ISSN 2277-3061

A Survey on SmartPhone Honeypot

Dr.Hanaa Mohsin Ahmed, Dr. Nidaa Flaih Hassan, Phd Student Assmaa A. Fahad
Computer Science Department, University of Technology, Baghdad, Iraq
salmanhanna2007@yahoo.com
Computer Science Department, University of Technology, Baghdad, Iraq
nidaaalalousi_5 @yahoo.com
Computer Science Department, University of Technology, Baghdad, Iraq
assmaa_fahad@yahoo.com

ABSTRACT

Smartphones are becoming a dominant form of mobile computing in the world. The Smartphone, as a platform, blends a traditional general computing platform with a specialized mobile phone platform. The general computing tradition is historically open, allowing its owners to install whatever software they choose and to add or remove hardware as they please. Also they are a vault for large amount of personal information about banking, social network, and inter-personal communication. These capabilities and information value make it an attractive target to internet miscreants.

This paper presents a survey on recent researches in Smartphone honeypot. Physical and virtual honeypots have been studied in details; however, there is only little work in the field of mobile related honeypot. The survey presents the challenges while setting up a smartphone honeypot, and summarizes the researches published in this area. We clarify the methods used to build their honeypot, and the results they obtained and their recommendations.

Keywords

SmartPhone; Honeypot;Physical and virtual honeypots ;Types; Evaluation

Council for Innovative Research

Peer Review Research Publishing System

Journal: International Journal of Computers & Technology

Vol 11, No.4

editor@cirworld.com

www.cirworld.com, member.cirworld.com

ISSN 2277-3061

INTRODUCTION

The primary goal of computer security is to defend computers against attacks launched by malicious users. There are a number of ways in which researchers and developers can work to protect the software that they write. Some are proactive, like code reviews and regression testing, while others are reactive, like the pwn2own contest where new vulnerabilities are used to exploit browsers. Some tools can take on aspects of both; one class of these tools is honeypot.

A honeypot is a computer which has been configured to some extent to seem normal to an attacker, but actually logs and observes what the attacker does. Thanks to these modifications, accurate information about various types of attacks can be recorded. The term honeypot was first presented by Lance Spitzner in 1999 in a paper titled To Build a Honeypot [1].

Honeypot as a term inspired by actual real-life honeypots. Since such represents a pot contains something desirable (the honey) to someone (a child or a nest of ants, for example), it could be used to lure them out and then observe them. The same is true for a computer honeypot: a tempting target is presented to an attacker, who then comes out and performs his attacks.

Honeypots are deliberately designed to be attack targets, mainly to learn about cyber-attacks and attacker behavior. When implemented as part of a security posture, honeypots also protect real networks by acting as a decoy, deliberately confusing potential attackers as to the real data.

Honeypots have been created in many different flavors. From single computer to whole networks of fake machines, called honeynets.

Types of Honeypots

There are several possible ways to classify honeypots. Some of the more popular are by the level of interaction available to the attacker, the type of data collected, and the type of system configuration [2, 3].

Level of interaction is the common type of classification; it is based on the level of interaction which is provided to the malicious user by the honeypot. The more interactive an environment presented, the closer the honeypot becomes to the actual targets of attack, and then potentially more accurate information can be gathered.

There are two levels: high-interaction and low-interaction.

1. High-interaction honeypots let the hacker interact with the system as they would any regular operating system, with the goal of capturing the maximum amount of information on the attacker's techniques. Any command or application an end-user would expect to be installed is available and generally, there is little to no restriction placed on what the hacker can do once he/she comprises the system.
2. Low-interaction honeypots present the hacker emulated services with a limited subset of the functionality they would expect from a server, with the intent of detecting sources of unauthorized activity [4]. For example, the HTTP service on a low-interaction honeypot would only support the commands needed to identify that a known exploit is being attempted systems.

Mobile Honeypot

To cope with the recent changes in the Internet, such as the advent of new popular applications, wide adoption of wireless network devices, introduction of high-speed subscriber link technologies to every household, diversity in users' demography in terms of culture and legal systems, and smart phones becoming as powerful as laptops and desktops, new types of honeypots have been proposed and introduced.

The term mobile honeypot can be used to describe prefixes of dark net address space that change a periodically, moving the dark net in the address space [5]. Here it is referring to honeypot that focus on attacks on mobile devices.

Multiple challenges while setting up a smart phone honeypot [6], they can be summarized as:

1. System Setup: How to build an actually smart phone honeypot system. From real devices to development emulators and maybe complete simulation. This largely depends on the OS we want to run as a honeypot and on the communication types we want to support. Compared to regular computers we have additional hardware and software capabilities that need to be present or simulated.
2. Monitoring: Monitoring the honeypot is one of the essential parts. The honeypot is only useful if we can exactly determine what the attacker is doing. Depending on the system setup monitoring can be highly complicated.
3. Containment: After compromise of the honeypot we need to make sure that the attacker cannot use the honeypot for carrying out attacks.
4. Visibility: To make the honeypot useful it needs to be visible for attackers. This can happen in many ways such as publishing the phone number, email address, instant messaging account name and a like in as many ways a possible. The honeypot then needs to inspect message content and such to e.g. open links contained in them in order to get infected.
5.

EVOLUTION OF MOBILE HONEYPOT:

There is only little work related to mobile honeypot [7], this is due to the limited hardware resources of the mobile devices and their software vulnerabilities.

The fundamental limitation in the Smartphone platform security is discusses by Husted et al.[8], they discusses the conflicting traditions between the cellular, which is restricted and very tightly controlled, and the general computing tradition, which is historically open; allowing its owner, i.e., users and administrators, to install whatever software they choose, and to add or remove hardware as they please. These two competing ideals clash on the Smartphone platform and this is exemplified by Android operating system platform created by Google. Following are several attempts in designing a mobile honeypots and the drawback in each design.

Freeman et al. (December 2009) discusses an experimental method for creating a 1st generation Smartphone honeypot, Smartpot, with the intention of discovering automated worms. They use Honeyd low-interaction virtual honeypot to discovering automated Smartphone worms by emulating the operating system Windows Mobile 5 and Windows Mobile 6, along with the available TCP/UDP ports of each operating system. A significant obstacle was discovered during the implementation of the Honeyd Smartphone honeypot, but designing a honeypot to specifically discover knowledge of the existence of automated worms is a possible concept. And the methodology of discovering available ports on actual Windows Mobile 5 and Windows Mobile 6 Smartphone devices using Nmap network scanner and then emulating those ports in a Honeyd honeypot seems viable [9].

Mulliner et al. (May 2011) propose HoneyDroid Smartphone honeypot using real mobile phone hardware rather than using the Android emulator. This honeypot designed to catch attacks originating from the Internet, mobile network as well as through malicious applications.

With HoneyDroid all relevant devices are virtualized, so Andrioid s not allowed to access hardware directly. This will put all of Android's hardware interaction under control, which can then be monitored and containment, which are not provided when using emulator approach.

The most drawbacks are that HoneyDroid does not behave exactly the same way the original Android system does. This might be detected by malware, which could then stop its attack and thus escape the honeypot [6].

Wahlisch et al. (August 2012) Design a low interaction server honeypot based on the standard tools Honeytrap and Dionaea in order to get statistical analysis of attacks.

The honeypot used to present a comparative study that analyzes to what extent those attacks depend on the network access.

They build the subsequent analysis of monitoring attacks on a Linux-based system that is connected to a mobile operator network. Their findings indicate that a few topological domains of the Internet have started to place particular focus on attacking mobile networks. A mobile device on average suffers from the same amount of attacks as a home network device [10].

Wahlisch et al. (August 2012) present a digital immune system, SKIMS, for Smartphone. This framework tries to protect the mobile device on its own. In cases insufficient, cooperation between neighbors is established.

The SKIMS system consists of multiple components that used to proactive and reactive defense of attacks; one of these components is a low interaction mobile honeypot. This honeypot is designed to collect malicious connection, it emulate (FTP, POP3, etc.) network services [11].

Yubo et al. (November 2012) propose a honeypot monitoring system for mobile communication by applying the idea of active honeypot combined with communication protection. They simulate the wireless access environment and capture the mobile phones, as well as analyze and monitor their communication behaviors. And they test the feasibility and efficiency of the system by testing an Android smart phone infected with a malware that can embezzle the phone’s address book.

They conclude that most ant viruses' solutions have big drawbacks [12]:

1. Antivirus software on the mobile terminal based on hardware devices, leading to:
    a. poor versatility
    b. large resource utilization
    c. Low virus capture rate.
2. Core network establishment suffers from difficult layout and high cost.
3. Solution based on base station is limited by the low flexibility and poor portability.

With honeypot monitoring system all these difficulties are overcome.

The most obvious defect in their honeypot is the limited supporting range of communication behavior. Some virus samples require Internet connection, but their honeypot cannot support GPRS, so many viruses can’t work

Wahlisch et al. (January 2013) Design a measurement system that capture traffic characteristics of malicious behavior on mobile devices and allows for comparison with non-mobile environments. The designed honeypot operate on standard PC

running Linux and connected to a mobile network this enables the analysis of malicious traffic across different network environments and bears the advantage of simplified long-term maintenance as the same tool basis can be re-used. Three sub honeypots are used to implement the designed honeypot, Kippo, Glastopf, and Dionaea. They deployed their honeypot on probes connected to a mobile network, as well as monitoring nodes connected to different types of wired Internet access and they did not find a relevant ratio of remote attacks that specifically target on the mobile system, neither from non-mobile nor mobile networks. And they conclude that mobile devices are currently more threatened with malicious applications (e.g., Trojan horse) compared to external, unsolicited requests via the Internet [7].

Liebergetd et al. (May 2013) Discusses that recently, attacks against smartphones have shifted towards local communication interfaces, which make the traditional honeypot concepts unsuitable. They propose a novel concept called nomadic honeypot that provides an infrastructure to enable mobile network operators to collect threat intelligence on smartphones. The nomadic honeypot requires that the smartphone is logically divided into two isolated partitions. The main partition hosts the mobile OS, but has no direct access to the device's communication hardware. The second partition hosts the infrastructure for our nomadic honeypot.

They implement their nomadic honeypot to run on the Galaxy S2 smartphone. And they choose Android as the mobile OS because of his openness characteristics, which can be virtualized on nonvirtualizable CPUs. The implementation proved to be very difficult because all drivers need to be modified to be interposed.

The nomadic honeypot has inherent usability drawbacks: It has some computational overhead, which means the devices will not be as fast as they could be and that the battery will not last as long [13].

Gelenbe et al.(July 2013) Design NEMESYS honeypot to collect and analyze information about the nature of cyber-attacks targeting the mobile devices and the core network so that the counter-measures can be taken. They identify a number of open with respect to the general problem of cyber threats against smartphone, and accordingly they design NEMESYS project.

They develop a data collecting, virtualization and analysis infrastructure, and the introduction of novel attack attribution and visual analytics technologies for the mining, presentation and representation of large amounts of heterogeneous data that are related to the smart mobile ecosystem in order to address these open issues [14].

CONCLUSION

This paper summarizes a survey on the current trends in mobile honeypot researches. From the number of published research in this field we can conclude that it is a very new research area. We also recognize that building an accepted mobile honeypot is a big challenge. Most attempts have encountered difficulties because of the mobile limited hardware resources and the complexity of the programs required to achieve the honeypot's function. Some of the researchers use a Smartphone only to implement their honeypot. Others are send the collected events to a PC connected to a mobile network for analysis, and another builds their honeypot on a PC connected to a mobile network. When all honeypot functions, or part of these functions, are built on a mobile device then the honeypot must be a low interaction honeypot. But if the honeypot implemented on a PC (which is recommended) then the honeypot can be designed as: a highly interaction honeypot.

REFERENCES

[1] Lance Spitzner:"To build a honeypot ". http://www.spitzner.net/honeypot.html, Aug 1999.

[2] Christian Seifert, Ian Welch, and Peter Komisarczuk: "Taxonomy of honeypots", Victoria University of Wellington, School of Mathematical and Computing Sciences, Computer Science. Technical Report June 2006.

[3] Feng Zhang, Shijie Zhou, Zhiguang Qin, and Jinde Liu. "Honeypot: A supplemented active defense system for network security", College of Computer Science and Engineering, University of Electronic Science and Technology of China, IEEE, 2003.

[4] Provos, Niels. "A Virtual Honeypot Framework." In Proceedings of the 13th USENIX Security Symposium. 2004.

[5] Balachander Krishnamurthy : "Mohonk: Mobile honeypots to trace unwanted traffic early", ACM SIGCOMM'04Workshops, Portland, Oregon, USA, August 2004.

[6] Mulliner, C., Liebergeld, S., and Lange, M. "Poster: HoneyDroid - Creating a Smartphone Honeypot", Poster at IEEE Security & Privacy, May 2011.

[7] Matthias Wählisch, André Vorbach, Christian Keil, Jochen Schönfelder, Thomas C. Schmidt, Jochen H. Schiller : "Design, Implementation, and Operation of a Mobile Honeypot", arXiv:1301.7257v1, 30 Jan 2013.

[8] N. Husted, H.saidi, A.Gehani :"Smartphone Security Limitations: Conflicting Traditions", ACM, GTIP, Oriando, Florida USA, December 2011.

[9] Michael Freeman and Andrew Woodward: "SmartPot - Creating a 1st Generation Smartphone Honeypot", Proceedings of the 7th Australian Digital Forensics Conference, 1-3 December 2009.

[10] M. Wählisch, S. Trapp, C. Keil, J. Schönfelder, T. C.Schmidt, and J. Schiller, "First Insights from a Mobile Honeypot," in Proc. of ACM SIGCOMM, Poster Session. New York: ACM, August 2012, pp. 305–306.

[11] Matthias Wählisch, Sebastian Trapp, Jochen Schiller, Benjamin Jochheim, Theodor Nolte, Thomas C. Schmidt, Osman Ugus, Dirk Westhoff, Martin Kutscher,Matthias Küster, Christian Keil, Jochen Schönfelder: "Vitamin C for your Smartphone: The SKIMS Approach for Cooperative and Lightweight Security at Mobiles", SIGCOMM'12, August 13–17, 2012, Helsinki, Finland.

[12] Yubo Song, Xiaoyun Zhu, Yelin Hong, Haoyue Zhang, Hangbo Tan:"A Mobile Communication Honeypot Observing System", Fourth International Conference on Multimedia Information Networking and Security, November 2012 IEEE.

[13] S. Liebergeld, M. Lange, and C. Mulliner, "Nomadic honeypots: Anovel concept for smartphone honeypots", in Proc. W'shop on Mobile Security Technologies (MoST'13), together with 34th IEEE Symp. On Security and Privacy, May 2013, to appear.

[14] E.Gelenbe, G.Gorbil, D. Tzovaras, S. Liebergeld, D. Garcia, M. Baltatu, and G. Lyberopoulos : "Security for Smart Mobile Networks: The NEMESYS Approach", arXiv:1307.0687v1, 2 Jul 2013.

Author' biography

Assist. Prof. Dr. Hanaa M. A. Salman awarded her MSc and her PhD from University of technology Iraq in 2002, 2006 respectively. Currently she is a senior lecturer in computer science and a head master of the programing section in comuter science/University of Technology. Dr. Hanaa has more than 17 years of experience and she supervise of graduate students,Msc and Phd, her research interests include Cryptography, Computer Security, Biometrics, image processing, and Computer graphics,data ming, forinsics.

Assist. Prof. Dr. Nidaa Flaih Hassan AL-Alousi awarded her MSc and her PhD from University of technology Iraq in 1996, 2005 respectively. Currently she is a senior lecturer in computer science and a head master of the network section in comuter science/University of Technology. Dr. nidaa has more than 19 years of experience and she supervise of phd,Msc students, her research interests image processing, and Computer graphics,parall processing.

Assistance prof. Assmaa A. Fahad awarded her Bch and her MSc from University of Bagdad Iraq in 1991, 1997 respectively. Currently she is a Phd Student in computer scince/university of Technology. research interests Operating System, and Security.