International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 6 – MAY 2018.

ANDROID BASED SYSTEM FOR CAMERA BASED ATTACKS

Nagendra K M[#1], SanjeevNaik L[#2], Hemanth Kumar G[#3], Dhruva Kumar H[#4] and B.S Jayasri[*5]

[#] *U.G.Students, Department of Computer Science and Engineering, The National Institute of Engineering, Mysuru, Karnataka, India*

[*] *Associate Professor, Department of Computer Science and Engineering, the National Institute of Engineering, Mysuru, Karnataka, India*

***Abstract*— Android user square measure perpetually vulnerable by An increasing range of malicious applications (Apps), generically known as malware. Malware constitutes a heavy threat to user privacy, money, device and file integrity. During this proposal we tend to note that by learning of their actions will classify malware into a little range of behavioral categories, every of that performs a restricted set of misbehaviors that characterize them. These mishaviors will be outlined by observance options happiness to completely different robot levels. Here we tend to square measure presenting Multi Level Anomaly Detector for robot Malware (MADAM), a unique host-based malware detection system for robot devices. MADAM detects and effectively blocks quite malicious apps, that come back form with un informed features while execution**

***Index Terms*— Mobile Security, App Monitoring, Malware Detection, Server Monitoring.**

I. INTRODUCTION

Smart phones and tablets became very in style within the last years. At the tip of 2014, the amount of active mobile devices worldwide was nearly seven billions, and in developed nations the quantitative relation between mobile devices and other people is calculable as a hundred and twenty.8%. Given their massive distribution, and also their capabilities, within the last 2 years mobile devices have became the most target for attackers. Android, the open supply operative system (OS) introduced by Google, has presently the biggest market share, that is bigger than eightieth. attributable to the openness and recognition, mechanical man is that the main target of attacks against mobile devices (98.5%), with over one million of malicious apps presently out there within the wild. Malicious apps (generically referred to as malware) represent the most vector for security attacks against mobile devices. Disguised as traditional and helpful apps, they hide treacherous code that performs actions within the background that threatens the user privacy, the device integrity, or maybe user's credit. Some common samples of attacks performed by mechanical man malicious apps area unit stealing contacts, login credentials, text messages, or maliciously subscribing the user to expensive premium services. what is more, of these misbehaviors are often performed on mechanical man devices while not the user noticing them (or once it's too late). it's been recently reported that almost hour of existing malware send concealed premium rate SMS messages. Most of those behaviors area unitexhibited by a class of apps referred to as Trojanized that may be found in on-line marketplaces not controlled by Google. However, additionally Google Play, the official marketplace for mechanical man apps, has hosted apps that are found to be malicious2. at the side of the immense increase of mechanical man malware, many security solutions are planned by the analysis community, spanning from static or dynamic analysis of apps, to applying security policies implementing information security, to run-time social control. However, these solutions still gift important drawbacks. specifically, they're attack-spe cific, i.e. they typically specialise in and tackle one reasonably security attack, e.g. privacy unseaworthy, or privilege increase (jail-breaking). Moreover, these frameworks usually need a custom OS. except these accidental security solutions, in a trial to limit the set of (dangerous) operations that AN app will perform, mechanical man has introduced its native security mechanisms within the style of permissions and apps isolation. These 2 mechanisms, severally, enforce access management to security important resources and operations, ANd avoid that an app will interfere with the execution of another one. However, each permissions and isolation mechanisms have shown weaknesses.

II. RELATED WORK

Y. Zhou and X. Jiang et al.[1]

The popularity and adoption of smart phones has greatly stimulated the spread of mobile malware, especially on the popular platforms such as Android. In light of their rapid growth, there is a pressing need to develop effective solutions. However, author defense capability is largely constrained by the limited understanding of these emerging mobile malware and the lack of timely access to related samples. In this paper, they focuses on the Android platform and aim to systematize or characterize existing Android malware.

N. Xu et al.[2] they investigate video-based vulnerabilities in 3G Smartphones. Particularly, they designs a new video-based spyware, called Stealthy Video Capturer (SVC). SVC can secretly record video information for the third party, greatly compromising Smartphone users' privacy.

F. Maggi, et al.[3] The pervasiveness of mobile devices increases the risk of exposing sensitive information on the go. In this paper, they arise his concern by presenting an automatic attack against modern touchscreen keyboards. they demonstrates the attack against the Apple iPhone - 2010's most popular touchscreen device - although it can be adapted to other devices (e.g., Android) that employ similar key-magnifying keyboards. their attacks processes the stream of frames from a video camera (e.g., surveillance or portable camera) and recognizes keystrokes online, in a fraction of the time needed to perform the same task by direct observation or offline analysis of a recorded video, which can be unfeasible for large amount of data.

III. PROBLEM STATEMENT

Along with the large increase of golem malware, many security solutions are planned by the analysis community, spanning from static or dynamic analysis of apps, to applying security policies implementing information security, to runE-time social control. However, these solutions still gift vital drawbacks. TaintDroid may be a security framework for golem devices that tracks data flow to avoid malicious stealing of sensitive data. Alterdroid may be a tool that compares the variations in behavior between an imaginative app and mechanically generated version that contain modifications (faults) to notice hidden malware, like in footage.

IV. PROPOSED SYSTEM

In this paper we have a tendency to gift a completely unique multi-level and behavior based mostly, malware detector for mechanical man devices referred to as MADAM (Multi-Level Anomaly Detector for mechanical man Malware). specially, to observe app misbehaviors, MADAM monitors the device actions, its interaction with the user and therefore the running apps, by retrieving 5 teams of options at four totally different levels of abstraction, specifically the kernel level, application-level, user-level and package-level. for a few teams of options MADAM applies AN anomaly based mostly approach, for alternative teams it implements a signature based mostly approach that considers activity patterns that we've derived from familiar malware misbehaviors. In fact, MADAM has been designed to observe malicious activity patterns extracted from many classes of malware. This multi-level activity analysis permits MADAM to observe misbehaviors typical of just about all malware which may be found within the wild. MADAM conjointly has shown economical detection capabilities because it introduces AN one.4% performance overhead and a forty five battery depletion. Finally, MADAM is usable as a result of it each needs little-to-none user interaction and doesn't impact the user expertise thanks to its potency.

V. OBJECTIVES AND METHODOLOGY

A. *Objectives*

- The projected system monitors 5 teams of automaton options, among that system calls (type and amount) globally issued on the device, the protection relevant API calls, and therefore the user activity, to find uncommon user and device activity patterns; to the current finish, it exploits 2 cooperating proximity-based classifiers to find and alert anomalies.
- The projected system intercepts and blocks dangerous actions by detective work specific activity patterns that take under consideration a group of famous security hazard for the user and therefore the device.
- When each time a brand new app is put in, MADAM assesses its security risk by analyzing the requested permissions and name information, like user scores and transfer variety, and it inserts the app in an exceedingly suspicious list if evaluated as risky.

B. *Methodology*

MADAM DETECTION ALGORITHM is the algorithms to detect the malwares, here we detail how MADAM exploits the cooperation of the architectural components and the retrieved features to detect a misbehavior. In particular, the Per-App Monitor and Global Monitor exploit two distinct sets of features to detect different misbehaviors, known (mis)behavioral patterns and anomalies. Moreover, they also cooperate to identify more complex misbehaviors whose detection needs the analysis of features from both components. Once the misbehavior has been detected, security is enforced by the User Interface & Prevention module, which stops the misbehavior, notifies the user and removes the malicious app. Moreover the App Evaluator reduces the likelihood of false alarms, focusing the attention of MADAM on only those apps which effectively bring a risk.
.

VI. CONCLUSION

Starting from the tip of 2011, attackers have increased their efforts toward mechanical man smartphones and tablets, manufacturing and distributing many thousands of malicious apps. These apps threaten the user knowledge privacy, cash and device integrity, and square measure tough to sight since they apparently behave as real apps transfer no hurt. This paper proposes MADAM, a multi-level host-based malware detector for mechanical man devices. By analyzing and correlating many options at four completely different mechanical man levels, MADAM is in a position to sight misbehaviors from malware activity categories that take into account a hundred twenty five existing malware families, that cover most of the noted malware. To the simplest of our data, MADAM is that the 1st system that aims at sleuthing and stopping at

run-time any reasonably malware, while not that specialize in a particular security threat, employing a behavior-based and multi-level approach. Not solely the accuracy of the runtime detection of MADAM is incredibly high, however it additionally achieves low performance (1.4%) and energy overhead (4%).

REFERENCES

[1] Y. Zhou and X. Jiang, "Dissecting Android Malware:Characterization and Evolution," IEEE Symp. Security and Privacy 2012, 2012, pp. 95–109.
[2] R. Schlegel et al., "Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones," NDSS, 2011, pp. 17–33.
[3] N. Xu et al., "Stealthy Video Capturer: A New Video-Based Spyware in 3g Smartphones," Proc. 2nd ACM Conf. Wireless Network Security, 2009, pp. 69–78.
[4] F. Maggi, et al.,"A Fast Eavesdropping Attack against Touchscreens," 7th Int'l. Conf.Info. Assurance and Security, 2011, pp. 320–25.
[5] R. Raguram et al., "ispy: Automatic Reconstruction of Typed Input from Compromising Reflections," Proc. 18th ACM Conf. Computer and Commun. Security,2011, pp. 527–36.
[6] "Android-eye," https://github.com/Teaonly/android-eye, 2012.
[7] "Nanohttpd," https://github.com/NanoHttpd/nanohttpd.
[8] A. P. Felt and D. Wagner, "Phishing on Mobile Devices,"Proc. WEB 2.0 Security and Privacy, 2011.
[9] D. Li, D. Winfield, and D. Parkhurst, "Starburst: A Hybrid Algorithm for Video-Based Eye Tracking Combining Feature-Based and Model-Based Approaches," IEEE Computer Soc. Conf. Computer Vision and Pattern Recognition — Workshops, 2005, p. 79.
[10] P. Aldrian, "Fast Eyetracking," http://www.mathworks. com/matlabcentral /fileexchange/25056-fast-eyetracking, 2009.