Android Malware Traceability Matrix For Digital Forensic Investigation

Mohd Zaki Mas'ud[,*], Siti Rahayu Selamat, A'aisyah Mardhiyyah Mohammad Shahini, Shahrin Sahib, Nazrulazhar Bahaman

[1]Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

[*]Corresponding e-mail: zaki.masud@utem.edu.my

Keywords: Digital forensic, traceability matrix, mobile malware

ABSTRACT – Android-based mobile devices are among the prominent mobile devices use by the community and the amount of data stored in such devices is much less as compared to the amount of data stored in computers, but this small amount of data is potential to reveal useful information for mobile malware attack incident investigation. The traceability process in a mobile malware incident has become a crucial part of the digital forensic investigation process due to its capability to map the events of an incident from different sources in collecting evidence of an incident to be used for other additional investigation aspects. Thus, the need of finding and mapping evidence in Android platform has also become more important. Based on this reason, this research project proposes the adaptability of the traceability matrix to represent the relationship in the digital forensic investigation process by assimilating the traceability features in the android base mobile device environment. The aim of this research is to construct the traceability matrix in mobile forensic investigation to identify the relationship between the components of forensic investigation and the incident events discovered on Android-based mobile devices.

1. INTRODUCTION

The usage of mobile devices in recent years has been tremendously increasing especially when its functionality can do more than just making calls and handling SMS. According to the International Telecommunication Union (ITU) [1], in 2016, there are 7.5 billion mobile users with more than 3.8 billion mobile - broadband subscriptions worldwide. Currently, Android OS is widely used by the mobile devices market shares; Gartner Inc. stated that 84.1% smartphone sales during the first quarter of 2017 is on Android platform [2]. Despite the rapid growth of Android-based mobile devices in the market, ahead of the other competitors, it also has become an ideal place for malware writers. The increase in mobile applications in Android has also ignited the possibility of malicious programs that can exploit mobile devices that are used for online banking, online shopping or any sensitive transaction.

Consecutively, mobile malware has become a serious threat in the cyberspace and contribute as one of biggest digital crime incidents. Digital crime nowadays has grown tremendous especially with the evolving of diverse digital devices on the mobile platform. This in turn increased the potential for data stored on mobile devices to be used as evidence in civil or criminal cases [3]. However, current digital forensic investigation process model is lacking the standard of investigation process. Additionally, the insufficient of traceability (cross-referencing and linking) in the investigation processes leads to the difficulty of identifying the origin of the crime [4]. The investigation becomes more critical in tracing the evidence due to the huge volume of evidence generated from diverse digital devices [5]. Analysis and forensics of malware behaviour is an essential technology that extracts the runtime behaviour of malware and supplies signatures to detection systems and provides evidence for recovery, clean up and forensics [6]. The objective of digital forensic investigation process in a cybercrime is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for reconstructing past events while maintaining the chain of custody. Whereas the traceability process has become a crucial part of the digital investigation process because it is capable to map the events of an incident from different sources in collecting evidence of an incident to be used for other additional investigation aspects.

2. METHODOLOGY

This research constructs an Android malware incident traceability matrix which map the events of the malware incident with the malware traces are acquired from different sources. This traceability matrix helps malware forensic investigator to obtain evidence from an incident during a mobile malware analysis or investigation. In this research, traceability is defined as the ability to discover the events of an incident from different sources in order to obtain useful evidence. In order to have the evidence well managed, work in [7] suggested that a traceability can be established from the source evidence to its lower level evidence and from the lower level evidence back to their sources.

For the purpose of this research a case study of investigating a GoldDream android malware infection is executed. The Android malware is executed on Samsung Galaxy Tab 7.7 GT-P6800 16GB 1GB RAM and the network traffic activity, the *system call* and androids event log or *logcat* is captured. The behavior of the GoldDream Android's malware is believed to have the capability to log all incoming and outgoing phone calls and received SMS. The log captured is then sent to an external server [8]. At the same time the GoldDream Android's malware also captured the device's information such as IMEI, phone number and model, which then sent to an external server. The tracing and mapping procedures for the malware incident traces is shown in Figure 1 and Figure 2.

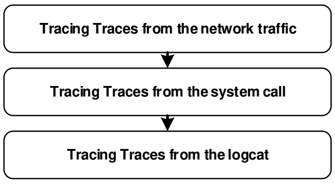

Tracing Traces from the network traffic
Tracing Traces from the system call
Tracing Traces from the logcat

Figure 1: Tracing procedures for tracing evidence of malware incident

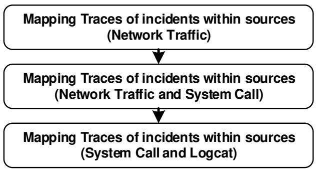

Mapping Traces of incidents within sources (Network Traffic)
Mapping Traces of incidents within sources (Network Traffic and System Call)
Mapping Traces of incidents within sources (System Call and Logcat)

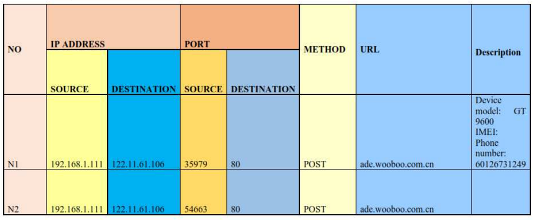
Figure 2: Mapping procedure for incident traces

3. RESULT AND DISCUSSIONS

The proposed Android malware incident traceability matrix identifies the relationship between the incident traces and the sources of evidence during the forensic investigation process. The sources of evidences for the traceability matrix in the case study are *network traffic*, *system call* and *logcat*. The relation between the sources of evidences is then defined by mapping the traces of malware behavior with each of the sources of the evidence. For example, every network traffic traces are mapped to *system call* traces and *system call* traces are mapped to *logcat* traces. Lastly, a traceability matrix for each link between the source evident is constructed. The information from multiple matrices is then combined into a main matrix in order to make important information more accessible. Figure 3, 4, 5 and 6 shows the main event versus evidence source matrix and the event versus the trace information matrix for each evidence source.

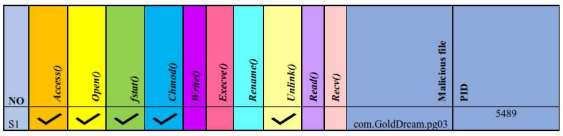
Case ID	Events	Evidence Source		
		Network	*System Call*	*Logcat*
1	GoldDream	N1	S1	L1
		N2	S2	L2

Figure 3 Main event Vs. Evidence Source



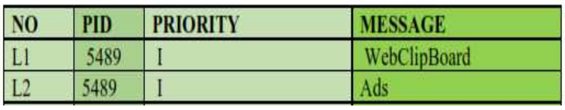
NO	IP ADDRESS		PORT		METHOD	URL	Description
	SOURCE	DESTINATION	SOURCE	DESTINATION			
N1	192.168.1.111	122.11.61.106	35979	80	POST	ade.wooboo.com.cn	Device model: GT 9600 IMEI: Phone number: 60126731249
N2	192.168.1.111	122.11.61.106	54663	80	POST	ade.wooboo.com.cn	

Figure 4 Network Traffic Vs. Evidence Source



NO	*Access()*	*Open()*	*fstat()*	*Chmod()*	*Write()*	*Execve()*	*Rename()*	*Unlink()*	*Read()*	*Recv()*	Malicious file	PID
S1	✓	✓	✓	✓				✓			com.GoldDream.pg03	5489

Figure 5 System call Vs. Evidence Source



NO	PID	PRIORITY	MESSAGE
L1	5489	I	WebClipBoard
L2	5489	I	Ads

Figure 6 *Logcat* Vs. Evidence Source

4. CONCLUSIONS

The traceability matrix in android forensic investigation introduce in this research is used to facilitate the forensic investigator on collecting the potential sources of evidence, tracing and mapping the evidence during the forensic investigation process. This help the investigator in identifying the traces relationship between the incident's events discovered. The traceability matrix shows the behavior of the mobile malware based on the attributes identified from the sources of evidence. This facilitates the investigator to have an early information that needed for the evidence to be discovered for the mobile malware cases. The construction of the traceability matrix is important to ensure the traces and the relationship of the evidence discovered during the investigation are completed with concern all potential sources of evidence.

ACKNOWLEDGEMENT

Authors are grateful to Universiti Teknikal Malaysia Melaka(UTeM) and Ministry of Higher Education of Malaysia for the financial support through Fundamental Research Grant Scheme FRGS/1/2015/ICT04/FTMK/02/F00290 and UTeM Short Grant Scheme PJP/2018/FTMK(4B)/S01631

REFERENCES

[1] International Telecommunications Union (ITU), 2016. ICT Facts Figures 2016. [ONLINE] Available at http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf. [Accessed 2 February 2017]

[2] Forni A. A. & Meulen R. V. D., 2017. *Gartner Says Worldwide Sales of Smartphones Grew 9 Percent in First Quarter of 2017.* [ONLINE] Available at http://www.gartner.com/newsroom/id/3725117. [Accessed 30 May 2017]

[3] Catanese S, Ferrara E, Fiumara G. Forensic analysis of phone call networks. *Social Network Analysis and Mining*. 2013 Mar 1;3(1):15-33.

[4] Shields C, Frieder O, Maloof M. A system for the proactive, continuous, and efficient collection of digital forensic evidence. *Digital investigation*. 2011 Aug 1;8:S3-13.

[5] Garfinkel SL. Digital forensics research: *The next 10 years. digital investigation*. 2010 Aug 1;7:S64-73

[6] Wu S, Wang P, Li X, Zhang Y. Effective detection of android malware based on the usage of data flow APIs and machine learning. *Information and Software Technology*. 2016 Jul 1;75:17-25.

[7] Hargreaves C, Patterson J. An automated timeline reconstruction approach for digital forensic investigations. *Digital Investigation*. 2012 Aug 1;9:S69-79.

[8] Mas' ud MZ, Sahib S, Abdollah MF, Selamat SR, Yusof R, Ahmad R. Profiling mobile malware behaviour through hybrid malware analysis approach. *Information Assurance and Security (IAS), 2013 9th International Conference*. 2013 Dec 4 (pp. 78-84). IEEE.