International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Smartphone as an Agent of Anti-forensics: A Case of Workplace Environment in Kenya

Kevin Omolo[a]*, Dr. Elisha Abade[b]

[a,b]*The University of Nairobi, School of Computing and Informatics, P.O. Box 30197, Nairobi, GPO, Kenya*

[a]*Email: kvnonyango@gmail.com,* [b]*Email: eabade@uonbi.ac.ke*

Abstract

Computer anti-forensic techniques work to ensure that forensic evidence left behind after a digital crime is not easily uncovered by forensic investigators, if they are to uncover them, there will be a considerable delay. Smartphones have become a common device within an organization's workforce where employees interact with highly confidential data that they access using their laptop computers at the workplace. This has led to the use of smartphones to commit digital crimes at the workplace. The primary objective of this study is to find out whether the use of smartphones at workplace environment in Kenya may be exploited to advance activities that may derail forensic investigations in the event of a digital crime. We also set to establish data security risks within organization and other techniques and/or methods by which smartphones may be used to exfiltrate data. Finally, we shall analyze research areas that require further attention from researchers to enhance defense and guard against smartphones data exfiltration. To achieve these objectives, we shall implement and test an android mobile software prototype, developed using android studio to send data exfiltration attempt to a web-based user interface when an employee within an organization uploads data above a set authorized limit. We shall review existing literature to understand other techniques that may be used to exfiltrate data from organizations as well as analyze research areas that require further attention from researchers to enhance defense and guard against data exfiltration through smartphones usage. We collected a total of two thousand five hundred and eighty-four records of data exfiltration attempts from our eleven sampled population. Of these records, One thousand eight hundred and ninety-one happened in the evening hours while six hundred and seven in the afternoon hours, then finally, eighty-six records were registered in the morning hours. In conclusion, the research study, has revealed that there exist challenges in reporting smartphone-based data exfiltration attempts while using the mobile-based software prototype. Data exfiltration attempts was observed to happen within organization's workplace, with evening hours being the most affected by this vice with a figure of over one thousand data exfiltration attempts. We also noted that there exists, at least three categories of data security risks that organizations are exposed to when employees have their smartphones within the workplace. We recorded an additional eleven other techniques and methods by which a smartphone may be used to steal data from an organization.

---

* Corresponding author.

Keywords: Cryptography; anti-forensics; naive anti-forensics; smartphone; Data Exfiltration.

1. Introduction

The effects of compromising security include violation of intellectual rights or forging of authenticity. These acts call for the deployment of forensic methodologies and tools to reconstruct what happened to digital content to answer questions such as who has done what, when and where. Computer anti-forensic techniques, on the other hand, works in the reverse to ensure that this is not easily arrived at. Of interest to this study, is the research done by [1] who talked of the anti-forensic technique as the act of hiding evidence. Reference [2] reported in their survey, that the act of hiding evidence has troubled forensic examiners as it purposes to ruin an examiner's work by ensuring that examiners do not easily reach evidence while doing their searches to establish illegality. In the same study, Reference [2] also talked of deliberate attempts to eliminate or neutralize evidentiary sources. To minimize footprint of illegality, References [3,4], have affirmed in their studies that perpetrators have retorted to the use of bootable USB drive, compact disk and virtual machines. All these techniques have only one major goal, hide the evidence so that the forensic investigator does not easily get to it during an investigation. References [5,6] defined Anti-forensics as a method undertaken to thwart the digital investigation process conducted by forensic investigators. References [3,7] both cited [8] definition of anti-forensics by taking a more traditional crime scene perspective and branding it simply as an attempt to negatively affect the existence, amount and/or quality of evidence from a crime scene or make the analysis and examination of evidence difficult or impossible to conduct. Reference [9] summed up the definition of anti-forensics as a way of ensuring that forensic investigators cannot establish the occurrence of a digital crime. However, if they do find out the occurrence of a digital crime, make it impossible to prove that it did take place.
In conducting our research study, we set out to answer the following research questions (RQs) to enable us to achieve our set objectives. The research questions are as follows:

RQ1: What are the data security risks that an organization is exposed to when its employees have their smartphones within their work area?

RQ2: What is the countermeasure for reporting smartphone data exfiltration by an employee within the organization?

RQ3: What are the various techniques or methods by which a smartphone may be used to steal data from an organization by an employee?

RQ4: What are the challenges in reporting smartphone data exfiltration?

As our primary objective was to establish whether the use of smartphones at workplace environment in Kenya may be exploited to advance activities that may derail forensic investigations in the event of a digital crime, we shall remain focused on addressing the fact that while employees are aware of the benefits they enjoy by bringing their smartphones into the workplace, managers too are aware of the benefits of having a constantly connected workforce [10]. This though may be overridden by the danger that some dishonest employees may expose their organization to, hence the need to ensure that smartphones are not used to commit digital crimes.

To answer the research questions, we shall begin our study by looking at related works to help us answer RQ1 and RQ3 in section 2 to justify our key contributions. Sections 3 shall outline the methodology followed while conducting this study. Section 4 shall look at the results found after the implementation of the mobile-based software prototype and shall answer RQ2. Section 5 shall give a detailed discussion of the results as we strive to answer RQ4.

2. Related Works

2.1. Definition of Anti-forensics

References [5,6] defined Anti-forensics as a method undertaken to thwart the digital investigation process conducted by forensic investigators. References [3,7] both cited [8] definition of anti-forensics by taking a more traditional crime scene perspective and branding it simply as an attempt to negatively affect the existence, amount and/or quality of evidence from a crime scene or make the analysis and examination of evidence difficult or impossible to conduct [9] summed up the definition of anti-forensics as a way of ensuring that forensic investigators cannot establish the occurrence of a digital crime, however, if they do find out the occurrence of a digital crime, make it impossible to prove that it did take place.

2.2. Primary Goals of anti-forensics

References [20, 4] cited [22] presentation on the primary goals of anti-forensics as:

- Avoiding detection that event has taken place.
- Disrupting the collection of information.
- Increasing the time that an examiner needs to spend on a case.
- Casting doubt on a forensic report or testimony [22,23].
- References [23,24] using anti forensics tools that exposes the existence of a forensic tool.
- Reference [24] Sabotaging the use of the forensic tool, for example by using the forensic tool itself to attack the organization in which it is running).
- Reference [24] Executing a direct physical attack on the forensic examiner for example, by bombing the building in which the examiner is working at or implementing tools to disconnect the examiner's tools as they work.
- References [23,24] Ensuring that the usage of anti-forensic tools is stealth and cannot be traced, once the offence is committed.

2.3. Types of Anti-forensic Techniques

References [7,25] categorizes anti-forensics into four groups, namely:

- Data hiding [25],
- Artifact wiping [25],
- Reference [25],Trail obfuscation, and

- Attacks against forensics processes or tools, which refer to attacks that force the forensic analyst to perform non-standard procedures or call into question the data recovered [25,1] distinguished several kinds of anti-forensic techniques, that is,

- Destroying evidence (making it unusable during the investigation),
- Hiding evidence (subverting an analyst by decreasing the visibility of the evidence),
- Eliminating sources (neutralization of the evidentiary sources) and
- Counterfeiting evidence (creation of a fake version of the evidence which is properly made to carry wrong or deviated information to divert the forensic process [26].

2.4. Data Hiding using Cryptography

References [27,29] published an article on Forensic Focus stating that Full-disk encryption may be employed as an anti-forensic technique by criminals who want to hide their data from investigators. References [27,28] affirms that when a long and complex password is used to encrypt a volume, a brute-force attack may still not be effective as the process to decrypt may take a long time for the forensic investigators to break hence giving the suspect enough time to delay forensic investigation thereby achieving its goal of delaying the investigation. Reference [27] gives the following workarounds for full-disk encryption:

- The possibility of obtaining the binary decryption key out of the memory dump, from the live running system before turning it off and taking the disk out [29].
- The possibility of getting a hold of an escrow key [29].

Reference [27] gives TrueCrypt and PGP as the examples of full-disk encryption tools that are secure and are designed to resist brute-force attacks. Reference [30] reported the use of a software application called Wickr, by parties who intend to be unfaithful to either their partners or their party leaders. According to their article, Wickr may be used by governments or companies to hide digital traces using 256-bit, Advanced Encryption Standard (AES) symmetric encryption and Rivest–Shamir–Adleman (RSA) 4096 encryption and works without relying on their PGP key and the end to end encryption [31]. They note that Wickr elevates the challenge faced by mobile forensics investigators as it would take them considerable time and effort to break, thereby allowing anti-forensics perpetrators to achieve their goal of delaying investigations.

2.5. RQ1. Data security risks resulting from the use of smartphones within an organization

- The threat of virus and malware

Reference [10] reports that malware exists to target employee's smartphones. This is further made worse by a much lower rate at which people install antivirus software on their phones . They [10] report that 97% of mobile malware is Android based. In our research study, which used android based smartphones and noted that the sampled population were always visiting android's app store to download application which was free in nature. Some of the applications are published with backdoor access that allow their command and control servers to

steal data resident on employee's smartphone. References [12,13] cites a report by Ponemon Institute of 2016, that, the average cost of a corporate data breach is $21,155 per day. In the light of this revelation, future research should concentrate on ensuring that the trust that users have put on the applications they download from app store is not tainted, maybe, by recommending a framework that would ensure systemic vetting of all applications published onto app store before they can publish, instead of the current free-for-all approach to app store publishing of application.

- The threat of lost or stolen mobile smartphones

Mobile smartphones have become part and parcel of employees, Reference [10] reports that smartphones are intertwined with the employee's working day and that average employee is likely to check work emails on their smartphone, downloads attachments containing client data and may also use a file sync/share solution on their smartphone to access work files remotely. Therefore, losing these smartphones means high risks to organizational data resident on them. He [10] goes on to report that a lost or stolen phone can be a treasure trove of easily accessible information if it falls into the wrong hands, so enabling these basic security features is essential. Reference [10] advises that all employees should enforce basic security features e.g. use of passcodes on their smartphones because they use them for a work-related purpose, even if that's just checking emails.

- Location-based Threats

Unknown to many, all smartphones have a way to identify their current location. In our research study, we enabled location feature of the smartphone to determine whether an employee is within the work environment, though used in this case for a noble cause, the location feature of a mobile smartphone may be used to track the movement of an employee with an intent to undertake terrorist activities within an organization or even its neighbors. Some users within our population sample never considered that leaving the location feature enabled could be a danger to their life or even to their organization. Reference [14] reports on the danger of geotagging, that is, a feature left by default on most smartphones and may be used through cell phone triangulation and GPS to get the exact location of an employee. This information may be used by criminals to plan an assault on an employee or may also use an employee's absence from home or work to advance criminal damage or theft.

2.6. RQ3

Techniques or mediums by which data may be exfiltrated from a smartphone [15] defines data exfiltration as the retrieval and transfer of data from an organization's laptop assigned to an employee via the unmonitored internet connectivity availed through activation of mobile data and mobile hotspot features to an external storage of an employee's choice without the organization's authorization.

2.7. This section answers RQ3

The motivation for this question was to gain an understanding of the various techniques or methods and mediums by which a smartphone may be used for data exfiltration within an organization. In our review, we found that organization's data in use or at rest, may be exfiltrated after a digital crime via the following ways

according to [15]:

- Use of existing smartphone mediums to exfiltrate data

Reference [15] confirms in his review that messages, HTTP, Bluetooth, NFC, Wifi direct, USB Connections, speaker, phone calls and infra-red emitter as mediums that exists in all smartphones and that they may be used to exfiltrate from an organization's data store, whether at rest or in use.

- Use of adversary models to exfiltrate data from a smartphone

Reference [15], presented mobile data exfiltration technique (MDET), which they used demonstrate how sensitive data may be obtained from Android devices in a covert manner using communication mediums found on almost all mobile devices. As a case study, they created two proof-of-concept application which used SMS and audio to exfiltrate data. Other adversary models mentioned by [15] in the same paper includes the work of [16]

2.8. Research Gap

Having reviewed articles and appreciated their contributions towards the field of anti-forensics. We have seen the various techniques that criminals may exploit to advance digital crimes. The researcher notes that all the reviewed papers have made major contributions to the various means and methods that digital crimes have taken. While contributing to this, the reviewed papers, have failed to consider the danger that smartphones pose to forensic investigators with the increasing technological advancement on their storage ability, whether internal or external, ability to stream internet connectivity at 4G speeds. This danger is even increased by the frenzy of Bring Your Own Device (BYOD) that is gaining ground in most organizations especially in the developing nation, Kenya being among them.

2.2. Conceptual Architecture of Smartphone Monitoring Solution (SmartWatch)

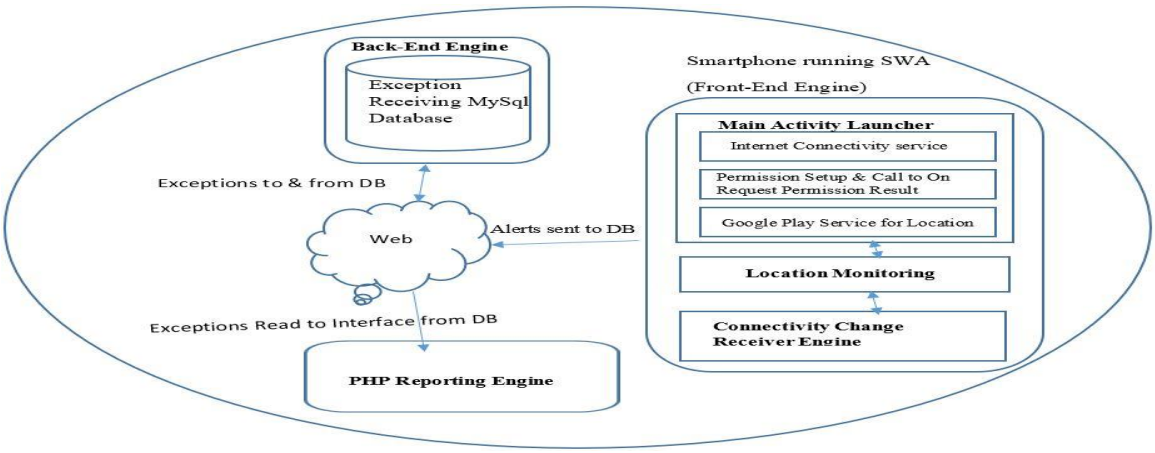

Figure 4

3. Research Methodology

3.1. Research Design

We shall review existing literature as outlined in section 2, to understand techniques that may be used to exfiltrate data from organizations as well as analyze research areas that require further attention from researchers to enhance defense and guard against data exfiltration through smartphones usage. Through this, we should be able to establish data security risks within organization and other techniques and/or methods by which smartphones may be used to exfiltrate data to answer RQ1, RQ3 and RQ4, this enabled us to analyze research areas that require further attention from researchers to enhance defense and guard against smartphones data exfiltration. RQ2 shall be answered by the researcher implementing and testing an android based mobile software prototype, developed using android studio. This application prototype is intended to send data exfiltration attempt to a web-based user interface when an employee within an organization uploads data above a set authorized limit

3.2. Target Population and Sampling Frame

The target population for our research shall be the IT/Management Information Systems (MIS), Human Resources and Finance departments. These departments have been chosen due to the sensitive nature of organizational information that they interact with on day-to-day basis and who are most likely to be involved with digital related crimes and/or deliberate cover-up of crimes that are likely to take place within an organization. Since the target population is finite, the following formula according to [17,18] is used to determine the sample size:

Where:

S = Required Sample size [18]

X = Z value (e.g. 1.96 for 95% confidence level) [18]

N = Population Size [18]

P = Population proportion (expressed as decimal) (assumed to be 0.5 (50%) [18]

D = Degree of accuracy (5%), expressed as a proportion (.05); It is margin of error [18]

4. Results and Discussion

4.1. To bring our study into focus, we shall show the results of RQ2 as follows:

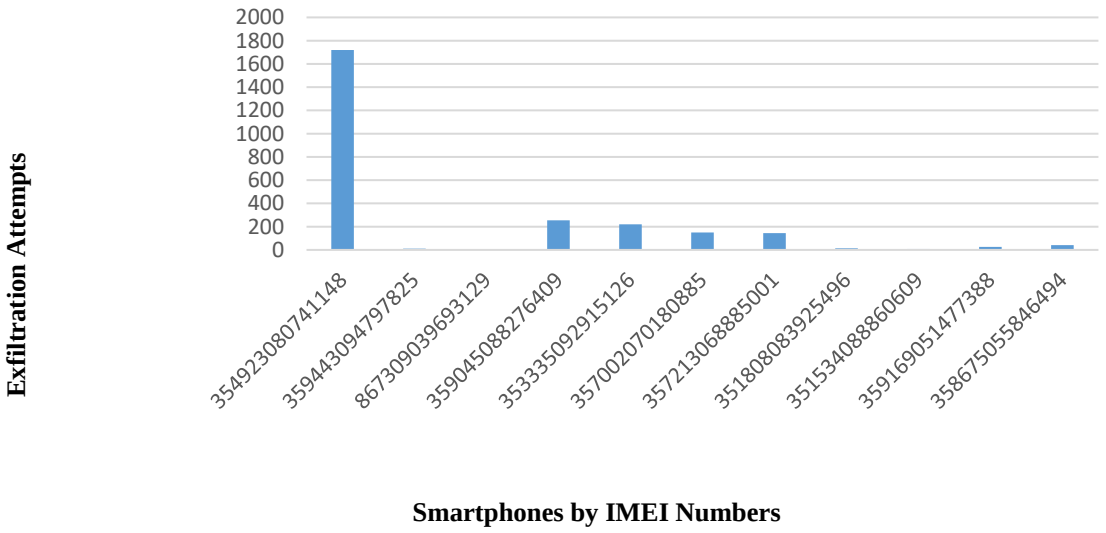

Figure 1: Bar Graph Showing Data Exfiltration Attempts by Total Sampled Population

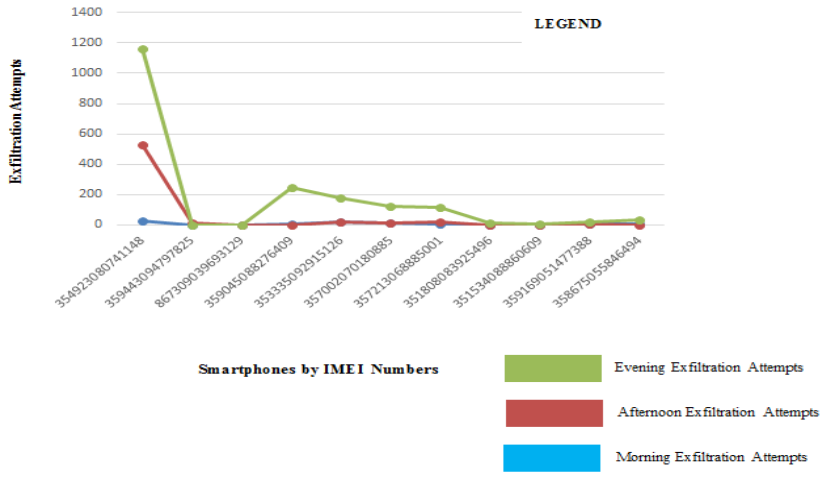

Figure 2: Line Graph Showing Data Exfiltration Attempts by Time of the Day

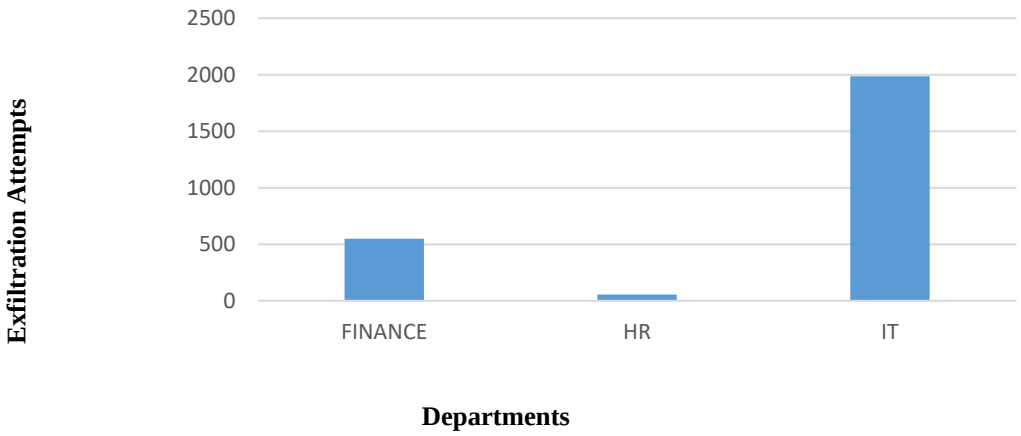

Figure 3: Bar Graph Showing Exfiltration Attempt by Department

4.2. Discussion of the Results

4.2.1. Fig. 1. Showing Data Exfiltration Attempts by Total Sampled Population

This figure affirms that there is general trend in the sampled population that reveals that data exfiltration with employees while on duty is evidently present. The trend shows figures within a similar range of value except for users with smartphone IMEI number ending with 41148, 93129, and 60609 whose values recorded would be considered as outliers. On interrogation of the reason behind the recorded values, it was confirmed that user of the smartphone number 41148, was IT officer who was actively involved in testing of the smartwatch application. The smartphone user number 93129 who had recorded two exfiltration attempts was confirmed to have taken leave off duty, therefore, the smartphone was out of radius limit of 50 meters, hence out of workplace,, which confirms the ability of the smartwatch application to only be able to send exfiltration attempts when the employee is within the radius of work environment

4.2.2. Fig. 2. Showing Data Exfiltration Attempts by Time of the Day

Figure 4-2 recorded some interesting and unexpected outcome. This is because values of exfiltration attempts revealed that majority of users switched on their mobile data on their smartphones in the evening and this trend continued with a steady rise during the entire period of the study. Evening exfiltration attempts recorded a total value of one thousand eight hundred and forty-one, followed closely by the afternoon hours which also showed very high and consistent values of data exfiltration. It is therefore fair to affirm that the more employees get worked up in the course of the day, the easier it is for them to get involved with illegal activities. The trend gives clear indication when the security officers should put more emphasis when looking at organizational data exfiltration attempts.

4.2.3. Fig. 3. Showing Exfiltration Attempt by Department

Figure 4-3 affirmed our earlier position at the beginning of the study where we had anticipated that data exfiltration attempts would more prevalent with the IT and finance departments. It confirmed that the employees in the IT department are highly likely to be involved with exfiltration attempts. This trend of high data exfiltration attempts was followed closely by the finance department. The organization has a reason to worry as these are the same departments that they have trusted with sensitive data. IT department's accessibility to confidential data of the organization and at the same time being the department that assigns access rights to other users including management staff worsens the situation and elevates the risk factor. This is because they are likely to give themselves rights that would favor data exfiltration without being noticed. It is therefore important that the exfiltration limits be set by a staff that is not within the IT department.

4.3. RQ4. Challenges and Future Research Direction in reporting smartphone data exfiltration with a focus to anti-forens

4.4. ics*Privacy*

The fact that smartwatch application must be installed on the employee's smartphone to monitor and report anomalies he/she may be doing is an ought right violation of users' privacy. Reference [19] acknowledges in

their presentation that, countermeasures are in most cases installed by enterprises to defend themselves against data exfiltration. According to [19] , directly monitoring the outgoing network traffic generated by employees and scan it for detecting sensitive information, such approaches lead to a mistrust between users' and their corresponding enterprises. Future explorations should look at the balance between privacy and the need to safely ensure that organizational data, either at rest or in use at the hands of employees, do not fall into the hands of dishonest employees.

4.4.1. Accuracy

While testing our prototype application, we noted that the addition of uploaded traffic was using inbuilt program defaults whose accuracy could not be scientifically verified in this research study, however, smartwatch is a prototype, we were not able to verify this with Google and therefore hope that future research may get full acceptance from Google to fully access and understand the basis of data constants we are using to retrieve the streaming values.

4.4.2. Automation

Smartwatch fully relies on the human administrator to capture the exception posted on the monitoring browser for its effectiveness. That is, without the administrator monitoring the posted alerts, the intended objective may not be realized. Future research should encourage smartphone manufacturers to sponsor or partner with University research students so that the projects/thesis that they present at the end of their studies are real-life solutions solving complete problems rather than leaving stated problems hanging for future implementation that may not see the light of the day.

4.4.3. Performance

We noted that the routine within the application that cumulatively sums up the data upload activities must run continuously via a handler on the background during the entire period a mobile data connection has been activated until such a time when an employee commences an upload activity which again shall have to attain a set thresh hold before the routine can terminate. Future research should address this anomaly through exploration on various application optimization measures that shall ensure that smartphone battery is conserved by any application running within the smartphone.

4.4.4. High Cost

Reference [19] affirms in his presentation, that cost is one of the main deal breakers for the organization especially when new technology is introduced or being considered. They [19] lament that cost is the primary concerns both for individuals and enterprises while deciding upon the incorporation of a system, tool, or technology in their infrastructure. In this research study, we consent to the same fact that we spent a considerable amount of money to facilitate license for hosting our administrator's website, and even human cost invested in the development of the smartwatch application prototype.

4.5. Limitation of the study

4.5.1.

Reference [15] reports that an ideal data exfiltration application countermeasure would be one that would not require explicit permission's acknowledgement to operate. In addition to the permission that are set on AndroidMenifest.xml, smartwatch also requires additional permission to be acknowledged by the installing user just before the first launch. Future research should explore ways by researchers may find an easy partnership with smartphone manufacturers so that their research ideas are given chances to achieve their intended objectives.

4.5.2.

The inability of the smartwatch application prototype to able to automatically disconnect an employee suspected of using mobile data for exfiltration. This is a limitation that is, introduced by Android Operating System as a way of protecting the privacy of the end users from hackers. Android did not, however, consider the good intentions of cybersecurity professionals who would be interested in using this feature to protect organizational data. Future research direction should explore the possibility of Google allowing privileged or licensed access to protected areas of the operating system to advance research in the field of smartphone security.

4.5.3. Human Biasness

Human biasness in setting up the surfing threshold or data limit is not based on any scientific formulae or research study. According to [19] Human biasness is also evident on the inclusion or exclusion of papers in literature reviews as well as the general references during this research study. Several research journals might have missed our eyes or touch, maybe because of inadequate searching ability due to lack of proper tools or experience, to get exhaustive journals in the field of smartphone data exfiltration.

4.5.4. Cost

Reference [19] asserts that cost is among the primary concerns both for individuals and enterprises while deciding upon the incorporation of a system, tool, or technology. In this research study, the cost was a major decider on what tool we subscribed to while looking for a site to host our administrative interface including the database. Cost also dictated our ability to engage google to license us to get full access to the mobile data activation and deactivation engine or module as this would require larger corporations with enough financial muscle.

5. Conclusions and Recommendation

In conclusion, the research study, has confirmed that there exist challenges in reporting smartphone-based data exfiltration attempts while using the mobile-based software prototype. Data exfiltration attempts was observed to happen within organization's workplace, with evening hours being the most affected by this vice with a figure

of over one thousand data exfiltration attempts. We also noted that there exists, at least three categories of data security risks that organizations are exposed to when employees have their smartphones within the workplace. We recorded an additional eleven other techniques and methods by which a smartphone may be used to steal data from an organization. We assert that RQ1 and RQ3 were answered during literature review, section 2. We answered RQ2 by developing smartwatch, which was a software prototype. RQ4 was reported in outcome combining our review of the literature and observation of the results during the study. The results of the study confirmed the objectives of this study and we found out that in average, an employee will activate his mobile data feature at least thrice or four times in a day averagely, even though, the organizations provide them with free internet resource. Based on this revelation, we recommend that organizations should put a lot of emphasis on the need deploy technology that shall automate suspicious data exfiltration activities within the work environment. This could be made possible by pushing to commercialization through possible partnership or sponsorship of the smartwatch to full-fledge commercial application. It may as well call for the execution of further research areas recommended in this study.

References

[1] A. Distefano, G. Me and F. Pace, "Android anti-forensics through a local paradigm", Digital Investigation, vol. 7, pp. S83-S94, 2010. Available: 10.1016/j.diin.2010.05.011 [Accessed 20 July 2019].

[2] N. Macek, P. Strbac, D. Coko, I. Franc, And M. Bogdanoski. Android forensic and anti-forensic techniques – a survey. In: the eighth international conference on business information security. Belgrade, Serbia, 2016.

[3] K. Conlan, I. Baggili and F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy", Digital Investigation, vol. 18, pp. S66-S75, 2016.

[4] S. Garfinkel, "Anti-Forensics: Techniques, Detection and Countermeasures", Citeseerx.ist.psu.edu, 2006. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.5063&rep=rep1&type=pdf. [Accessed: 21- Jul- 2019].

[5] S. Azadegan, W. Yu, H. Liu, M. Sistani and S. Acharya, "Novel Anti-forensics Approaches for Smart Phones", 2012 45th Hawaii International Conference on System Sciences, 2012.

[6] Dmu.ac.uk. (n.d.). De Montfort University - Leicester, UK. [online] Available at: https://www.dmu.ac.uk.

[7] Gary C. K. Anti-forensics and the digital investigator. In C. Valli & A. Woodward (Ed.), Proceedings of the 5th Australian Digital Forensics Conference. Mt. Lawley, Western Australia: Edith Cowan University, 2007

[8] M. Rogers. Panel session at CERIAS 2006 Information Security Symposium. Retrieved September 11, 2007, from http://www.cerias.purdue.edu/symposium/2006/materials/pdfs/antiforensics.pdf

[9] S. Berinato (2017). The Rise of Anti-Forensics. [online] CSO Online. Available at: http://www.csoonline.com/article/2122329/investigations-forensics/the-rise-of-anti-forensics.html

[10] Netstar.co.uk. Your Employees' Smartphones Are a Major Risk to Security of Data. 2018

[11] S. Allam, S. Flowerday and E. Flowerday, "Smartphone information security awareness: A victim of

operational pressures", Computers & Security, vol. 42, pp. 56-65, 2014.

[12] J. Raphael, "7 mobile security threats you should take seriously in 2019", CSO Online, 2019. [Online]. Available:https://www.csoonline.com/article/3241727/mobile-security/5-mobile-security-threats-you-should-take-seriously-in-2018.html.

[13] CSO Online. (n.d.). CSO. [online] Available at: https://www.csoonline.com/.

[14] MakeUseOf. 4 Smartphone Security Risks To Be Aware Of. [online] Available at: https://www.makeuseof.com/tag/4-smartphone-security-risks-to-be-aware-of/ [Accessed 5 Nov. 2018], 2018

[15] Q. Do, B. Martini and K. Choo, "Exfiltrating data from Android devices", Computers & Security, vol. 48, pp. 74-91, 2015.

[16] Zhou, X, Demetriou, S, He, D, Naveed, M, Pan, X, Wang, X, Gunter, CA & Nahrstedt, K 2013, 'Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources', Proceedings of the 20th Conference on Computer and Communications Security, ACM, pp. 1017-1028.

[17] R. Krejcie and D. Morgan, "Determining Sample Size for Research Activities", Educational and Psychological Measurement, vol. 30, no. 3, pp. 607-610, 1970.

[18] Kenpro.org. (n.d.). Kenya Projects Organization [KENPRO] | Project Management, Research and Publishing. [online] Available at: http://www.kenpro.org/.

[19] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. Babar and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures", Journal of Network and Computer Applications, vol. 101, pp. 18-54, 2018.

[20] A. Joshi, and D. Bhilare, "Emerging trends and research in digital forensics", Oiirj.org, 2014. [Online]. Available: http://www.oiirj.org/oiirj/jan-feb2014/33.pdf.

[21] Ljmu.ac.uk. (n.d.). Postgraduate students. [online] Available at: https://www.ljmu.ac.uk/study/postgraduate-students.

[22] V. Liu and F. Brown, "Bleeding-Edge Anti-Forensics", Infosec World Conference & Expo, MIS Training Institute, 2006. [Accessed 22 July 2019].

[23] S. Isaiah Moses, "Measuring the Robustness of Forensic Tools' Ability to Detect Data Hiding Techniques", BYU ScholarsArchive, All Theses andDissertations. 6464, vol. 6464, 2017. [Accessed 22 July 2019].

[24] Calhoun.nps.edu. (2014). Calhoun Home. [online] Available at: https://calhoun.nps.edu/.

[25] Gla.ac.uk.(n.d). University of Glasgow - Postgraduate study. [online] Available at: https://www.gla.ac.uk/postgraduate

[26] Goniv.com. (n.d.). Welcome to goniv PUBLICATION. [online] Available at: http://www.goniv.com/.

[27] O. Afonin, D. Nikolaev and Y. Gubanov, "Countering Anti-Forensic Efforts – Part 2", Forensic Focus - Articles, 2015. [Online]. Available: https://articles.forensicfocus.com/2015/09/15/countering-anti-forensic-efforts-part-2/.

[28] "Colorado Technical University", Coloradotech.edu. [Online]. Available: https://www.coloradotech.edu/.

[29] "Forensic Magazine", Forensic Magazine. [Online]. Available: https://www.forensicmag.com.

[30] M. Al-Hadadi and A. AlShidhani, "Smartphone Forensics Analysis: A Case Study", International Journal of Computer and Electrical Engineering, vol. 56, , pp. 576-580, 2013. Available: 10.7763/ijcee.2013.v5.776.

[31] "IJCEE", Ijcee.org, 2008. [Online]. Available: http://www.ijcee.org/.

[32] A. Bangert, "Using Experimental Research to Investigate Students' Satisfaction with Online Learning", Student Satisfaction and Learning Outcomes in E-Learning, pp. 130-148, 2011.

[33] Champlain.edu. (n.d.). Champlain College | Degree Programs | Colleges in Vermont. [online] Available at: https://www.champlain.edu/