WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Model for Trojan Horses Detection in Android Smartphones

Woira Jeremiah Byansi[1]*, Muwanga Kosea Erasto [2], Onyango Laban Oliver Owin [2]

[1,2] School of Science and Technology, Bugema University, PO box 6529, Kampala, Uganda

* E-mail: lonyango@bugemauniv.ac.ug

DOI : https://doi.org/10.55248/gengpi.5.0724.1808

ABSTRACT

Mobile devices have become the order of the day in this era with increasingly powerful computing, networking and sensing capabilities and at the same time are target by attackers and malware because of the numerous services they offer like e-mail exchange, mobile transactions, surfing the internet, storage of personal and organisational important information. In the year 2017 Uganda lost close to shs. 151 billion to cyber criminals and research by Patrick in 2018 revealed that close to 90% of organisation in Uganda operate below cyber security standards. The aim of this research was to develop a Trojan horse detection model in android smartphones to prevent attack by cyber criminals. Honeypot was developed to mimic the behaviour of information and this would attract the malware and safe guards the information and therefore it's important to safe guard these mobile devices since they have become part and parcel of human life. It's highly recommended that the mobile or application developers should incorporate this application within the device. This research employed exploratory design which came up with a model as the end product because it was able to answer research questions such as what, how and why and finally heuristic data analysis was used to analyse the output of the test results.

1. INTRODUCTION

Mobile devices have emerged as popular appliances with increasingly powerful computing, networking and sensing capabilities. With the current technological advances, mobile devices such as smartphones, tablets and netbooks have developed the world and maintained their commercial value to an acceptable level for all social classes (Gelembe et al., 2013). Mobile payment for utility bills is the most used e-Government service (62.6%), followed by online registration for the Tax Identification Number (TIN). E-payments are now main (Kitogo, 2018) stream, as 62.1% of individuals have sent or transferred money within Uganda using an electronic method, most likely a mobile phone-to-mobile phone transfer involving mobile money (Rogers, 2016). A new report from Serianu, a pan African cyber security consulting and training firm, revealed that Uganda lost close to Shs151 billion ($42m) to cyber criminals in 2017 alone (Patrick, 2018).

The Uganda Cyber Security Report also revealed that 90% of Ugandan organizations operate below the cyber security poverty line and this needs a huge investment in monitoring, detection and prevention tools. (Patrick, 2018). Mobile malware and vulnerabilities made headlines well over 2015, and attacks became more common way for cybercriminals to steal sensitive data. (Rogers, 2016). The pace at which malware evolved on mobile devices is alarming, adding that with banking Trojans generating revenues in the millions, and ad-click fraud and crypto mining apps flooding online stores, McAfee researchers expected to see considerably more exploitation of mobile devices in 2018. As global cybercrime was estimated to cost $600bn in 2018, the preferred choice of access for most of the world's population is a mobile device, said the report, suggesting that 2018 may be the year of mobile malware (Rogers, 2016).

Karanja (2017) states that mobile banking security threats have become a major concern to the financial service providers and their clients where corporations manage a workforce armed with multiple mobile devices these devices alone increase the number of vectors open to cyber-attacks and make corporate information more exposed than any other time in corporate history. In 2015 whatsApp introduced a web version that replicates the experience of the mobile app on a PC which brought with it new security threats. Check Point, a cyber-security firm, discovered that hackers could use WhatsApp web to distribute malware such as ramson ware, Bots and remote access tools (RATs) that give hackers remote access to victims PCs (Muncaster, 2018). According to the (Report, 2017), Nokia issued its report which revealed a new all-time high in mobile device malware infections, a sharp increase in compromised smartphones and major IoT device security vulnerabilities

2. PROBLEM STATEMENT

Smartphones are targeted by malware because of the wide range of services they offer such as Emails exchange, mobile transactions, internet surfing, taking pictures, keeping important data, user location and social networking with the help of applications Collett, (2017), however, Mobile Trojans such as banking Trojans are one of the most dangerous species in the malware world (Kaspersky, 2016). They steal money from mobile users' bank

accounts, putting mobile users into heavy losses, stealing of personal and confidential information, and denied access to files, degrade mobile functions, deleting or stealing of personal data, disabling the device completely, embarrassing service providers and inconveniencing users (Lovi& Bansal, 2014).

A report from Serianu, revealed that Uganda lost close to Shs151billion ($42m) to cyber criminals in 2017 alone Patrick, (2018) and 90% of Ugandan organizations operate below the cyber security poverty line and this needs a huge investment in monitoring, detection and prevention tools. (Patrick, 2018).

3. OBJECTIVE

The objective was to develop a Trojan horse detection model in android smartphones to prevent the attack.

4. LITERATURE REVIEW

Mobile Device Malware Detection Techniques

Two malware approaches were proposed for the analysis and detection of malware (Burguera et al 2011). Arash et al (2017) proposed a technique to enable mobile network operators to detect android malware and violations of user privacy through network analysis. First blacklisting was done, since majority of malicious applications use DNS in order to find the IP address of the remote server. After getting the remote server the malicious application send the information obtained about the IP address. With the help of string matching they traced out what user information is being sent to the remote server. Their main focus was on the HTTP based conversations.

Aubrey-Derrick et al, (2009) proposed a method in which first static analysis is done to extract function calls using the command readelf, after that they applied Prism and Nearest Neighbour algorithm (PART) for the classification purpose. There are many tools which automate the process of detection like Taintdroid (Enck& William, 2014). Taintdroid is a tool which tracks the flow of privacy sensitive data through the applications. If there is any leakage then it logs the details in order to identify the app which is leaking the information. Asaf et al, (2010), describes another tool called Crowdroid which performs behaviour-based malware detection system.

Mobile Honeypot system

According to Mathias (2012), a honeypot is a trap for collecting data from unauthorized system access and learns about the nature and the characteristics of attacks. It is used for a probe that either resides on a mobile device and running on a mobile operating system or operated in the network of mobile devices. (Matthias, 2012). However Mathias et al (2013) defined the term mobile honeypot as a honeypot that focuses on mobile device attacks, honeypots can either be mobile themselves in running on the mobile device in this case they are usually low interaction honeypots used for deception and detection of known attacks.

Trapping Trojan Horses Using a Honeypot

In contrast to other security measures such as firewalls that ultimately try to keep the attacker out of the system, honeypots are designed and meant to be compromised. Their value lies in luring the attacker into entering a system and collecting information on how this is done. Mathias et al (2013) showed that honeypots are typically classified as low interaction or high interaction honeypot and client or server honeypot. A low interaction honeypot primarily collects information about the attacker and detects known attacks. The limited level of interaction between attacker and target is achieved by not providing fully functional services but only emulations thereof with known exploits.

On the other hand, a high interaction honeypot provides a fully functional system. They are used to reveal current and new attacks that do not have to be catered for when setting up the honeypot. Since the high-interaction honeypot is a fully functional system, it has to be closely monitored for successful attacks to prevent the attacker from using the honeypot to target other systems on the network (Mathias et al 2013).

The Researcher' primary goal was to design a model that detects Trojan horse malicious activities in mobile devices.

5. RESEARCH METHODOLOGY

The research was exploratory in nature because it suggested a model to solve a practical problem and also helped to answer all types of research questions such as what, how and why. A heuristic approach was then taken in order to find a solution to the problem when the classical methods were too slow. Heuristic data analysis methods were used to analyze data from the honeypot which data was used to understand attack patterns and make informed decisions on how to secure the android devices.

6. FINDINGS AND RESULTS

Based on objective the research reviewed the android architecture and various android based honeypots and their respective models, analysed existing documents, analysed other existing models that formed the sources of requirements that was used to develop the model. Honeyspotlabsac was one of the android honeypot frameworks that were reviewed to come up with the new model. This application runs on the Android operating system at the

application level and to emulate telnet, SMS, and http services. As a result, a log file of all interactions and accesses is generated, however it does not emulate other services like SSH, FTP and does not provide the mobile phone user alerts to assess the vulnerabilities and threats.

Honeyd honeypot creates virtual hosts on a network and this host can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems this specific honeypot enables a single host to claim multiple addresses.

Barrera &Oorschot (2011) analyzed popular platforms of mobile devices from 2010 such as: Android, BlackBerry, iPhone and Symbian, and presented a classification of installing third party software on smartphones, using three generic models: Walled Garden Model, Guardian Model and End-user Control Model.

Table 1: Shows comparison of different honeypots and their characteristics

Characteristics	**Honeydroid**	**HoneyM**	**Honeyd**	**HoneypotLabsac**
Framework	NO	YES	YES	YES
Application level	NO	NO	NO	YES
Operating system level	NO	NO	YES	NO
Kernel level	YES	NO	NO	NO
Hardware Virtualisation	YES	NO	NO	NO
Low Interactive	NO	YES	YES	YES
High Interactive	YES	NO	NO	NO
Android Operating system	YES	NO	NO	YES
Other operating systems	NO	YES	YES	NO
Mobile Operating system	YES	YES	NO	YES

Characteristics	**Honeydroid**	**HoneyM**	**HoneyD**	**HoneypotLabsac**
Framework	NO	YES	YES	YES
Application Level	NO	NO	NO	YES
Operating System Level	NO	NO	YES	NO
Kernel Level	YES	NO	NO	NO
Hardware Virtualisation	YES	NO	NO	NO
Low Interactive	NO	YES	YES	YES
High Interactive	YES	NO	NO	NO
Android Operating System	YES	NO	NO	YES
Other operating systems	NO	YES	YES	NO
Mobile operating system	YES	YES	NO	YES

Network model

Undirected graphs was used to show the movement of devices on the network and how the honeypot would detect Trojan horses in the mobile devices. For all mobile network nodes, there is a graph G (V, E), where V is the set of nodes with in the network and E is a set of edges in the mobile network.

Further where V= $\{v_1, v_2, v_3, v_4 - - - - - - - - v_n\}$ and

$$E= \{(v_1, v_2), (v_2, v_3) - - - - - - - - - (v_n, v_{n+1})\}$$

The nodes in the graph V= $\{v_1, v_2, v_3, v_4 - - - - - - - - v_n\}$ are susceptible to attacks by various hacker nodes as they move from one point to another. In the set of nodes v, there is a node $v_h \epsilon V$ called the hacker node that lies amongst the other communication nodes. Such that $(v_h, v_i) \epsilon V$ is an insecure connection. Therefore to secure this node v_i, there is a node v_H called the honeypot that is used to attract the attacker v_h, to make him think he is

attacking the real node v_i yet this is a trap to luring him, data logs from node V_H are stored in the node application database and later threat and audit reports are made. The user node v_i uses this data to further secure the network and make informed decisions.

Therefore $(v_i, v_H) \epsilon V$ and $(v_H, v_{i+1}) \epsilon V$ is a secure route because of the node $v_H$that prevents Node v_i and v_{i+1} from being attacked by Node v_h.

But (v_h, v_H) is an insecure connection.

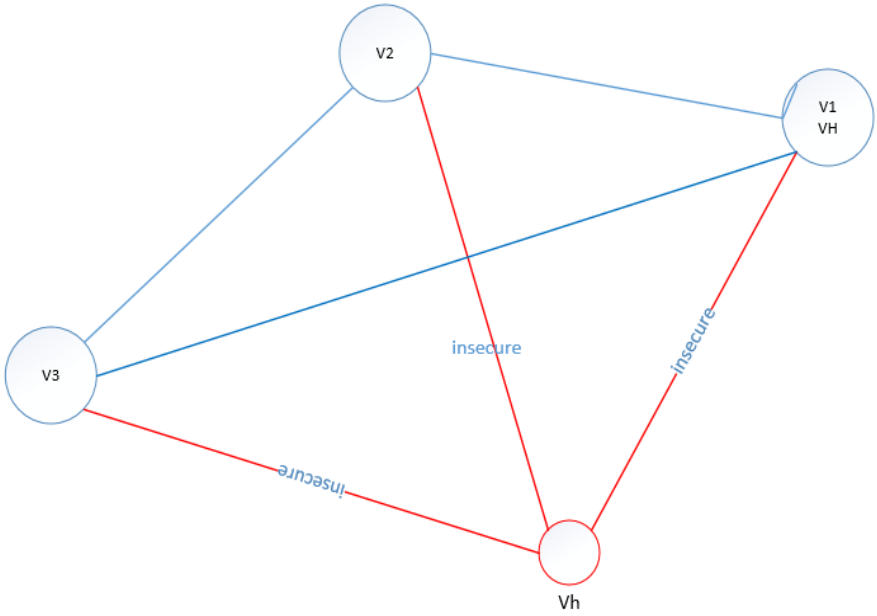

Figure 1: shows movements of nodes on a network

To further secure v_i, a firewall node v_f is put between the nodes. (v_H , v_i)

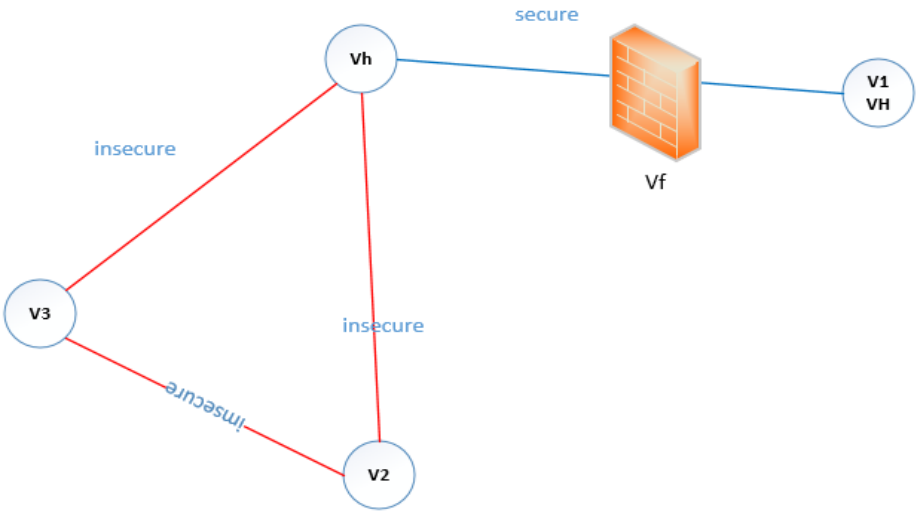

Figure 2: shows how to secure the moving nodes using a firewall

Architecture of the Model

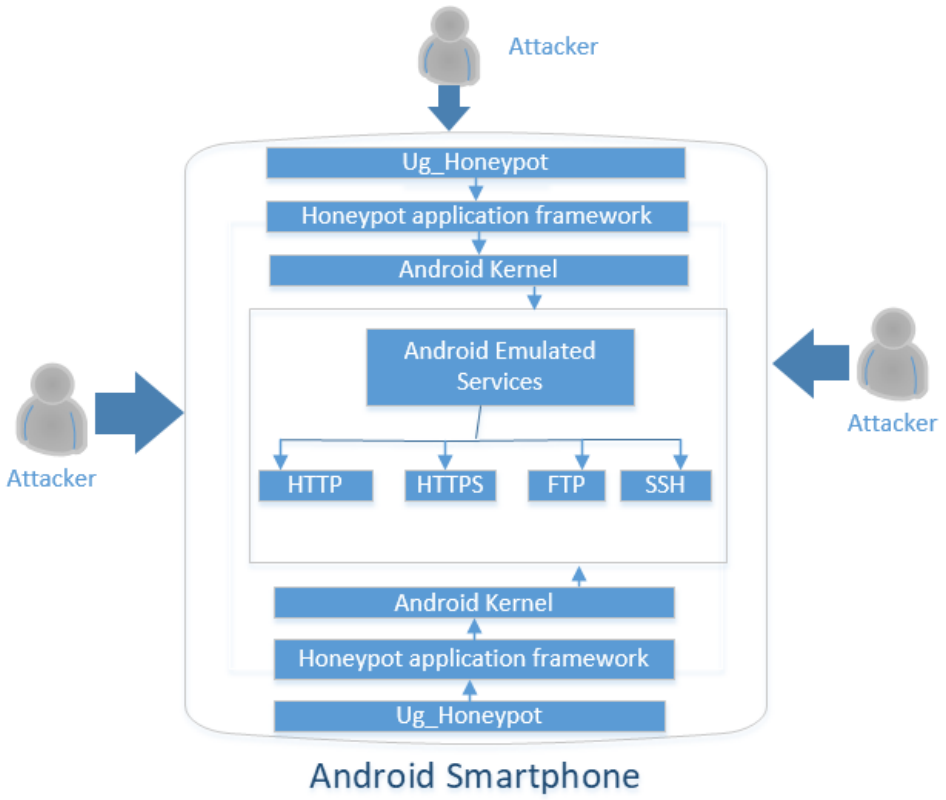

Figure 3: Architectural design of the honeypot model

The honeypot architecture presents a high level view of the system with the main components of the system and how the emulated services communicate. This honeypot architecture consisted of components such as Honeypot, Honeypot application framework, Attacker and android kernel. The attacker is first attracted by the honeypot and any interactions with the emulated services. Data logs are captured by the honeypot. The services and the honeypot are started by the user through a GUI. Therefore through this GUI honeypot configurations are made.

Logical design

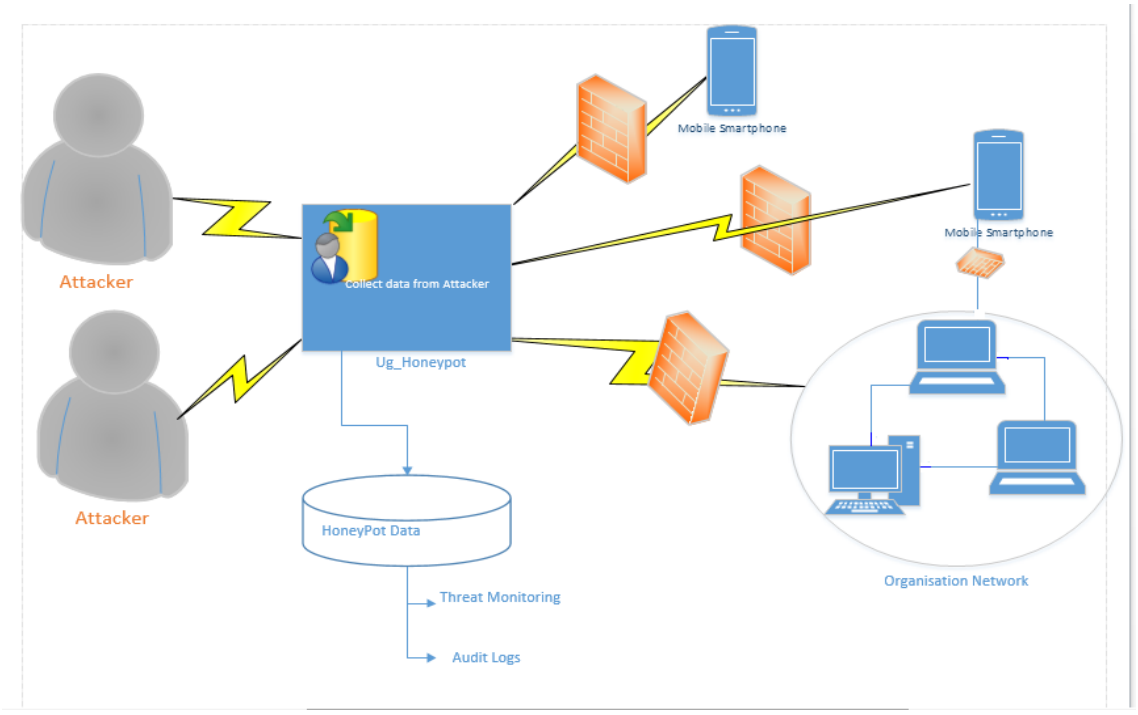

Figure 4: Logical design of the model

A low interaction honeypot was designed to run on the smartphone itself as an application at the application layer to emulate services such as HTTP, FTP, HTTPS and SSH, as a result a data log file of all activity interactions was generated and stored in the honeypot database, this honeypot attract the attacker making him think he is attacking the real smartphone yet it is just a trap to catch his actions on the network. All the data logs of the attacker are stored in the honeypot database where the user can retrieve reports, do threat monitoring and Audit attacker logs, to further secure these smartphone networks, a firewall was put in the network to stop the attacker from getting to other big networks where the smartphone is connected.

7. CONCLUSION

Mobile devices have become order of the day in people's way of life and therefore needs to be protected against external attacks since most of personal information that is private is stored in these devices, detection of Trojan horses in mobile devices (smartphones) is a must. An android honeypot that ran at the application layer was designed and emulates services such as HTTP, HTTPS, SSH and FTP which is captured and stored by the honeypot for analysis hence preventing such attacks.

Recommendations

Though the current set objectives of detection of Trojan horses in mobile devices (Smartphones) were achieved, more functionality and recommendations were suggested to make the model more productive and further understand how Trojan horses compromise systems, halt attacks and also trace where they originate.and further improve the honeypot as per the following recommendations;

- To develop the IOS and windows smartphone honeypot versions since the existing honeypot only covers android smartphones.
- To develop a honeypot that simulates other services that are not covered by the existing honeypot.

REFERENCES

Arash H. L., Andi F. A. K., Hugo G., FonMbah K, &Ghorbani, A. A., (2017). Towards a Network-Based Framework for Android Malware Detection and Characterization, 15th Annual Conference on Privacy, Security and Trust, (pp. 233 -242).

Asaf S., Uri K. & Yuval E., (2010). Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method. J. Syst. Softw., issue 83: (pp1524–1537).

Aubrey-Derrick S., Jan H. C., Ahmet C., &Sahin A., (2009). Detecting symbianos malware through static function call analysis. In 4th International Conference on Malicious and Unwanted Software, (pp 15–22).

Aubrey-Derrick, S., Ahmet, C., and Sahin, A., (2010) Static smartphone malware detection. In proceedings of the 5th Security Research Conference (Future Security 2010), ISBN: 978-3-8396-0159-4, (pp. 146)

Barrera, d. &Oorschot, V. P. (2011) "Secure Software Installation On Smartphones". Security Privacy, IEEE, vol. 9, issue 3, (p. 42 –48).

Burguera, I., Zurutuza, U., &Nadjm-Tehrani, S., (2014). Crowdroid: Behaviour-Based Malware Detection System for Android, DOI: 10.1145/2046614.2046619

Cerbo, F., Girardello, A., Florian, M., & Svetlana, V., (2011) Detection of malicious applications on android os. In Proceedings of the 4th international conference on Computational forensics, IWCF'10, (pp. 138-149).

Enck, W., Peter, G., Byung-Gon, C., Landon, P., Jaeyeon, J., McDaniel, P., Anmol, N., (2010). TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones, DOI: 10.1145/2494522

Gelenbe, E., Garcia, D., Tzovaras, D., Baitatu, M.,(2013). Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem. NEMESYS. DOI: 10.1007/978-3-319-01604-7_36 ·

Karanja, J. N. (2017). Investigation into the risk facing Mobile Banking.

kaspersky lab (2016, October 14) mobile banking Trojans explained.

Kitogo, E. J. (Tuesday, March 6, 2018). Ministry of ICT and National Guidance and NITA-U release findings of National IT Survey 2017/2018.

(MALWARE'2010), Nancy, France, France, 2010.Collett, S. (2017, august 1). Home :Information Security. Retrieved febuary 18, 2018, from csoonline website: https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html

Matthias, W., Vorbach, A., Christian, K., Schonfelder, J., Schmidt, T., & Jochen, S., (2013). Design,Implementation,and Operation of a Mobile Honeypot. doi.org/10.48550/arXiv.1301.7257

Matthias, W., Sebastian, T., Christian, K., Jochen, S., (2012). First Insights from a Mobile Honeypot. DOI: 10.1145/2377677.2377743

Muncaster, P. (2018). Mobile Malware Infections Hit 16 Million in Q3.

Patrick Max Ocaido (2018) Uganda Loses Shs150bn to Cyber Criminals - New Report

Report, N. t. (2017, march 27). Home:News:Releases. Retrieved january 23, 2018, from Nokia.com: https://www.nokia.com/en_int/news/releases/2017/03/27/nokia-malware-report-reveals-new-all-time-high-in-mobile-device-infections-and-major-iot-device-security-vulnerabilities

Rogers, R. (2016, October 6). Cybercrime: The Importance of Mobile Threat Defense.