UNIVERSITI PUTRA MALAYSIA

IMPROVING MALICIOUS DETECTION RATE FOR FACEBOOK APPLICATION IN OSN PLATFORM

LAAVANYA A/P ANGAMUTHU

FSKTM 2018 41

IMPROVING MALICIOUS DETECTION RATE FOR FACEBOOK APPLICATION IN OSN PLATFORM

By

LAAVANYA A/P ANGAMUTHU

Thesis submitted to the Faculty of Computer Science and Information Technology, University Putra Malaysia, in fulfillment of the requirements for the Master of Information Security

JUNE 2018

COPYRIGHT PAGE

DEDICATIONS

‘‘This sweet dedication goes to respected lecturers, thoughtful friends and supportive family’’

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Information Security

IMPROVING MALICIOUS DETECTION RATE FOR FACEBOOK APPLICATION IN OSN PLATFORM

By

LAAVANYA A/P ANGAMUTHU

JUNE 2018

Supervisor: Dr. Aziah Aswami
Faculty: Faculty of Computer Science and Information Technology

Online social networks (OSNs) have become the new vector for cybercrime, and hackers are finding new ways to propagate spam and malware on these platforms, which we refer to as social malware. As we show here, social malware cannot be identified with existing security mechanisms (e.g., URL blacklists), because it exploits different weaknesses and often has different intentions. In this dissertation, we show that social malware is prevalent in Facebook, the largest OSN to date with more then a billion users and develop an efficient and scalable social malware detection system that takes advantage of the social context of posts. We deploy this detection system to detect malicious in order protect Facebook users from social malware. We find that our detection method is both accurate and efficient. Furthermore, we show that, social malware significantly differs from traditional email spam or web-based malware. One of the major factors for enabling social malware is malicious third-party apps. We show that such malicious apps are also widespread in Facebook. Therefore, to identify malicious apps, we ask the question: given a Facebook application, can we determine if it is malicious? Our key contribution in this part is in developing malware detection in Facebook third party application by using Naïve Bayes algorithm technique .We identify a set of features that help us distinguish malicious apps from benign ones. For example, we find that malicious apps often share names

with other apps, and they typically request fewer permissions than benign apps. Then, leveraging these distinguishing features, we show that can detect malicious apps with 99.5% accuracy, with no false positives and a low false negative rate (4.1%). Finally, we explore the ecosystem of malicious Facebook apps. We identify mechanisms these apps use to propagate and find that many apps collude and support each other.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk Ijazah Sarjana Keselamatan Maklumat

IMPROVING MALICIOUS DETECTION RATE FOR FACEBOOK APPLICATION IN OSN PLATFORM

By

LAAVANYA A/P ANGAMUTHU

JUNE 2018

Peyelia: Dr. Aziah Aswami
Faculti: Faculty of Computer Science and Information Technology

Rangkaian sosial dalam talian (OSN) telah menjadi vektor baru untuk jenayah siber, dan penggodam mencari cara baru untuk menyebarkan spam dan malware pada platform ini, yang kami merujuk sebagai malware sosial. Seperti yang ditunjukkan di sini, malware sosial tidak boleh dikenalpasti dengan mekanisme keselamatan sedia ada (cth., Senarai hitam URL), kerana ia mengeksploitasi kelemahan yang berbeza dan sering mempunyai niat yang berbeza. Dalam disertasi ini, kami menunjukkan bahawa malware sosial lazim di Facebook, OSN yang terbesar setakat ini dengan lebih dari satu bilion pengguna dan membangunkan sistem pengesanan malware sosial yang cekap dan berskala yang mengambil kesempatan daripada konteks sosial siaran. Kami menggunakan sistem pengesanan ini sebagai aplikasi Facebook bernama MyPageKeeper untuk melindungi pengguna Facebook dari malware sosial. Kami mendapati bahawa kaedah pengesanan kami adalah tepat dan cekap. Tambahan pula, kami menunjukkan bahawa malware sosial jauh berbeza dengan spam e-mel tradisional atau malware berasaskan web. Salah satu faktor utama yang membolehkan malware sosial adalah aplikasi pihak ketiga yang berniat jahat. Kami menunjukkan bahawa aplikasi berniat jahat itu juga tersebar luas di Facebook. Oleh itu, untuk mengenal pasti aplikasi berniat jahat, kami bertanya: diberikan aplikasi Facebook, bolehkah kita menentukan sama ada berbahaya? Sumbangan utama kami

dalam bahagian ini adalah untuk membangunkan Penguji Aplikasi Rapi Facebook (FRAP) - dasarnya alat pertama yang memberi tumpuan kepada mengesan aplikasi berniat jahat di Facebook. Kami mengenal pasti satu set ciri yang membantu kita membezakan aplikasi berniat jahat dari orang-orang yang tidak bermaya. Sebagai contoh, kami mendapati bahawa aplikasi berniat jahat sering berkongsi nama dengan aplikasi lain, dan mereka biasanya meminta lebih sedikit kebenaran daripada aplikasi yang tidak selamat. Kemudian, memanfaatkan ciri-ciri yang membezakan ini, kami menunjukkan bahawa boleh mengesan aplikasi berniat jahat dengan ketepatan 99.5%, tanpa positif palsu dan kadar negatif palsu yang rendah (4.1%). Akhir sekali, kami meneroka ekosistem aplikasi Facebook yang berniat jahat. Kami mengenal pasti mekanisme aplikasi ini digunakan untuk menyebarkan dan mendapati bahawa banyak aplikasi bersatu dan menyokong satu sama lain.

ACKNOWLEDGEMENT

I feel grateful and thanks to GOD because of His bless and mercy. During this period, I am able to learn so many new things especially related to security in Information Technology. First, I would like dedicate this appreciation to my supervisor, Dr. Aziah Asmawi who always patient in helping me and giving advice for improvements. I am very thankful towards his effort and sharing of knowledge to support me until the end of this project. Next my appreciation goes to my parent who always gives me endless moral support and encouragement. Always give advices to keep me strong. Not to be forgotten, thanks to my friends who are not tired to give their opinion and constructive comments that able to improve my project. Thank you.

APPROVAL FORM

This thesis was submitted to the Senate of University Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master Information Security. The members of the Supervisory Committee were as follows:

DR. AZIAH

Faculty of Computer Science and Information Technology

University Putra Malaysia

(Supervisor)

Date: June 2018

DECLARATION FORM

Declaration by graduate student

I hereby confirm that:

- This thesis is my original work
- Quotations, illustrations and citations have been duly referenced
- This thesis has not been submitted previously or concurrently for any other degree at any other institutions
- Intellectual property from the thesis and copyright of thesis are fully-owned by University Putra Malaysia (UPM)
- Written permission must be obtained from supervisor and Deputy Vice-Chancellor (Research and Innovation) before thesis is published in book form
- There is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity was upheld as according to Rule 59 in Rules 2003 (Revision 2013-2014). The thesis has undergone plagiarism detection software

Signature: ________________________ Date: __________________

Name and Matric No.: LAAVANYA A/P ANGAMUTHU (GS 47262)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.0 Introduction

As for introduction, this chapter will briefly explain about the research background, highlight the problem statement, research objective, research scope, research schedule and brief description of thesis structure.

In this background research, there is a brief description about related field of study for this project. Background research is mainly to collect information to have understanding in-depth about related subject. For this project, understanding about malware especially behaviours nature is a foundation to have overall overview about this project. Besides, study about malware detection system is also important to know how malware analysis is being done. Lastly, as this project are using memory analysis to gather information, knowing what is memory analysis and how can it be used in this project is very helpful.

Most online social network even Facebook and Twitter become medium to human communicated with others in world. Some use for their personal usage, entertainment, business and etc. Regular users make pervasive use of social networks too, to stay in touch with their friends or colleagues and share content that they find interesting. The trust relationships that build by online social network for user make them use the account with undoubtful. There are many reasons how the trust was developed within user. For example, the user might know the owner of the trusted account in person or the account might be operated by an entity commonly considered as trustworthy, such as a popular news agency. But if the account fall to hackers or enemy they might misuse and can exploit form their own purpose.

Most of research which discuss on compromised account to spread the content which is fake become advantages to criminal because most of OSN user are not aware on this and mostly will reach to any post or message posted from trusted account [1]. These favorable probabilities of success exceedingly attract the attention of cyber criminals. If attacker successfully compromised the account from trusted OSN, they can misuse that account for own benefit by spread spam message, link, phishing or adware in website link [2]. This attack considers as traditional and mostly focus on large population. Most of these accounts has large circle in social media and their popularity become most suggested in many social network users. Recent attacks show that compromising these high-profile accounts can be leveraged to disseminate fake news alerts, or messages that tarnish a company's reputation **[3], [4], [5], [6].**

Malicious software or malware is any malicious code in software that can be used to compromise computer operations, gather sensitive information, gain access to private computer resources and do any illegitimate action on data, host or networks. Malware can infect and exploit resource from various system platforms. There are various classes of malware such as virus, worms, Trojans, bots, back doors, rootkits and etc. Malware are considered as dangerous as it can attack main security goals which is confidentiality, integrity and availability.

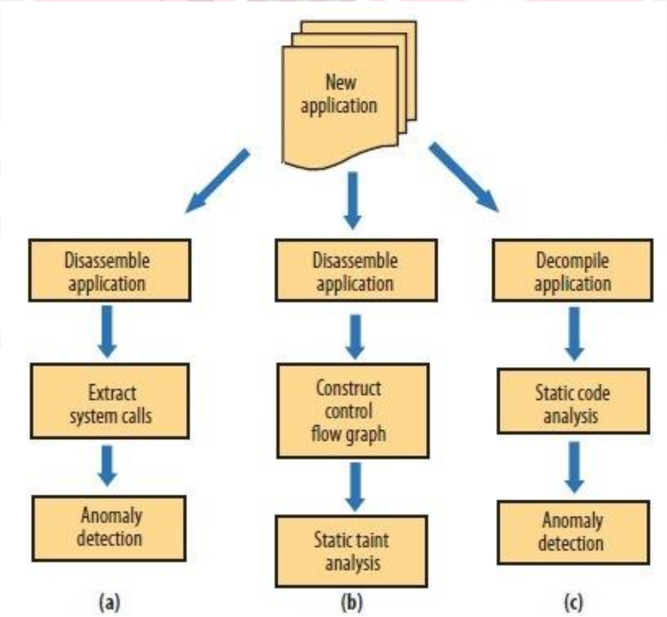
In this modern technology, malware also rapidly evolve through various stealth techniques to avoid detection. By only depends on the signatures and anomaly-based techniques is not reliable. Therefore, as a researcher, we need to focus more on finding the generalized and scalable features of malware. Nowadays, malware creator also works on anti-antivirus techniques to give a complex challenge for anti-malware researcher to detect malware. This is because most of anti-antivirus is aims to bypass existing antivirus system. This is a few examples of methodologies use by malware creators to avoid anti-virus detection **[1].**

a) **Code Obfuscation**: Malware code try to look tangled and causing the signature based approach failed by includes some unnecessary jumps, replacing unused registers, no-op instructions and others.

b) **Encryption**: Encrypted malware consists of encrypted part that able to beat easily signature based approach

c) **Polymorphism & Metamorphism**: Polymorphism makes use of payload while metamorphism can change itself or do self-mutating. These two methodologies are powerful and difficult to be detected.

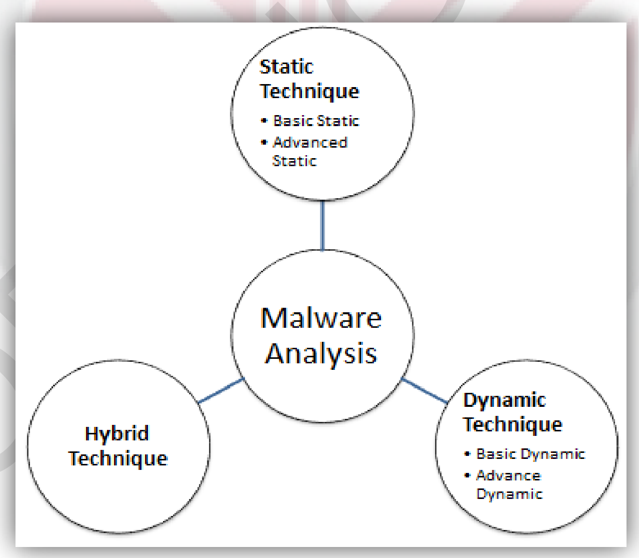
Figure 1: Malware Detection System



Malware detection technique needs to be periodically updated and must always one step further than those entire anti-antimalware products. As shown in Figure 1, Malware Detection

System consists of three main parts which is analysis technique or as known as malware analysis, detection approach and deployment approach **[4].** Malware analysis is the important part need to be considered to achieve an effective technique and approach. Malware analysis is a process to perform analysis and study the components on malware's code and identify the characteristic of their behavior. Besides, as shown in Figure 2, in malware analysis there are three main techniques can be used which is static technique, dynamic technique and hybrid. Static technique is being done without running the malware while dynamic technique will execute malware. Hybrid is the combination of Static and dynamic technique **[5].**

Figure 2: Malware Analysis Method



This project will use dynamic technique. There are two type of dynamic technique which is basic dynamic analysis and advanced dynamic analysis. Basic dynamic will used virtual machine to do malware analysis and monitor the process and the behavior of malware, while the advanced dynamic will further analyze in depth about the malware. Second part of malware detection system is detection approach. Detection approach can be used are anomaly, signature or hybrid.

In this paper, we propose new detection method where to use user profile to analyses their content in OSN. By using user activity history and their pattern, we can get the behavior act of compromised account by using light manner method. The existing OSN give a high-quality service like message, upload post or photo, check friend list, share the feeling etc. However, how a user involves in each activity is completely driven by personal interests and social habits. Thus, the interaction patterns with several OSN activities tend to be divergent across a large set of users. While a user tends to conform to its social patterns, a hacker of the user account who knows little about the user's behavior habit is likely to diverge from the patterns.

As we discuss in previous paragraph, we conduct a study on online user social behaviors by collecting and analyzing user clickstreams **[7], [8], [9], [10]** of a well-known OSN website. Based on our observation of user interaction with different OSN services, we propose several new behavioral features that can effectively quantify user differences in online social activities. For each behavioral feature, we deduce a behavioral metric by obtaining a statistical distribution of the value ranges, observed from each user's clickstreams. Moreover, we combine the respective behavioral metrics of each user into a social behavioral profile, which represents a user's social behavior patterns. To validate the effectiveness of social behavioral profile in detecting account activity anomaly, we apply the social behavioral profile of each user to differentiate clickstreams of its respective user from all other users. We conduct multiple cross-validation experiments, each with varying amount of input data for building social behavioral profiles. Our evaluation results show that social behavioral profile can effectively differentiate individual OSN users.

As described in previous paragraph, the malware is a large group of software. Some of the malware is used just to distract people from work, some for fun, however there is some malware which is very harmful. Sometimes it tries to steal your bank account or even ruin your computer.

1.2 Problem Statement

Modern malwares tend to become tricky and confusing the malware scanner as they able to combine several characteristics of undesirable program from different classes **[2]**. Besides, they are also evolved rapidly in every aspect especially on advancing their attack strategies **[8]**. To avoid detection, there are some malware that use obfuscating techniques such as reuse a legal code, capable to modify their structure (polymorphism) and able to replace some routine of targeted resource (stealth virus) **[9]**. Those evolvement and advanced trick cause code-centric approach becomes ineffective.

Online social networks are widely use these days for communication. Users can share more type of information among friends. But there exist some social network users who misuse the features of these social networks and promote the spreading of malicious content. They do this by uploading the malicious post in other user page. These contents spread at a fast rate. There is no proper mechanism to detect these malicious posts immediately and remove it effectively.

There is various attack been address by researchers but compromised accounts in OSN are more popular among hackers. The comprising account in online social network one of profitable for criminal earns money. Most of this activity mainly targeting the big organizational, fan page and business account. Unfortunately, should the control over an account fall into the hands of a cyber-criminal, he can easily exploit this trust to further his own malicious agenda. Previous research showed that using compromised accounts to spread malicious content is advantageous to cyber criminals because social network users are more likely to react to messages coming from accounts they trust. The impact on this issue and attacks can cause reputation damage or financial loss. The detection of compromised accounts is quite challenging due to the well-established trust relationship between the service providers, account owners, and their friends.

1.3 Research Objective

The objective of this project generally is to develop a model based on data-centric approach that can detect OSN third party applications based on trace pattern found in memory dump. The objective is specifically defining as below;

a) **To propose a set of social behavioral features that can effectively characterize the user social activities on OSN.**

By using online dataset proposed by research, we extract benign and malware features to run the analysis. The dataset been placed by previous who work on malware detection on Facebook application. This dataset proven increase the rate of detection as they include few combination of APK module.

b) **To develop framework to evaluate and provide accurate analysis to detect malicious application in Facebook**

The main goal of this research are to develop framework to evaluate and provide more accurate result on detect malicious third party application in Facebook. As the scope focus on APK format application, we include android module in order the system synchronize with it.

1.4 Research Scope

Our approach considers both extroversive and introversively behaviours. Based on the characterized social behavioural profiles, we can distinguish a user from others, which can be easily employed for compromised account detection [11]. Specifically, we introduce eight behavioural features to portray a user's social behaviours, which include both its extroversive posting and introversively browsing activities. A user's statistical distributions of those feature values comprise its behavioural profile. While users' behaviour profiles diverge, individual user's activities are highly likely to conform to its behavioural profile. This fact is thus employed to detect a compromised account, since impostors' social behaviours can hardly conform to the authentic user's behavioural profile. Our evaluation on sample Facebook users indicate that we can achieve high detection accuracy when behavioural profiles are built in a complete and accurate fashion.

1.5 Research Schedule

This project is one year period which start in June 2017 and expected to finish in June 2018. Generally, this project has six activities which are project implementation plan, knowledge gathering, experimentation design, implementation and development, testing and evaluation and lastly report write up. Each project activities have their own milestones that need to be achieved. The details for project activities and time take can be refer in Gantt chart in Appendix section.

1.6 Thesis Structure

The structure of this thesis consists of six chapters including Introduction, Literature Review, Methodology, Project Implementation, Result and Discussion and last chapter is Conclusion.

Chapter 1 is briefly explaining introduction of background study of the related subject towards this project. Besides, this chapter also consist problem statement, research objective, research scope, research result expectation and thesis structure. Research objective are derived from problem statement and expected to be achieved at the end of this project. Research scope and research schedule is to highlight the scope of this project and to ensure this project is on the right track per schedule stated.

Chapter 2 is a list of literature review for this project. Literature review is a source of research article and journal that being used to give more understanding about related topic. This chapter is important as it is to ensure this project is possible to be done and to avoid any duplication of previous work (research gap). Besides, this chapter act as knowledge resource that help to do improvement, tips, proof of concept based on previous research. This is able to help to increase success rate for this project.

Chapter 3 is the chapter that explained methodology that being used to develop this project. Methodology are one of essential element in every project as it to ensure the project is properly plan and can be execute smoothly. In this chapter also explained the framework that being used in this project.

Chapter 4 is project implementation and development. In this chapter, the approach used is being explained in detail. Besides, the design and the functionalities of the approach also are highlighted. This chapter provides overall and process flow chart for this project. All the detail per the implementation of the approach also can be found in this chapter.

Chapter 5 is an explaining the result. In this chapter, all the result and finding related to this project will be provided here. An evaluation of the result and the discussion are explained in this chapter.

Chapter 6 is the chapter of conclusion for this project. It consists the advantage and limitation for this project. Besides, there are also suggested future enhancements that can be done. This chapter also concludes the whole project, result and the achievement while doing this project.

REFERENCES

[1] T. Jagatic, N. Johnson, M. Jakobsson, and T. Jagatif, “Social phishing,” Commun. ACM, vol. 50, no. 10, pp. 94–100, 2007.

[2] C. Grier, K. Thomas, V. Paxson, and M. Zhang, “@spam: The underground on 140 characters or less,” in Proc. ACM Conf. Comput.Commun. Security, 2010, pp. 27–37.

[3] (2011). Fox news’s hacked twitter feed declares Obama dead [Online]. Available: http://www.guardian.co.uk/news/blog/ 2011/jul/04/fox-news-hacked-twitter-obama-dead

[4] Bloomberg. (2013). AP Twitter account hacked in market-moving attack [Online]. Available: http://www.bloomberg.com/news/articles/2013-04-23/dow-jones-drops-recovers-after-false-reporton-ap-twitter-page

[5] (2013) [Online]. Available: http://theonion.github.io/blog/2013/05/08/how-the-syrian-electronic-army- hacked-the-onion/

[6] (2014). Skype twitter account hacked, anti-microsoft status retweeted more than 8,000 times [Online]. Available: http://www.theverge.com/2014/1/1/5264540/skype-twitter-facebookblog accounts-hacked

[7] Ruan, X., et al., Profiling Online Social Behaviors for Compromised Account Detection Information Forensics and Security, IEEE Transactions on, 2016. 11(1): p. 176-187

[8] B. Viswanath et al., “Towards detecting anomalous user behavior in online social networks,” in Proc. 23rd USENIX Secur. Symp., Santiago, CA, USA, pp. 223–238, 2014

[9] B. Viswanath, M. A. Bashir, M. Crovella, S. Guha, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, “Towards detecting anomalous user behavior in online social networks,” in Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14). San Diego, CA: USENIX Association, 2014, pp. 223–238.

[10] N. Z. Gong, M. Frank, and P. Mittal, “Sybilbelief: A semi-supervised learning approach for structure-based sybil detection,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, 2014.

[11] Hua, W.Z., Yanqing. Threshold and Associative Based Classification for Social Spam Profile Detection on Twitter. in Semantics, Knowledge and Grids (SKG), 2013 Ninth International Conference on. 2013.Beijing: IEEE.

[12] Lee, K.C., James Webb, Steve. Uncovering social spammers: social honeypots+ machine learning. in the 33rd international ACM SIGIR conference on Research and development in information retrieval. 2010. New York, USA: ACM.

[13] Cao, C.C., James. Behavioral detection of spam URL sharing: Posting patterns versus click patterns. in Advances in Social Networks Analysis and Mining (ASONAM), 2014 IEEE/ACM International Conference on. 2014. Beijing: IEEE.

[14] “Longest path problem,” 2014 [Online]. Available: http://en.wikipedia.org/wiki/Longest_path_problem

[15] K. Singh, S. Bhola, W. Lee, xbook: redesigning privacy control in social networking platforms, in: Proceedings of the 18th Usenix Security Symposium, 2009.

[16] "List of Common Malware Types," For17seconds, [Online]. Available: http://www.malwaretruth.com/the-list-of-malware-types/. [Accessed 24 July 2015].

[17] J. Chen, M. H. Alalfi, T. R. Dean, and Y. Zou, “Detecting android malware using clone detection,” J. Comput. Sci. Technol., vol. 30, no. 5, pp. 942–956, 2015.

[18] D. J. J. T. SUFATRIO, T.-W. CHUA, and V. L. L. THING, “Securing Android: A Survey, Taxonomy, and Challenges,” May 2015.

[19] B. Reaves, J. Bowers, S. A. Gorski III, O. Anise, R. Bobhate, R. Cho, H. Das, S. Hussain, H. Karachiwala, N. Scaife, B. Wright, K. Butler, W. Enck, and

P. Traynor, “&ast;droid: Assessment and evaluation of android application analysis tools,” CSUR, vol. 49, no. 3, pp. 55:1–55:30, Oct. 2016.

[20] D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, and K. Rieck, “Drebin: Effective and Explainable Detection of Android Malware in Your Pocket,” in NDSS, 2014.

[21] V. Avdiienko, K. Kuznetsov, A. Gorla, and A. Zeller, “Mining Apps for Abnormal Usage of Sensitive Data,” in ICSE, 2015.

[22] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. Le Traon, D. Octeau, and P. McDaniel, “FlowDroid: Precise Context, Flow, Field, Objectsensitive and Lifecycle-aware Taint Analysis for Android Apps,” in PLDI, 2014,

pp. 259–269.

[23] L. Li, A. Bartel, T. F. Bissyandé, J. Klein, Y. L. Traon, S. Arzt, S. Rasthofer, E. Bodden, D. Octeau, and P. McDaniel, “IccTA: Detecting Inter-Component Privacy Leaks in Android Apps,” in ICSE, 2015.

[24] W. Yang, X. Xiao, B. Andow, S. Li, T. Xie, and W. Enck, “AppContext: Differentiating Malicious and Benign Mobile App Behavior Under Contexts,” in ICSE, 2014.

[25] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, “TaintDroid: An Information-flow Tracking System for Realtime Privacy Monitoring on Smartphones,” in OSDI, Berkeley, CA, USA, 2010, pp. 1–6.

[26] A. R. Beresford, A. Rice, N. Skehin, and R. Sohan, “MockDroid: Trading Privacy for Application Functionality on Smartphones,” in HotMobile, 2011, pp. 49–54.

[27] O. Tripp and J. Rubin, “A Bayesian Approach to Privacy Enforcement in Smartphones,” in USENIX Security, 2014, pp. 175–190.

[28] P. Bielik, V. Raychev, and M. Vechev, “Scalable Race Detection for Android Applications,” in OOPSLA, 2015, pp. 332–348.

[29] H. Tang, G. Wu, J. Wei, and H. Zhong, “Generating Test Cases to Expose Concurrency Bugs in Android Applications,” in ASE, 2016, pp. 648–653.

[30] Guang Gong, “Fuzzing Android System Services by Binder Call to Escalate Privilege,” in BlackHat USA 2015, 2015.

[31] H. Ye, S. Cheng, L. Zhang, and F. Jiang, “Droidfuzzer: Fuzzing the android apps with intent-filter tag,” in MoMM, 2013, pp. 68:68–68:74.

[32] W. Choi, G. Necula, and K. Sen, “Guided GUI Testing of Android Apps with Minimal Restart and Approximate Learning,” in OOPSLA, 2013, pp. 623–640.

[33] X. Jiang and X. Zhu. veye: behavioral footprinting for self-propagating worm detection and profiling. Knowledge and information systems, 18(2):231–262, 2009.

[34] Juniper. Third annual mobile threats report.

[35] J. O. Kephart and W. C. Arnold. Automatic extraction of computer virus signatures. In 4th virus bulletin international conference, pages 178–184, 1994.

[36] A. P. Felt, H. J. Wang, A. Moshchuk, S. Hanna, and E. Chin, “Permission Re-Delegation: Attacks and Defenses,” in USENIX Security, 2011.

[37] J. Sahs and L. Khan, “A Machine Learning Approach to Android Malware Detection,” in EISIC, 2012, pp. 141–147.

[38] N. Peiravian and X. Zhu, “Machine Learning for Android Malware Detection Using Permission and API Calls,” in ICTAI, 2013, pp. 300–305.

[39] D. Octeau, P. McDaniel, S. Jha, A. Bartel, E. Bodden, J. Klein, and Y. Le Traon, “Effective Inter-component Communication Mapping in Android with Epicc: An Essential Step Towards Holistic Security Analysis,” in USENIX Security, 2013, pp. 543–558.

[40] M. I. Gordon, D. Kim, J. H. Perkins, L. Gilham, N. Nguyen, and M. C. Rinard, “Information Flow Analysis of Android Applications in DroidSafe,” in NDSS, 2015.