kingdom (2006).
14. Rohit, S.K. and Thangakumar, K. “A Cloud-Based Intrusion Detection System for Android Smartphones”. Proceedings of International Conference on Rada, Communication and Computing (ICRCC), SKP Engineering College, Tiruvannamalai, India. Pages 180-184 (2012).
15. Donny, J.O., Liza, P. and Lei, C. “Preventing Cell Phone Intrusion and Theft using Biometrics Fingerprint Biometric Security Utilizing Dongle and Solid-State Relay Technology”. IEEE security and Privacy Workshops, Huntsville, Texas, USA. (2013).
16. Kishor, K.N., Albert, H. and Johan, V.D. “Intrusion Detection in Bluetooth-Enabled Mobile Phones”. Council for Scientific and Industrial Research (CSIR), Modelling and Digital Science (MDS), Pretoria, South

Africa and Faculty of Engineering, Telkom Centre of Excellence, North-West University, Potchefstroom Campus, South Africa. (2015).

17. Pradeep, K., Rajkumar, S., Partha, P. and Debi, P. "A bio-signal based framework to secure mobile devices". Department of Computer Science and Engineering, Indian Institute of Technology, India and School of Electrical Sciences, Indian Institute of Technology, Bhubaneswar, India, Journal of Network and Computer Applications Pages 62–71 (2017).

Biographies

1. Tope Roseline, Olorunfemi is a student, teacher and security expert. She received BSc degree in Computer Science from Kogi State University, Nigeria, and MEng in Electrical and Electronic Engineering Science Department, University of Johannesburg, South Africa. She is currently pursuing her PhD degree in power system security at the Department of Electrical and Electronic Engineering Science, University of Johannesburg. She is a member of Institute of Information Technology Professionals South Africa (IITPSA) and South African Institute of Computer Scientists and Information Technologists (SAICSIT). She has demonstrated working in the corporate industry for more than 5years before furthering her education. Strong education professional skilled in mobile App development, mathematical optimization, information security and intrusion detections.
2. Nnamdi Nwulu is a researcher, educationist and engineer. He holds BSc and MSc degrees in Electrical & Electronic Engineering and a PhD degree in Electrical Engineering. His research interests include application of mathematical optimization techniques, soft computing and energy systems. He is currently an Associate Professor in the Department of Electrical & Electronic Engineering Science at the University of Johannesburg. He is also a Professional Engineer registered with the Engineering Council of South Africa (ECSA), a Senior Research Associate in the SARChI Chair in Innovation Studies at the Tshwane University of Science and Technology and Associate Editor of the African Journal of Science, Technology, Innovation and Development (AJSTID).