International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 8, Issue 5, September - October 2019 ISSN 2278-6856

Protecting against eavesdropping on Mobile Phones to snip data with Information Security Awareness and Steganography principles.

Ms Istteffanny Isloure Araujo[1], Dr Hassan Kazemian[2]

[1]Intelligent Systems Research Centre from School of Computing and Digital Media of London Metropolitan University, Flat 3, 48 The Brent, Dartford, DA1 1YN, United Kingdom,

[2]Intelligent Systems Research Centre from School of Computing and Digital Media of London Metropolitan University, 166-220, Holloway Rd, London, N7 8DB, United Kingdom,

Abstract: ***Eavesdropping on Mobile Devices is the primary concern here. Since the mobility of computers, including laptops, tablets, PDAs and smartphone, are demanding and criminals now start to target these devices as the usage is more than desktops. This initial research is focusing on drawing attention to this topic. Let set how to combat mobile interception by criminals tends to investigate whether steganography applications can benefit digital criminals' interception on such devices. The concentration is on mobile phones interception by criminals to steal personal data; therefore, it consists of developing a framework, mechanism and algorithm to prevent it. The anticipated implications imply Legal and Ethical Issues. Everyone should familiarise and follow this carefully to make sure it does not cause any particular privacy concerns to general individuals. Only personal and authorised devices were used to test the technical work produced by this research.***

Keywords: Algorithms, Espionage, Interception, Privacy, Smartphones, Surveillance, Steganography.

1. INTRODUCTION

Eavesdropping must be an issue in politics where the government is worried about individuals' privacy rights if they suspect the person is a criminal. Government has been spying on prospective terrorist. Government does for the common benefit. There are not many concerns of breaking any laws, but instead to protect the population. However, criminals have started to take advantage of eavesdropping technology to facilitate crimes. In addition to eavesdropping, another technology that can be useful to criminals is steganography. They can hide contents in other files and applications to infect people's mobile devices. They are eavesdropping on Mobile Devices to steal data such as passwords. There is a need for a framework in Smartphone in order to build a framework, mechanism or robust algorithm to identify and fight back.

Focusing on the safety of Mobile Devices is essential. They are substituting computers. Desktop capabilities adjusts to mobile devices now. They can be taken anywhere with individuals from which they are performing serious, sensitive transaction like mobile banking that must be securer, trustful. This trust depends not only of the mobile application itself but on the safety of the device as well, from physical security to application usage. The crucial question is "How to combat interception of Criminals on Mobile Devices when they are eavesdropping?" Another relevant question is "How can Steganography be used to Eavesdrop Mobile Devices and steal data?". The need to know how the criminals act it is essential to prevent it. This paper has six parts. Part One is the introduction of this where necessary information about the topic initiates. Part Two has some Literature Research on Eavesdropping, detailing how some countries have started to consider Eavesdropping as a challenge to IT Security Professionals and Privacy Policies.

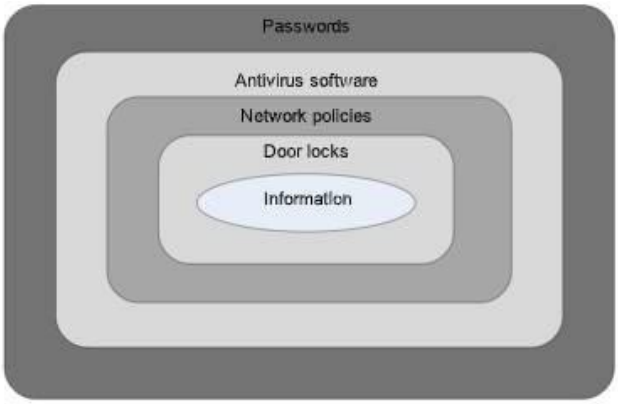

Figure 1. Protecting the Information.

part three concerns to the Methodology initially used here, taking into consideration Security Projects and Algorithm implementation. PartFour explains the current work and preliminary results on this initial project. It includes what has been happening up until now and the straightforward suggestions of what can be done to combat Eavesdropping on Mobiles. Chapter Five describes the initial work plans and more information on implications such as Legal, Professional, academic and Ethical Issues. Chapter Six is the conclusion of this Awareness Paper.

2. LITERATURE REVIEW

Eavesdropping has become a big business for criminals, and with mobile devices on the rise, it makes it be possibly the biggest target for criminals. O'Donnel[16] affirms that Mobile Security focuses on the device and application plus securing the Network itself in his article posted on TechTarget. Mobile Security is making sure all possible doors closed since it is the entrance to the safe hidden inside one of the lounges in the house. To protect with confidence, it is not easy. Even powering down devices, individuals' data from mobile devices is still vulnerable at any time. Spreading virus over victims' phones is one of the attacks on the rise. NSA Security professionals can commit security flaws in order to progress with crucial investigations [8], but criminals do it more often. Unglerlaider[23] has also made people aware that NSA can track phones and send drones after a mobile phone as they have the biggest Spy Centre in the world [1].

Nevertheless, not only the government can acquire our data, but eavesdropping software are becoming widely available and more popular each day [5]. One example is the software FlexiSpy which denotes excuse espionage advertising it as a way to protect children, monitor employees and catch cheating partner [11]. Also, depending on the country, this activity and software are entirely illegal. One example is for Brazilian citizens since 2013 when the legislation changed to make against the law any espionage on another individuals' device. That includes any electronic device, even if on the partner's [28]. The Italians have not come behind with this topic; they also have managed to take control of devices even if encrypted or moving very fast. Italians also do this using infection by installing the software on people's device or by individuals plugging their devices in infected machines. Even, Social Networks have been accused of surveillance to user's microphones on devices to listen to user's conversations and surroundings [21].

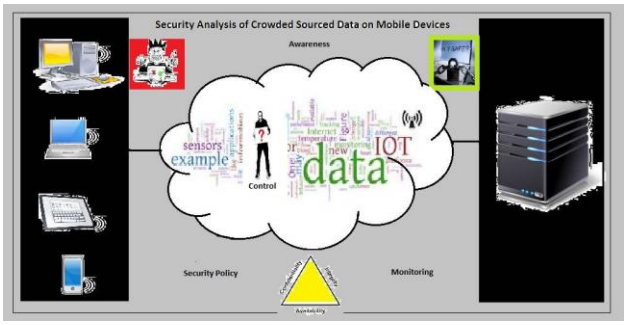

Figure 2. Data available accross multiple devices.

Watson [27] explains that this becomes all legal once it is in the user's privacy policies that every application needs to produce. It is substantial that people understand what those privacy policies allow devices to do. Information Security is to be at school for pupils and adolescents. It is demanding to understand how the Information Security World is vast. Banks have started to lose money due to fraud of cards and their websites also managed and accessed via smartphones. More investigations are happening daily. Hill [13] reinforces that the word eavesdropping is also for some applications. Applications are doing a lot with permissions when they get the accept touch. The user's privacy policy and such things are all there listed but ignored. The reading of the small letters, as usual, do not get through people's eyes. They want to get on with downloads and updates straight away. Another country that has already made some precautions to stop eavesdropping is Africa. They developed Seecrypt application, and guaranteed users can get around the NSA with their application [18].

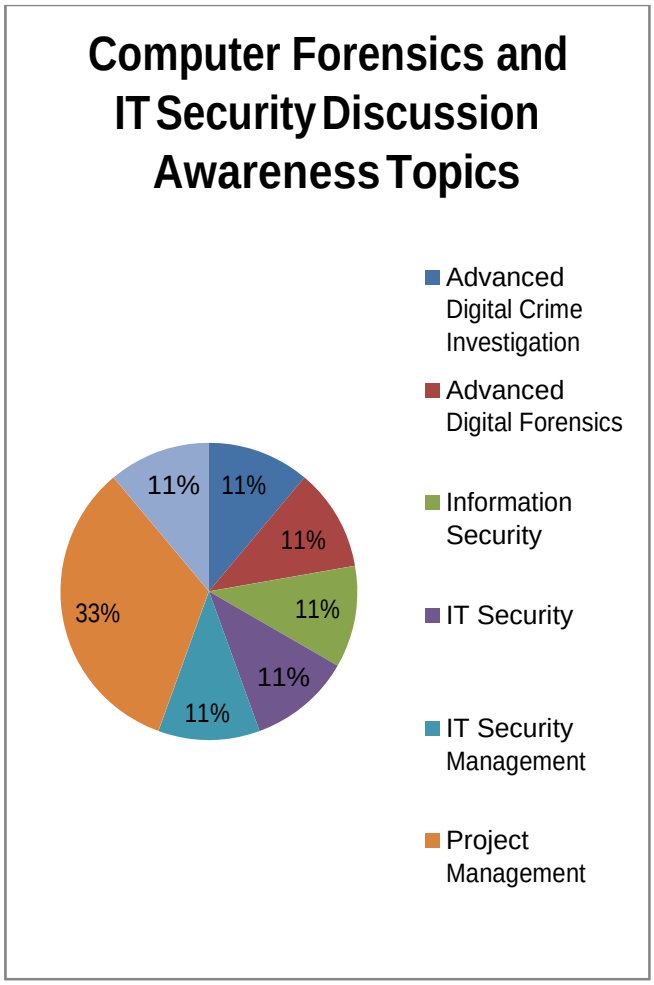

Figure 3. Professions on IT Security for men and women.

They must prove this concept daily as the news sometimes shows that this is just a today sentence. It appears unfeasible for anyone that is not an NSA member to prove this. Researches have claimed to have decoded the spy tools the government used to spy phones [26]. Of course, it could also be another spam and requires further analysis. Taylor [22] has mentioned the fact that cell phones are less secure than landlines. They are very vulnerable to eavesdropping. It has provided three main factors that would indicate eavesdropping such as battery not lasting, warmth between calls and occasional beeping noisy.

Again, it would be attractive to proof if this is always the case when eavesdropping.
Parker [17] ignores the fact that Mobile Devices are more accessible to eavesdropping as agents have been eavesdropping landlines for years. Nevertheless, Parker reminds individuals about securing devices with passwords and suggests a few encryption applications for mobile devices which do not impede more sophisticated criminals. Also, once a device is on WIFI, it can be intercepted by the Network Administrator so what is the solution to stop such interception? Remember, now everyone accesses free WIFI on the go!

2.1. Mobile Interception by Criminals

In 1996, Brookson[2] was already concerned with computer security and wrote a paper entitled Mobile Secure Telephony with the first few recommendations to protect the end-users. Schelegel et al.[20] started to investigate Smartphone eavesdropping back in 2011. It is only a matter of minutes for a malicious eavesdropping malware infect mobile devices while Chang [4] in the same year investigated how to make Smartphone surveillance a reality with SmartWatch.

2.1.1. Digital Criminals targeting Smartphones

Lu Yu Chan et al.[25]did severe research to detect eavesdropping when using Convert channel communication. Lai [15] highlighted how companies are eavesdropping customers Mobile Devices to persuade them to buy or subscribe to products. Canlar et al.[3] has acknowledged the fact that criminals are targeting smartphones more than desktops. She developed a new way of forensic analysing smartphones live as digital criminals are working on devices.

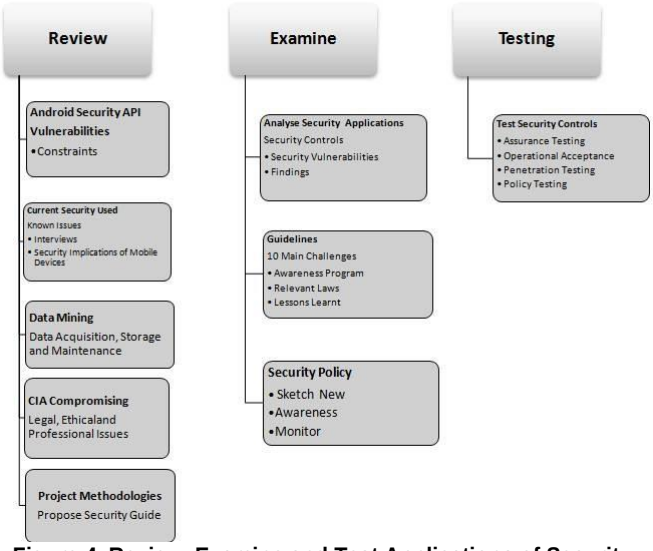

Figure 4. Review, Examine and Test Applications of Security.

2.1.2. The Identify and Prevent Research Initiative

Back in 2005, the weaknesses of wireless networks regarding signal leakage and other attacks initiated with Wireless Local Area networks [7]. To relate if there is any improvement in this sector is necessary to investigate the interceptors' attacks growth. They are committing more crimes. Michael Cobb [6] relates in his article, the facility that a third party has to listen on the back of iPhones, mainly via Bluetooth, but everything needs to be reviewed, examined and tested.

Figure 5. CIA Model on Mobile.

Elizabeth Smith [21] also wrote about eavesdropping mobile phones using Bluetooth and suggested that people should pair in private and make devices undiscoverable. Taking this to account, consider merging the approaches

Figure 5. CIA Model so crucial on the Security World.

that other researchers have started to protect the data. Instead of only detecting and investigate the crimes, relate weaknesses of the wireless medium band. It is essential to identify and prevent eavesdropping on mobile devices with applicable measures.

2.2. The Business of Stealing Personal Data

Some applications on the internet claim to have the power to spy on phones, even if no access to the device [19]. Many of these are even being offered free of charge. As informed computing users, the already known danger that some free software can imply needs to be accountable.

Investigate further such applications, finding out how they work in order to understand how to prevent scammers.

2.2.1. Stealing Personal Data

The government per instance has the capital to invest in this business, and the article by Ryan Gallagher [12] relates that the NSA has spent $1.3 million to upgrade their cell spy machines in 2009. Ryan also shows other hardware and technologies used for this finality together with prices that vary between about $18000 to $135000, not affordable for a part-time criminal. More economic criminals use radio scanners to spy Mobile Devices and steal data. They have been targeting Telecom, especially the ones with internet and email — E.G. healthcare databases, where data from thousands of individuals at once [14]. Eavesdropping mobiles have started to flourish as a crime at the beginning of the century with the evolution of mobile devices and internet usage compromising the Confidentiality, Integrity and Availablity (CIA) of the devices. Digital crimes, such as eavesdropping is on the rise. It cannot be expected to have a permanent solution to combat this practice and protect the individuals' privacy. Data is evolving, moving, the fight is a daily job. The University of St. Andrew's have suggested that Encryption Algorithms is the starting point to prevent these interceptions by criminals [24].Again, NSA can intercept even communications that are encrypted, and some researches have claimed to have decoded NSA algorithm. Therefore, if this is the case, the same technology used by NSA can also be available to criminals. The upper platform on top to secure the population data from frauds, between other several crimes lead to the stealing of the data by these means needs daily updates. More women and men must be educated to occupy such tasks.

2.2.2. Privacy Policy

Privacy Policy is a policy all websites and applications must have to let us know how they protect data obtained from devices, especially over the internet. It is part of the legislation, and it differs as per country. In Europe, the Commissions has a framework where it states that everyone has the right to have their data protected, and all companies dealing with data must adopt this framework [10].

Figure 6. Behind Mobile Devices.

Criminals exploit privacy when they invade a Mobile Device to steal data. On Mobile Devices, they do that by collecting data from SMS, MMS, WI-FI Networks, Bluetooth and GSM. All applications in the market available for download must guarantee the privacy and integrity of the users. However, some malicious software will infect devices by playing with the permissions of applications.

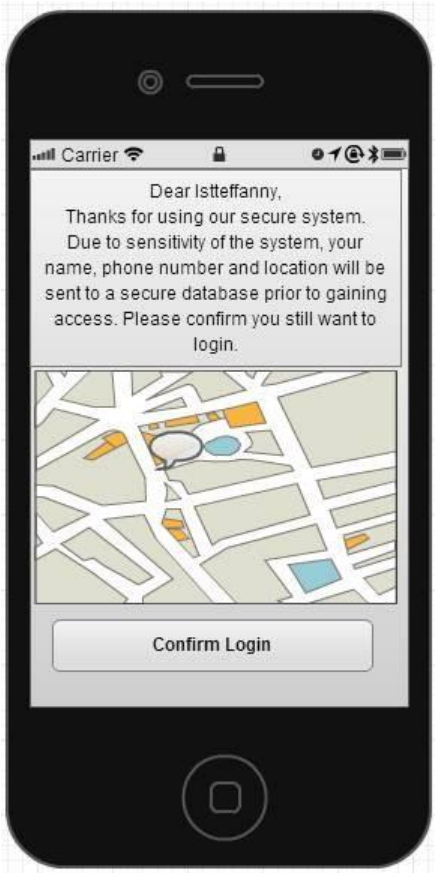

Figure 7. Privacy Policy on Mobile Devices.

It will then be able to interact, damage and possibly get monetary gains by exploiting the OS of the device. It efficiently gathers and views sensitive data [28]. Banking is one of the most sensitive and private data that criminals have their eyes shining. Reports of keyloggers, WIFI Virus and Touch Logs are increasing rapidly [9].

3.METHODOLOGY

To develop a way to combat eavesdropping using Steganography is an experimental studying attempting to broaden the knowledge on the subjects and product at least some data. There were practical experiments with private cell phones that gave details of how to identify this practice. After identifying eavesdropping on the device, the most effective way of preventing this interception is proven to be awareness, otherwise how to protect something not known? It is a Deductive Qualitative Approach aiming from extensive research to specific instances related to the matter. RUP/USDP is the notation for the developing of the application that born from this study. Free access to recent journal papers, security software to test ideologies and several different devices with different OSs is crucial to prove concepts. The developing measure works on Mobile

Devices in general and not just one type of Operating System. Not many researches have intentionally used Steganography to combat eavesdropping. Eavesdropping and Steganography need to marry well in order to apply on a Smartphone of different makes equally. Therefore, the Deductive Qualitative Approach is the best available approach to tackle this new solution. The Methodology to develop the "framework" does not necessarily need to be RUP/USDP. Depending on the solution, another methodology such as DSDM for more dynamic development. However, Javaderived languages for mobile devices like Android or J2me to build the software is highly recommended for anyone that decides to follow these ideas and implement another solution.

4.CURRENT WORK AND PRELIMINARY RESULTS

The goal is to combat mobile interception by criminals who use Eavesdropping to steal personal data by developing frameworks, mechanisms and algorithms. The main Research Question is "How to combat Eavesdropping Interception on Mobile Devices by Criminals Motivated on stealing Personal Data? Can Steganography benefit such an activity?"For accomplishing this goal: Literature Research focusing on the most recent papers and articles but noting down what has been considered in the past to overcome the criminality eavesdropping devices! The research question may seem to broaden at present, but all contribute to the knowledge of an individual, and it can avoid a crime. The security of our data is specific enough to affect everyone.
Criminals can eavesdrop in various ways. They are using different methodologies, either Bluetooth, WIFI, Hardware such as Antenna that captions Radio Signals. Infected applications can bypass encryption algorithms. Plus, masking the data on mobile devices using Steganography. However, can we use it Steganography to protect our mobile data instead? The answer is clearly, yes. It can be the approach to combat eavesdrop on mobile devices hence sensitive data stealing, proof of copyright and identity theft.

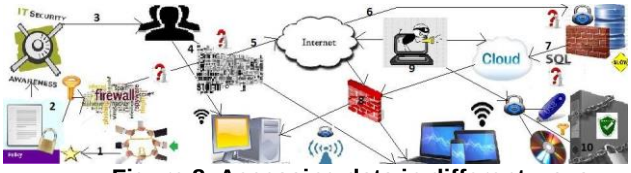

Figure 8. Accessing data in different ways.

Another point to make here is the fact that dealing with the investigation and gathering sensitive information from the general public was not allowed. No analysis of sensitive data from people not involved with this research was legal, nor people indirectly involved, and no readers are maliciously affected. The aim is to educate and protect instead of violating and break the rules. Methods discussed presents valuable awareness, hints, software and ideas to get more confident with Information security.

5.CONCLUSIONS

This journal demonstrates how important it is for research professionals to work on prevention of crimes related to Mobile Devices. Eavesdropping is the most challenging to identify without any background measures implemented by IT Security professionals. For this reason, it is feasible and beneficial for all inhabitants that use Mobile Devices together with sensitive data to be aware that the data needs to be protected carefully. People must read the small prints; otherwise, the stealth by criminals who will compromise the confidentiality and integrity of victims is only a matter of time. Different countries have different rules and are tackling prospective crimes in different ways, so citizen do not have their identity and capital stolen so often. Every individual must cooperate to have the private data protected at all times. It is a standard measure to prevent such criminal activity related to eavesdropping Mobile Devices. Sometimes, mobile devices have less attention than a computer when it comes to Information Security and viruses. However, they are more used than PCs. Child and Adolescents need to be well informed. Not just men, but women must draw more attention to computing and programming careers specialised and security and digital investigations. The future needs an earlier understanding of this technology. Everybody, including criminals, are using it. Protecting our data and sensitive information needs serious consideration. Women must be invited and welcome to participate and work in these discussions as they are particularly vulnerable to attacks. There is a way to protect the device capabilities of sharing leaking this information out when criminals eavesdrop, and we should find the solution to maintain intact the devices. Avoid eavesdropping by applying simple concepts of Steganography and hiding sensitive information away from predators. Efficiently covering sensitive information, read the privacy policy and customise it, providing an initial alternative to mobile defence for mobile security purposes with pure awareness.

References

[1] Bamford, J. (2012). The NSA Is Building the Country's Biggest Spy Center (Watch What You Say). Available: http://www.wired.com/2012/03/ff_nsadatacenter/. Last accessed 6th Oct 2019.

[2] Brookson, C. (1996). Mobile secure telephones. Information Management & Computer Security. 4, 7-10.

[3] Canlar, E. et al. (2013). Windows Mobile LiveSD Forensics. Journal of Network and Computer Applications. 36, 677-684.

[4] Chang, K. (2014). Integration with cloud and mobile technologies: The next step for the security and surveillance industry. Available: http://www.digitimes.com/supply_chain_window/story.asp

?datepublish=2014/06/27&pages=PR&seq=201. Last accessed 2nd Oct 2019.

[5] Chandramohan, M. et al. (2011). 1 Detection of Mobile Malware in the Wild. Available: https://www.academia.edu/1335332/PrePrint_Detection_of_Mobile_Malware_in_the_Wild. Last accessed 1st Oct 2019.

[6] Cobb, M. (2014). Preventing iPhone Spying and other Mobile Management Tips. Available: http://searchsecurity.techtarget.com/tip/How-to-prevent-iPhone-spying-mobile-phone-management-tips. Last accessed 1st Oct 2019.

[7] Curran, K., & Smyth, E. (2005). Exposing the Wired Equivalent Privacy Protocol Weaknesses in Wireless Networks. International Journal of Business Data Communications and Networking. 1, 59-83.

[8] Cushing, T. (2013). Even Powering Down A Cell Phone Cannot Keep The NSA From Tracking Its Location. Available: https://www.techdirt.com/articles/20130723/12395923907/even-powering-down-cell-phone-cant-keep-nsa-tracking-its-location.shtml. Last accessed 6th Oct 2019.

[9] Dujmovic, J. (2014). Little Known - Ways Hackers Take Over the Phone, Data and Money. Available: http://www.marketwatch.com/story/little-known-ways-hackers-take-over-your-phone-data-and-money-2014-08-22. Last accessed 5th Oct 2019.

[10] European Commission. (2014). Reform of Data Protection legislation. Available: http://ec.europa.eu/justice/data-protection/. Last accessed 3rd Oct 2019.

[11] Flexispy. (2014). Spy on Mobiles, Cell Phones and Tablets. Available: http://www.flexispy.com/en/spy-on-mobile-phone-to-reveal-secrets.htm. Last accessed 4th Oct 2019.

[12] Gallagher, R. (2013). Meet the machines that steal the phone's data. Available: http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/. Last accessed 4th Oct 2019.

[13] Hill, K. (2014). Facebook Wants to Listen in on what we are doing.Available: http://www.forbes.com/sites/kashmirhill/2014/05/22/facebook-wants-to-listen-in-on-what-youre-doing/. Last accessed 6th Oct 2019.

[14] Keating, G. (2005). Hackers Eavesdrop on Phone networks to Steal Data. Available: http://codeverge.com/grc.security/hackers-eavesdrop-on-phone-networks-to-steal-dat/1656920. Last accessed 6th Oct 2019.

[15] Lai, Y. (2013). Analysing strategies of mobile agents on malicious cloud platform with Agent-Based Computational Economic Approach. Expert Systems with Applications.40, 2615-2620.

[16] O'Donnel, J. (2014). Pulse Secure puts VPN, MAM in harmony for mobile security. Available: http://searchconsumerization.techtarget.com/news/2240232363/Pulse-Secure-puts-VPN-MAM-in-harmony-for-mobile-security?utm_medium=EM&asrc=EM_NLN_35086668&utm_campaign=20141010_Pulse+Secure+creates+harmo. Last accessed 1st Oct 2019.

[17] Parker, M. (2014). What Can You Do to Stop Eavesdropping on Cell Phones & Home Lines? Available: http://everydaylife.globalpost.com/can-stop-eavesdropping-cell-phones-home-lines-36881.html. Last accessed 06th Oct 2019.

[18] Patriot Update. (2013). App to Prevent Government Eavesdropping on Cell Phones. Available: http://patriotupdate.com/2013/06/app-to-prevent-government-eavesdropping-on-cell-phones/. Last accessed 2nd Oct 2019.

[19] Privacy Rights Clearinghouse. (2014). Wireless Communications: Voice and Data Privacy. Available: https://www.privacyrights.org/wireless-communications-voice-and-data-privacy. Last accessed 4th Oct 2019.

[20] Schlegel, R. et al. (2011). Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. Available: http://www.cs.indiana.edu/~kapadia/soundcomber-news.html. Last accessed 4th Oct 2019.

[21] Smith, E. (2014). How to stop Eavesdropping on Bluetooth. Available: http://classroom.synonym.com/stop-eavesdropping-bluetooth-10938.html. Last accessed 5th Oct 2019.

[22] Taylor, S. (2014). How to Stop Cell Phone Eavesdropping. Available: http://www.ehow.com/how_7657638_stop-cell-phone-eavesdropping.html. Last accessed 5th Oct 2019.

[23] Unglerlaider, N. (2013). What it is Like to Be ANsa Cyberspy. Available: http://www.fastcompany.com/3012913/the-code-war/what-its-like-to-be-a-nsa-cyberspy. Last accessed 4th Oct 2019.

[24] University of St. Andrews. (2008). What is Data Encryption. Available: https://www.st-andrews.ac.uk/ktc/techopportunities/spotlight/dataencrypt/. Last accessed 6th Oct 2019.

[25] Yu-Chan et al. (2013) Covert channel based eavesdropping malware analysis and detection for android

Systems. European Conference on Information Warfare and Security, ECCWS. 20132048-8602:304-312

[26] Zetter, K. (2014). Researches find and Decode the Spy Tools Government use to Hijack Phones. Available: http://www.wired.com/2014/06/remote-control-system-phone-surveillance/. Last accessed 6th Oct 2019.

[27] Watson, P. (2012). Smartphone Apps Now Use Microphone to Record Conversations. Available: http://www.infowars.com/smartphone-apps-now-use-microphone-to-record-your-conversations/. Last accessed 5th Oct 2019.

[28] Wikipedia. (2014). Mobile Security. Available: http://en.wikipedia.org/wiki/Mobile_security. Last accessed 4th Oct 2019.

AUTHORS

Istteffanny Isloure Araujoreceived the B.S.c and M.S.c degrees in Computer Science and Computer Forensics and IT Security from London Metropolitan University in 2013 and 2015, respectively. Now, she is in the Intelligent Systems and Research Centre of the School of Computing and Digital Media. Her subject area is Big Data, Digital Security, Copyright and Privacy using Steganography. She also is an Associate Lecturer in subjects like Databases, Fundamentals of Computing, Programming, Network and Cloud Security, Networks and Operating Systems, Game Development and Ethical Hacking.

Dr Hassan Kazemian received a B.Sc. in Engineering from Oxford Brookes University, UK in 1985. He received an M.Sc. in Control Systems Engineering from the University of East London, UK in 1987. He followed with a PhD in Learning Fuzzy Controllers from Queen Mary University of London, UK, in 1998. He is currently a professor at London Metropolitan University. He worked for Ravensbourne College University Sector, UK, as a senior lecturer for eight years. Previous lecturing experience includes the University of East London, UK, University of Northampton, UK, and Newham College, UK. Research interests include AI and ML applications to cybersecurity. Prof. Kazemian is a Fellow of the Institution of Engineering and Technology FIET (formerly IEE) UK, Chartered Engineer (C.Eng.) UK, and Fellow of British Computing Society (BCS) UK.