Mobile Forensics: Evidence Collection and Malicious Activity Identification in PPDR Systems

Konstantia Barbatsalou, Edmundo Monteiro and Paulo Simoes
CISUC/DEI, University of Coimbra
Coimbra, Portugal
{konstantia, edmundo, psimoes}@dei.uc.pt

ABSTRACT

During the last decade, smartphones have shown increased computational and networking capabilities. With the high bandwidth supported by Fourth Generation/ Long-Term Evolution (4G/LTE) technology, end-users will enjoy improved quality of communications, especially concerning data transfer services [1] in commercial and dedicated, Public Protection and Disaster Relief (PPDR) systems. PPDR infrastructures "are used by agencies and organizations dealing with the maintenance of law and order, the protection of life and property and with emergencies" [2]. With this transition, many research fields are developing, especially related to security issues. This work summarizes how the discipline of Mobile Forensics (MF), with various acquisition methods, complements traditional anti-malware and detection systems and contributes to malicious activity identification in PPDR systems. Additionally, a framework based on MF methods is proposed, alongside with its infrastructure and components. Estimations about the validation procedure and expected results are performed. Lastly, upcoming challenges and further research are discussed.

KEYWORDS

Information Security, Mobile Forensics, Live Forensics, Public Protection and Disaster Relief (PPDR), PPDR security

1 INTRODUCTION

Mobile communications are a part of users' everyday life. Not only have handsets become a means of everyday interaction, but they also bring a new aspect to it, with increased computational capabilities that allow previously complicated and demanding services, such as Voice over IP (VoIP), video streaming, etc. to run without any impediments. This particular trait has also been an objective from the PPDR systems discipline, which also had an increasing demand of high-bandwidth services. However, the widespread use of this kind of services also brings big risks concerning the increasing number of threats and attacks against mobile devices and networks. Characterized by bigger complexity, the negative impact in the functionality of targeted systems is also severe.

Initially, this paper presents the current threat and attack vectors and enlists the implemented mechanisms against their activity, as well as their advantages and drawbacks. Additionally, ForEmSys, a framework based on Mobile Forensics methods for evidence collection and identification of malicious activity is presented and discussed.

The rest of the paper is structured as follows. Section 2 discusses previous research work in the field, while Section 3 presents the proposed ForEmSys framework. Lastly, Section 4 concludes with a discussion about its potential impact.

2 RELATED WORK

Lately, the use of LTE technologies has expanded from commercial communication networks to

Public Protection and Disaster Relief (PPDR) systems, driven by the need for broadband support and improved Quality of Service (QoS). LTE systems will complement and gradually replace the previous generation of "Terrestrial Trunked Radio (TETRA) and TETRAPOL specifications" [3], [4]. The PPDR dedicated version of LTE will combine the existing features of commercial networks with PPDR-related characteristics, such as group communications, push-to-talk (PTT) and end-to-end security monitoring [5].

This new discipline brings certain risks, such as threats of intrusion deriving from malicious third parties in communications. While this threat already exists on legacy systems, the increasing usage of IP-based communications, the adoption of off-the-shelf technologies and the complexity of mobile terminals introduce novel attack vectors. Potential attackers are capable of eavesdropping voice, video and data communications, jamming communications or injecting fake data to disturb situational awareness. Due to the emerging need for devices protection against malicious activity, various methods have been developed [6]. While some use traces of existing malicious software, such as signatures as identification means, others aim to observe the device behavior during normal and infected states and create patterns as anomaly identifiers [7]. Each detection category has its own advantages and drawbacks and they all serve as components in more complex structures, such as mobile markets with native application-checking mechanisms [8], [9], antivirus software [10] and Intrusion Detection Systems (IDSs) [11], [12]. Both markets and antivirus suites use static detection techniques, a method ineffective against unknown and zero-day malware, trait existing in mobile IDSs, using behavior-based techniques. Additionally, an IDS, when consisting of a host and a network instance, is capable of identifying other threat types, such as eavesdropping, spoofing and Denial of Service. Despite that fact, an IDS is collecting a big amount of data, a considerable number of which is irrelevant to malicious activity, or restricted solely to events.

An approach to evidence collection from mobile devices related to malicious events and their identification while interacting with other security mechanisms derives from the use of Mobile Forensics (MF), "the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods" [13]. After the increase in use and capabilities of mobile devices, it has become a routine task for investigators and a thriving source of research interests for the academic community. More precisely, to determine if a device has been compromised "it is necessary to perform either a post-mortem analysis, where a duplicate of the flash memory is examined, or a live examination of the device" [14]. While live acquisition occurs in almost real-time and is capable of retrieving volatile data, post-mortem acquisition occurs after or during a device shutdown, with three different approaches; manual, logical and physical [15]. Physical methods interact with the device hardware, logical methods interact with the file system and manual acquisition is summarized by whatever an individual is capable of retrieving by the normal device usage. To the best of our knowledge, few research works have been conducted in the field of using MF methods for malicious activity detection and evidence collection [16], including approaches related to live process acquisition [17], [18], network traffic analysis [19], and signature-based detection for malware in running devices [20]. Novel approaches towards that direction are adopted in projects related to PPDR systems.

There is currently a significant amount of projects aiming at developing secure environments for new generation PPDR networks. Among others, the SALUS (Security and interoperability in next

generation PPDR communication infrastructures) European Framework Program (FP7) project focuses on "designing, implementing and evaluating a next generation communication network concept for PPDR agencies, supported by network operators and industry, which will provide security, privacy, seamless mobility, QoS and reliability support for mission-critical Personal Mobile Radio (PMR) voice and broadband data services" [21]. More precisely, the project examines and benchmarks the functionality of new generation PPDR networks in the context of three different scenarios (city security, disaster recovery and temporary protection). This way, the whole spectrum of technological and economic factors is covered and observations about migration to 4G wireless communications are made. Towards the security perspective, a Security Services Centre is responsible for the management and control of the security mechanisms implemented for all the infrastructures participating in a PPDR system. The category on which the current work focuses on is related to security mechanisms applied in mobile terminals and aims to identify attacks and threats by the use of MF methods, by interacting with other security components.

Knowledge and results deriving from the current work, as well us research in mobile security for PPDR will be incorporated in the deliverables of the SALUS project. Implemented security mechanisms will be enhanced with an evidence collection and malicious activity identification module.

3 FOREMSYS FRAMEWORK

In the context of Mobile Forensics as a means of identifying and collecting evidence about potential malicious activity with generated alerts deriving from various security mechanisms in a PPDR system environment, we propose the ForEmSys framework, a detailed overview of which is depicted in Figure 1.

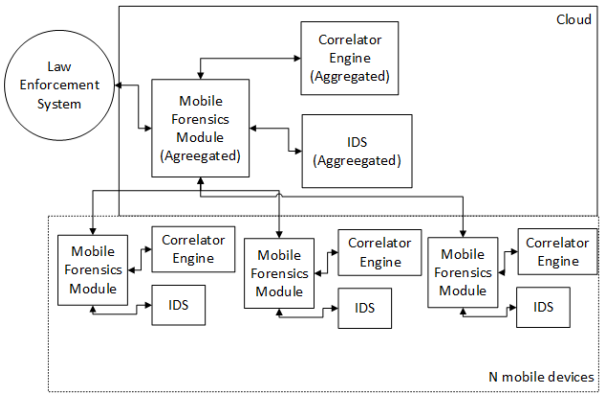

Figure 1. ForEmSys architecture

A Law Enforcement System, belonging to forces such as police and complementary departments (fire service) is responsible for the management of both the aggregated and host instances. Each PPDR LTE device is equipped with the system's mobile version, consisting of an IDS, a correlation engine and a module responsible for conduction of forensic acquisition. A framework management interface is available for command and control operators, while the MF module runs as a service in host mobile devices. According to the state-of-the-art research, a hybrid IDS approach (host- and network- based) will be adopted, so as to take profit from the best of both worlds and maximize the number of detected potential malicious attacks. Anomaly and signature based techniques will be used for detection purposes. Due to the fact that an IDS generates many, not needed alarms, the correlation engine will filter incidents irrelevant to MF, so as to achieve efficient load distribution. After receiving an alert concerning an event, the forensic module performs post-mortem or live acquisition, according to the nature of the asset that has been compromised.

Considering that physical acquisition demands interaction with hardware and usually sets the mobile device in a non-operational state, option

ISBN: 978-1-941968-03-1 ©2014 SDIWC

that is excluded because of the need for continuous service provision, pseudo-physical or logical acquisition will be conducted. Logical is regarded as a more appropriate candidate because it does not require a system reboot (responsible for volatile data loss) and is also flexible in acquiring either specific parts of the file system or the whole copy of it if needed. The same mechanism is used for the aggregated instance and the mobile devices, with the main difference being that no individual can be certain about the data integrity in the latter. However, under certain circumstances, even falsified evidence, especially in nodes within proximity can be an indicator of massive device compromising. The aggregated instance collects information from the mechanisms of PPDR devices, ensures its validity and generates rules concerning future attacks of the same or similar type.

The following step after the framework outline, concerns the technology used for the components. Technology used in the PPDR mobile devices is one of the most important factors, since it affects the decisions taken for the rest of the infrastructure. The Android operating system was considered as the most appropriate candidate due to its widespread use, its open source distribution, which facilitates the access to libraries and other development tools, and overall the bigger percentage of malicious applications and attacks designed for it [22], thing that makes the research field relatively broad. Additionally, forensic acquisition can be performed in two modes, in rooted and non-rooted devices and further observations can be made about the effectiveness of each method.

Evidence collection and identification of malicious activity traces examined by the audit trails of the mobile forensic module is conducted through two directions. Firstly, we propose a technique for improving the efficiency of signature-based detection techniques, by observing changes occurring in malicious software signatures during an infection process. This way, the community benefits from the improved version of a resource friendly detection method. Secondly, when signature-based detection proves to be unsuccessful, malicious activity is identified by the use of anomaly-based detection techniques. In that particular case, forensic acquisition techniques can prove useful either by retrieving traces of the behavior of an infected device and comparing them to a non-infected sample or by live capturing of equivalent events and observing if they belong to a previously recorded ruleset.

Before the phase of experiments conduction, the datasets used have to be defined. Since the research focuses on a universe of different threat and attack types, the datasets have to relate to an equivalent variety. Some of the available datasets to be selected are the Information Security Centre of Excellence (ISCX) 2012 IDS dataset, replacement of the KDDCup99 [23], the ICSX Botnet dataset, dedicated to botnet identification, datasets from the Malware Genome Project [24] and the CAIDA DDoS Attack 2007 Dataset [25]. Nevertheless, the creation of our own datasets, such as a sequence of specific attacks cannot be excluded in case of need.

Both techniques have to be evaluated upon their conduction during a dedicated experimental phase. Firstly, for signature-based techniques, we will aim to the efficiency and optimization of their performance, by maintaining a reasonable number of comparisons between the potential and sample signatures. Decision trees and Rule Clustering will be used towards that direction. Secondly, machine-learning algorithms will be applied in order to evaluate anomaly-based detection techniques. Support Vector Machine (SVM), due to different approaches than the rest of methods of the same type and especially to the trait of generalization error minimization [26],

ISBN: 978-1-941968-03-1 ©2014 SDIWC

Artificial Neural Networks (ANNs), because of their capabilities of recognizing patterns under difficult circumstances, such as incomplete and noisy data and the potential of unknown forms recognition [27], Bayesian Networks, mainly due to the fact that they are able to use prior knowledge and Fuzzy Logic, due to the specification on certain attacks and high power consumption indications are the most appropriate candidates.

Receiver Operating Characteristic (ROC) Curves and Area Under Curve (AUC) serve as evaluation tools about the effectiveness of anomaly detection methods. Ratios such as True Positive (TPR), False Positive (FPR) detection Rates will be calculated for each detection method.

Last but not least, the framework operating in practice can provide information about the effectiveness of each forensic acquisition type (post-mortem and live) on malicious activity detection, depending on which one of them retrieves the more relevant data to the compromised assets.

4 DISCUSSION

The ForEmSys framework contributes to the area of security preservation in PPDR environments with the following aspects:

- Due to the different types of alert sources and in combination with the MF methods, there is no limitation to the kinds of attacks that can be identified. They vary from plain malware activity, to Denial of Service (DoS), botnets, etc. However, experimental observation is required so as to acquire a precise view of the identification efficiency for each threat/attack type.
- Improvement of signature-based detection techniques by observation and tracking of changes occurring due to evolving malware transformation. Evidence collection of previous events can provide sufficient information in constructing malware signature transformation profiles.
- Post-mortem and live forensic methods, with access to processes and real-time information provide new approaches in identifying patterns of attacks in behavior-based detection. While post-mortem methods provide sources of evidence for pattern examination, live ones, with almost-real time access of elements offer the potential for immediate identification.

With the proper validation, efficiency of the previously mentioned methods will be evaluated. Thus, strengths and weaknesses are defined and can be a trigger for further research and optimization.

5 CONCLUSION

In this paper, we presented an extended approach to the use of MF. Evidence collection, but also identification of malicious activity based on it, are a promising solution to the mobile ecosystem, especially in PPDR networks, where protection of data and other assets is a critical matter. Towards this direction, we presented ForEmSys, a framework operating in PPDR systems, which receives input of other security mechanisms, performs forensic acquisition on devices and identifies potential malicious activity based on the data retrieved. With further research performed on the subject, existing methods will ameliorate while new, challenging ones will arise.

ACKNOWLEDGEMENTS

This work was partially funded by Project QREN ICIS (Intelligent Computing in the Internet of Services – CENTRO-07-0224-FEDER-002003). We also thank the team of FP7 Project SALUS (Security

and interoperability in next generation PPDR communication infrastructures) for the fruitful discussions and feedback on the ForEmSys framework.

REFERENCES

[1] G. Pande, "Performance Evaluation of Video Communications Over 4G Network," In *Intelligent Computing, Networking, and Informatics*, Springer India, pp. 797-803, 2014.

[2] A. R. Jamieson, "*Radiocommunication for public protection and disaster relief*," 2004. [Online]. Available: https://www.itu.int/itunews/manager/display.asp?lang=en&year=2006&issue=03&ipage=publicProtection&ext=html.

[3] S.-q. Li, Z. Chen, Q.-Y. Yu, W.-X. Meng and X.-Z. Tan, "Toward Future Public Safety Communications: The Broadband Wireless Trunking Project in China," *Vehicular Technology Magazine*, IEEE, vol. 8, no. 2, pp. 55-63, 2013.

[4] R. Ferrús, O. Sallent, G. Baldini and L. Goratti, "LTE: The Technology Driver for Future Public Safety Communications," *Communications Magazine*, IEEE, vol. 51, no. 10, pp. 154-161, 2013.

[5] K. Balachandran, K. C. Budka, T. P. Chu and T. L. Doumi, "Mobile Responder Communication Networks for Public Safety," *Communications Magazine*, IEEE, vol. 44, no. 1, pp. 56-64, 2006.

[6] M. La Polla, F. Martinelli and D. Sgandurra, "A Survey on Security for Mobile Devices," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 446-471, 2013.

[7] A. Shabtai, Y. Kanonov, Y. Elovici, C. Glezer and Y. Weiss, ""Andromaly": a behavioral malware detection framework for android devices," *Journal of Intelligent Information Systems*, vol. 38, no. 1, pp. 161-190, 2011.

[8] Y. Zhou, Z. Wang, W. Zhou and X. Jiang, "Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets." In *Network and Distributed System Security Symposium*, 2012, 2012.

[9] N. Viennot, E. Garcia and J. Nieh, "A Measurement Study of Google Play,", *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 1, ACM New York, NY, USA, 2014.

[10] V. Rastogi, Y. Chen and J. Xuxian , "Catch Me If You Can: Evaluating Android Anti-Malware Against Transformation Attacks", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 99-108, IEEE, 2014

[11] G. Portokalidis, P. Homburg, K. Anagnostakis and H. Bos, "Paranoid android: versatile protection for smartphones," In *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC'10, pp. 347-356, New York, NY, USA, 2010.

[12] D. Damopoulos, G. Kambourakis and G. Portokalidis, "The best of both worlds: a framework for the synergistic operation of host and cloud anomaly-based IDS for smartphones," In *EuroSec '14 Proceedings of the Seventh European Workshop on System Security*, New York, NY, USA, 2014.

[13] W. Jansen and R. P. Ayers, SP 800-101. *Guidelines on Cell Phone Forensics*. Gaithersburg, MD, United States: National Institute of Standards & Technology, 2007.

[14] E. Casey, "*Smartphone forensics and mobile malware analysis*," 2013. [Online]. Available: http://www.caseite.com/content/smartphone-forensics-and-mobile-malware-analysis.

[15] K. Barmpatsalou, D. Damopoulos, G. Kambourakis and V. Katos, "A critical review of 7 years of Mobile Device Forensics," *Digital Investigation*, vol. 10, no. 4, pp. 323-349, 2013.

[16] K. Barbatsalou, B. Sousa , E. Monteiro and P. Simoes, "Mobile Forensics for PPDR Communications: How and Why," Accepted for publication at the *10th Int. Conf. on Cyber Warfare and Security (ICCWS-2015)*, South Africa, 2015.

[17] V. L. L. Thing, K.-Y. Ng and E.-C. Chang, "Live memory forensics of mobile phones," *Digital Investigation*, vol. 7, pp. 74-82, 2010.

[18] A. Houmansadr, S. A. Zonouz and R. Berthier, "A cloud-based intrusion detection and response system for mobile phones," In *DSNW '11 Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops*, pp. 31-32, Washington, DC, USA, 2011.

[19] P. Schutz, M. Breuer, H. Hofken and M. Schuba, "Malware proof on mobile phone exhibits based on GSM/GPRS traces," In *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013)* , 2013.

[20] F. DiCerbo, A. Girardello, F. Michahelles and S. Voronkova, "Detection of malicious applications on

Android OS," In *Proceedings of the 4th international conference on Computational forensics*, pp. 138-149, 2010.

[21] SALUS, 2014. *SALUS - Security and interoperability in next generation PPDR communication infrastructures*. [Online] Available at: http://www.sec-salus.eu

[22] CISCO, "*CISCO 2014 Annual Security Report*," 2014.

[23] ISCX, "*Information Security Centre of Excellence (ISCX) Datasets*," 2012. [Online]. Available: http://iscx.ca/datasets.

[24] Android Malware Genome Project, "*Android Malware Genome Project*" 2012. [Online]. Available: http://malgenomeproject.org

[25] CAIDA, "*Center for Applied Internet Data Analysis - Data*" 2007. [Online]. Available: http://www.caida.org/data/passive/ddos-20070804_dataset.xml.

[26] C. A. Catania , F. Bromberg and C. G. Garino , "An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection," *Expert Systems with Applications*, vol. 39, no. 2, pp. 1822–1829, 2012.

[27] R. Moskovitch, S. Pluderman, I. Gus, D. Stopel, C. Feher, Y. Parmet, Y. Shahar and Y. Elovici, "Host Based Intrusion Detection using Machine Learning," In *2007 IEEE Intelligence and Security Informatics*, New Brunswick, NJ, USA, 2007.