Asian Journal of Applied Science and Technology (AJAST)
(Open Access Quarterly International Journal) Volume 2, Issue 2, Pages 137-142, April-June 2018

Monet: A user Oriented Behaviour based Malware variants detection based system for Android

Ms.D.Thamarai Selvi

Assistant Professor, Department of Computer Science and Engineering, National Engineering College, Kovilpatti, India. Email: dts-cse@nec.edu.in

Article Received: 24 January 2018 *Article Accepted: 27 February 2018* *Article Published: 08 April 2018*

ABSTRACT

Last years malware for smart phones has rocketed. Market operators face the challenge of keeping their stores free from malicious apps, a task that has become increasingly complex as malware developers are using advanced techniques to defeat malware detection tools. One such technique commonly observed in recent malware samples consists of hiding and clarifying modules containing malicious functionality in places that static analysis tools (e.g., within data objects). In this paper, we describe MONET, a dynamic analysis approach for detecting such hidden or clarified malware components distributed as parts of an app package. The key idea in MONET consists of analyzing the behavioral differences between the original app and a number of automatically versions of it, where a number of faults have been carefully injected. Observable differences in terms of activities that appear or vanish in the modified app are recorded, and the resulting differential signature is clarified through a pattern-matching process driven by rules that relate different types of hidden functionalities with patterns found in the signature. The extensive experimental results obtained by testing MONET over relevant apps and malware samples support the quality and viability of our proposal.

Keyword: Malware detection, dynamic analysis.

1. INTRODUCTION

The popularity and advanced functionality of mobile devices has made them attractive targets for malicious and intrusive applications (apps). Although strong security measures are in place for most mobile systems, the area where these systems often fail is the reliance on the user to make decisions that impact the security of a device. As our prime example, Android relies on users to understand the permissions that an app is requesting and to base the installation decision on the list of permissions. Previous research has shown that this reliance on users is ineffective, as most users do not understand or consider the permission information. We propose a solution that leverages a method to assign a risk score to each app and display a summary of that information to users. Results from four experiments are reported in which we examine the effects of introducing summary risk information and how best to convey such information to a user. Our results show that the inclusion of risk-score information has significant positive effects in the selection process and can also lead to more curiosity about security-related information.

2. RELATED WORK

According to their survey, it was reported that over 98% of new malware samples are in fact derivatives (or variants) from existing malware families. These malware variants use more sophisticated techniques like dynamic code loading, manifest cheating, string and call graph obfuscation to hide themselves from existing detection systems. Although these techniques can help malware to hide their malicious logic, we observe that the "runtime behaviors" of malware's core functionalities, such as unauthorized subscription of premium services or privilege escalation at runtime, remain unchanged. The runtime behaviors of a new malware variant and its earlier generation are usually very similar. A detection system based on runtime behaviors of malware will be able to detect most malware and their variants more reliably. In addition, the static structures of the malware are often similar within a

malware family. With this observation, we present the design and implementation of Monet, an Android malware detection system that combines "static logic structures" and "dynamic runtime information".

They have displayed Monet, a structure for malware investigation in light of the thought of differential blame examination. They have depicted its engineering and star vided a formal model of differential blame examination. Also, they have displayed an open-source model usage of ALTERDROID with a flexible outline that can be the reason for further research here. Differential blame examination in the route actualized by ALTERDROID is an intense and novel element investigation system that can distinguish conceivably noxious components covered up inside an application bundle.

They have concentrated on the intriguing application situation, which is portrayed by two procedures attempting to impart outside their sandboxes for noxious purposes, for example, for delicate information exfiltration. Two recognition strategies have been produced, requiring the arrangement of relapse and classification issues. To check their adequacy, they have executed seven nearby secretive channels on the Android stage, and they have played out a trial estimation and location crusade. The acquired outcomes demonstrate that both techniques are portrayed by a decent discovery execution and can be utilized as a precise IDS programming on a present day cell phone to uncover the nearness of perils abusing data stowing away.

Every one of the calculations was connected utilizing their default parameters in Weka for binarized traits and ostensible class so as to acquire a model in light of a metalearner. The accuracy of every individual calculation was taken as the principle trademark keeping in mind the end goal to pick the best mix of choices. The element determination was made utilizing ChiSquare and Relief demonstrating that it is not an applicable exercise since similar outcomes were gotten when no element choice was performed.

They displayed Apposcopy, a static investigation approach for recognizing malware in the versatile applications biological community. Apposcopy performs profound static investigation to concentrate information flow and control-flow properties of Android applications and utilizations these outcomes to recognize whether a given application has a place with a known malware family. Their analyses demonstrate that Apposcopy can distinguish malware with high exactness and that its marks are flexible to different program confusions.

3. PROPOSED METHODOLOGY

We propose the addition of a summary risk rating for each app. A summary risk rating enables easy risk comparisons among apps that provide similar functionalities. We believe that one reason why current permission information is often ignored by users is that it is presented in a "standalone" fashion and in a way that requires a lot of technical knowledge and time to distill useful information, making comparison across apps difficult. An important feature of the mobile app ecosystem is that users often have choices and alternatives when choosing a mobile app. If a user knows that one app is significantly riskier than another but provides the same or similar

functionality, then this fact may cause the user to choose the less risky one. This will in turn provide incentives for developers to better follow the least-privilege principle and request only necessary permissions.A summary risk rating also enables proactive risk communication (e.g., when the user searches for apps) so that users can take this information into the decision process. This is in contrast to the current reactive approach, where often times the user sees the permission/risk information of an app as a final warning only after the user has made the decision to choose the app. Our hypothesis is that when a summary risk rating is presented in a user-friendly fashion, it will encourage users to choose apps with lower risk. The user sees the permission/risk information of an app as a final warning only after the user has made the decision to choose the app. An effective risk communication approach for Android could provide communication approach for Android could provide.

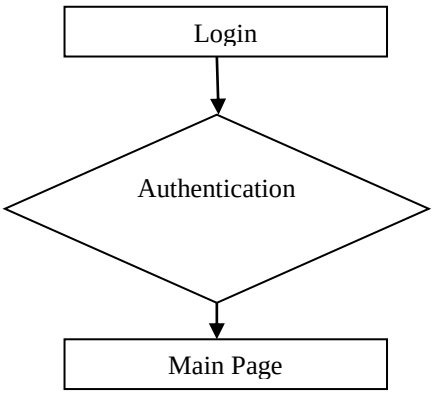

Fig 1: System flow

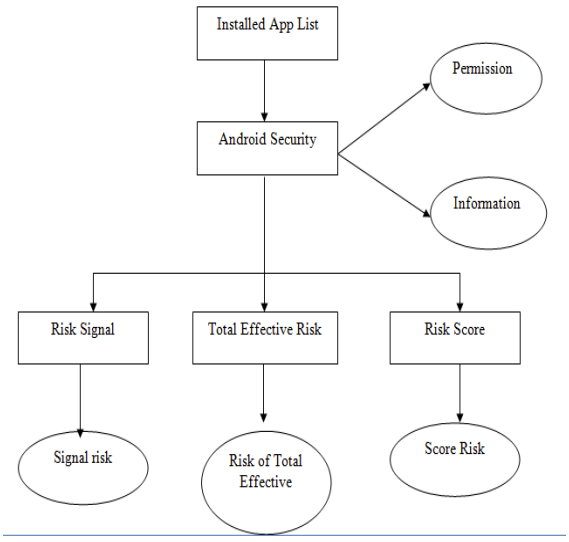

Fig 2: Data flow

4. CONCLUSION AND FUTURE ENHANCEMENT

The results from four user studies validated our hypothesis that when risk ranking is presented in a user-friendly fashion, e.g., translated into categorical values and presented early in the selection process, it will lead users to select apps with lower risk. The majority of participants preferred to have such a risk metric in Google Play Store.

We expect that adding a summary risk metric would cause positive changes in the app ecosystem. When users prefer lower-risk apps, developers will have incentives to better follow the least-privilege principle and request only necessary permissions. It is also possible that the introduction of this risk score will cause more users to pay for low risk apps. Thus, this creates an incentive for developers to create lower risk apps that do not contain invasive ad networks and in general over-request permissions. Our studies are not the last word on the question of how to best present risk information. For example, we have also not examined how the risk score interacts with other factors to affect a users choice, such as user ratings in the natural setting and whether an app is free or not. Also of interest is how users behave when choosing among a list of search results (as opposed to choosing between two options). These topics are important ones for future research.

A summary risk rating enables easy risk comparisons among apps that provide similar functionalities. We believe that one reason why current permission information is often ignored by users is that it is presented in a "standalone" fashion and in a way that requires a lot of technical knowledge and time to distill useful information, making comparison across apps difficult. An important feature of the mobile app ecosystem is that users often have choices and alternatives when choosing a mobile app. If a user knows that one app is significantly riskier than another but provides the same or similar functionality, then this fact may cause the user to choose the less risky one. This will in turn provide incentives for developers to better follow the least-privilege principle and request only necessary permissions.

REFERENCES

[1] Adnan Ibrahim, AfhalParavath, Aswin P. K., Shijin Mohammed Iqbal and ShaeezUsman Abdulla, "GSM Based Digital Door Lock Security System," IEEE International Conference on Power, Instrumentation, Control and Computing (PICC), vol.15, pp.4673-8072, 2015.

[2] Muthukumaran. N and Ravi. R, 'Hardware Implementation of Architecture Techniques for Fast Efficient loss less Image Compression System', Wireless Personal Communications, Volume. 90, No. 3, pp. 1291-1315, October 2016, SPRINGER.

[3] Muthukumaran. N and Ravi. R, 'The Performance Analysis of Fast Efficient Lossless Satellite Image Compression and Decompression for Wavelet Based Algorithm', Wireless Personal Communications, Volume. 81, No. 2, pp. 839-859, March 2015, SPRINGER.

[4] Muthukumaran. N and Ravi. R, 'VLSI Implementations of Compressive Image Acquisition using Block Based Compression Algorithm', The International Arab Journal of Information Technology, vol. 12, no. 4, pp. 333-339, July 2015.

[5] Muthukumaran. N and Ravi. R, 'Simulation Based VLSI Implementation of Fast Efficient Lossless Image Compression System using Simplified Adjusted Binary Code & Golumb Rice Code', World Academy of Science, Engineering and Technology, Volume. 8, No. 9, pp.1603-1606, 2014.

[6] Ruban Kingston. M,Muthukumaran. and N, Ravi. R, 'A Novel Scheme of CMOS VCO Design with reduce number of Transistors using 180nm CAD Tool', International Journal of Applied Engineering Research, Volume. 10, No. 14, pp. 11934-11938, 2015.

[7] Alfredo de Santis, Aniello Castiglione, and Umberto Ferraro Petrillo,"An Extensible Framework for Efficient Secure SMS," International Conference on Complex, Intelligent and Software Intensive Systems, pp.843-850, 2010.

[8] Arun Cyril Jose, Reza Malekian and Ning Ye, "Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home," IEEE.Translations on Consumer Electronics, vol. 4, pp.5776-5787, 2016.

[9] Gerard Rushingabigwi, Liguo Sun, Godfrey Lugoloobi and Frank Mwezi, "An Electric Circuits Remote Switching System based on GSM Radio Network," International Journal of Research in Engineering and Technology, vol.3, no.11, pp. 2321- 4708, 2014.

[10] Taewan Kim, Hakjoon Lee, and Yunmo Chung, "Advanced Universal Remote Controller for Home Automation and Security," IEEE Transactions on Consumer Electronics, vol. 56, No. 4., pp. 2537-2542, 2010.

[11] Muthukumaran. N and Ravi. R, 'Design and analysis of VLSI based FELICS Algorithm for lossless Image Compression', International Journal of Advanced Research in Technology, Vol. 2, No. 3, pp. 115-119, March 2012.

[12] Manoj Kumar. B and Muthukumaran. N, 'Design of Low power high Speed CASCADED Double Tail Comparator', International Journal of Advanced Research in Biology Engineering Science and Technology, Vol. 2, No. 4, pp.18-22, June 2016.

[13] N. Muthukumaran, 'Analyzing Throughput of MANET with Reduced Packet Loss', Wireless Personal Communications, Vol. 97, No. 1, pp. 565-578, November 2017, SPRINGER.

[14] P.Venkateswari, E.Jebitha Steffy, Dr. N. Muthukumaran, 'License Plate cognizance by Ocular Character Perception', International Research Journal of Engineering and Technology, Vol. 5, No. 2, pp. 536-542, February 2018.

[15] N. Muthukumaran, Mrs R.Sonya, Dr.Rajashekhara and Chitra V, 'Computation of Optimum ATC Using Generator Participation Factor in Deregulated System', International Journal of Advanced Research Trends in Engineering and Technology, Vol. 4, No. 1, pp. 8-11, January 2017.

[16] Keziah. J, Muthukumaran. N, 'Design of K Band Transmitting Antenna for Harbor Surveillance Radar Application', International Journal on Applications in Electrical and Electronics Engineering, Vol. 2, No. 5, pp. 16-20, May 2016.

[17] Akhil. M.S and Muthukumaran. N, 'Design of Optimizing Adders for Low Power Digital Signal Processing', International Journal of Engineering Research and Applications, Vol. 5, pp. 59-65, March 2014.

[18] Muthukumaran. N and Ravi. R, 'Quad Tree Decomposition based Analysis of Compressed Image Data Communication for Lossy and Lossless using WSN', World Academy of Science, Engineering and Technology, Volume. 8, No. 9, pp. 1543-1549, 2014.

[19] Marvin Mark. M and Muthukumaran. N, 'High Throughput in MANET using relay algorithm and rebroadcast probability', International Journal of Engineering Research and Applications, Vol. 5, pp. 66-71, March 2014.

[20] Gooli Rajasekhara Reddy and Imthiazunnisa Begum, "Design and Implementation of Anti-Theft ATM Machine Using Raspberry PI," International Journal & Magazine of Engineering, Technology, Management and Research, vol. 2, no. 11, pp.680-683, 2015.

[21] JayashriBangali and ArvindShaligram, "Design and Implementation of Security Systems for Smart Home based on GSM technology," International Journal of Smart Home., vol.7, No.6, pp.201-208, 2013.