Usage Patterns Based Security Attacks for Smart Devices

Soumya Kanti Datta, Christian Bonnet and Navid Nikaein, *Members, IEEE*
Mobile Communication Department, EURECOM, France
Emails: {dattas, bonnet, nikaeinn}@eurecom.fr

Abstract—Smart devices are increasingly becoming part and parcel of daily life and as well as becoming the center of attraction for security attacks. This paper introduces a novel malware which exploits the usage patterns of smart devices and launches malicious attacks. A useful Android application is developed which aims to provide user-specific power saving profiles by analyzing individual usage patterns. The application collects various usage information including running applications, battery level and status, brightness level, status of wireless networks and amount of data transfer. These informations are analyzed at a remote server to generate usage patterns and personalized power saving solutions. Since the application requires access to wide range of information from the smart devices, the application is examined for potential malicious exploitation. The malicious functionalities are well hidden in the application and can be triggered by hidden commands sent as a part of the power saving profiles from the remote server. As the malware takes advantage of individual usage patterns, it is relatively difficult to detect it. Possible attacks on smart device resources have been mentioned in details. Effective countermeasures are being developed and implemented to detect and erase such malwares. Research directions for the countermeasures are still open.

Index Terms — Android; Countermeasures; Malware; Power saving profile; Smart device; Usage pattern.

I. Introduction

Now-a-days, mobile malwares are on the rise especially for Android platform since it is open source and there is no application screening process. Google depends on the end users or researchers to report the malicious activities of applications. For this reason the privacy and security threats on Android platform are significant. Smartphone users typically download apps from online app store offered by Google, Samsung etc. The attackers have various ways to distribute various types of malwares [4], [5]. In repackaging attack, popular applications are repackaged with malicious content. Update attack releases a malware as an updated version of an application. User with automatic update feature on in the devices will be automatically affected. Several such malwares has been identified by security researchers around the globe which call for better ways of identifying mobile malwares and development of malware detecting and removing applications.

In this paper, we focus on usage pattern based malware attacks on Android powered smart devices. We have developed an application which records usage information and transmits them to a remote server which generates personalized power saving profiles and sends them back to the devices. Our research showed that a great deal of private information can be obtained if the application has declared necessary permissions. While we developed a benign application with a legitimate goal, but the same concept can be used to exploit the smart devices and make them the center of malicious attacks. As a proof-of-concept, we introduced malicious codes into the application and have launched attacks by exploiting the usage pattern of the device. When a malware is aware of the usage pattern it can modify its behavior to efficiently hide the malicious activities of users. For example, the application can (i) connect to remote command and control server during the interval when there is maximum network usage, (ii) send, receive and delete SMS, (iii) build a location profile compromising location privacy and (iv) perform operations that cost money to the users. Distribution of such applications is also explained.

Rest of the paper is organized as follows. Section II describes the procedure of usage pattern and power saving profile generation and summarizes the Android application named ‘Power Monitor’ with malicious code. Section III describes how usage pattern is exploited to launch attacks while Section IV discusses countermeasures. Section V concludes the paper with future research directions.

II. Power Monitor Android Application

A. Usage pattern and power saving profile generation

Several prior researches have been carried out in usage pattern generation and identifying its diversity [6] [7] [8]. In our research, we have significantly extended the approach by collecting exhaustive information from the smart devices. An Android application named Power Monitor is developed to gather informations about (i) running Android applications, (ii) battery status (AC/USB charging or USB charging) and battery level, (iii) contextual information like date, time and coarse location, (iv) brightness level and screen time out value, total interaction time with the smart device, (v) status of network technologies and amount of Wi-Fi, 3G and 4G data transfer, (vi) load on CPU and its operating frequency. The complete list of the monitored features can be found at [1].

These collected informations are collected and processed at a remote server to derive usage patterns. Each pattern is characterized by spatial and temporal context and reveals enormous usage behaviors like choice of applications during that time, location, battery behaviors, amount of network data transfer and more. Such behaviors are further processed by another algorithm to develop personalized power saving profiles. They are pushed to corresponding mobile devices and on being intelligently activated, reduces the overall power consumption. The algorithms running in the remote server can be ported to the application itself [2].

B. Malicious power monitor

As the proof-of-concept, several malicious parts have been inserted among the modules of the application. Power Monitor initially runs for seven days to gather usage behavior. After that the power saving profiles are received. The malicious commands are embedded as a part of the received profiles. The remote server in this case acts as a command and control (C&C) server. Sending commands over SMS or IRC channel is quite common as mean to launch attacks. But in this case, the profiles for power saving are carrying the commands for the same. This is a new way of communication between the C&C server and the mobile botnet (which in this case is the mobile device running malicious version Power Monitor). Since the remote server has the knowledge about the usage pattern of the device, several stealthy attacks can be launch. This generates an efficient malware which evades detection by humans and mobile anti-malware applications.

C. Inserting malicious codes into power monitor

Since the application has access to very high number of smart device features, the malicious codes can be repackaged into the application. In this case, the "apk" file of Power Monitor is reverse engineered to obtain the source code and then malicious parts are inserted. Then the malware is released. Another way is to launch an update attack. Here a developer can himself add malicious parts and release the application as an updated version of Power Monitor. Smart device users with automatic update switched on will be infected when the application is downloaded. Also a similar application can be developed by anyone.

III. Attacks Exploiting Usage Pattern

Usage pattern reveals how the smart devices are being used in day-to-day basis. This section gives a detailed overview of how the usage pattern is exploited to mount attacks on the smart devices.

A. Attack on CPU and battery resources

The usage patterns reveal the time duration in everyday for which the CPU operates at maximum or very high frequency due to much computational load. One of the power saving profiles generated for those patterns contain malicious command to launch computationally complex operations (e.g. mining Bitcoin) [9]. It drives up the load on CPU which is forced to operate on higher frequency. This in turn consumes more battery, thereby reducing battery life instead of reducing battery consumption. This is an attack on the CPU and battery resources of Android powered devices and is quite difficult to spot as it happens once in a while. The remaining profiles aim at reducing unnecessary applications. This frees up the load on CPU, lowers operating frequency and saves battery. Since the attack is performed when there is maximum CPU load, it makes detection tough even using behavioral analysis.

B. Draining network data transfer limits

The time intervals during which there is maximum network usage can also be known from the usage patterns. Normally the corresponding power saving profiles set maximum limit for network usage for the time duration. But the C&C server can also generate a profile which commands the application to increase the network usage manifold. It can be detected from the application that whether the user is connected to 3G network or Wi-Fi. Generally the amount of data plan for 3G network is fixed. This malicious application drives up the network usage over 3G by uploading and downloading high volume contents. This will affect users who use 3G network all the time and finish the quota of 3G usage. As a result it will lead to increased financial expenditure and battery draining very quickly. Such scenario demonstrates an attack on hardware resources of the device as well as financial loss of user. Since the attack is launched less frequently and that too during the time when network usage is quite high, it is most likely to be ignored by the user and anti-malware applications. This makes malware stealthy.

C. Dissipating power at display hardware

The brightness level and screen time out value can be obtained from the display module of Power Monitor [1]. The usage patterns identify the time intervals which correspond to maximum user-interaction with device (e.g. during playing games or watching movies). If the brightness level and screen time out value are quite high, then the power dissipation of display hardware also drives up. The corresponding power-saving profiles are supposed to tone down these two settings. Similar to the previous two cases, one malicious profile could keep the brightness at maximum level which would drain battery very fast. This is also an attack on the hardware resource.

D. Information leak and financial loss using SMS

The popularity of instant messaging applications (e.g. WhatsApp, Viber) reduced the usage of SMS. This has in turn increased the possibilities of SMS based attacks. The C&C server can analyze the usage information to learn about devices which does not send SMS. Those devices can be used to send SMS to premium numbers. Power Monitor having access to read, write and delete SMS, can launch such attack. Android 4.4 fixed this issue where only one system SMS application can operate on SMS. But the issue remains unaddressed in previous versions which are vulnerable to such attack. In order to make it stealthy, Power Monitor launches such attacks when there device is in silent mode and the SMS is deleted soon after it is sent to remove any trace or feedback to the users. Same method can be used to steal SMS sent from financial institutions. This violates privacy as well as leads to financial loss for the user.

E. Additional attacks

Additional attacks that can be launched are as below.

- The application can potentially take screenshots from the mobile devices. They can be further processed to identify user id and password for various accounts [3].
- Instead of downloading a power saving profile, another malware from 3rd party server can be downloaded. The malicious software in Power Monitor can activate it to infect the mobile as botnets.
- It is possible to deduce when the user is travelling abroad using the Android APIs. The malware can automatically trigger the 3G network when travelling abroad which costs the user financially.

F. Impacts of the malware

If such malware infects a mobile device, there will be severe consequences. It could not only have high impact on the hardware resources of the devices, but also lead to financial loss and compromise of privacy. The degree of the impact could be determined by how much overall system is compromised.

IV. Countermeasures

Developing countermeasures for such stealthy and intelligent malware is challenging. The malware has been tested with several popular anti-malware applications and the former has not been detected once. Although the research on the countermeasures is on-going, we would like to briefly discuss the following two approaches –

A. Dynamic Analysis

It is a behaviour based analysis of Android applications. It is performed by installing and running the application in a controlled environment (e.g. Sandbox) whiles the actions, API calls and behaviour are monitored and analysed [14]. Author Egele provided a comprehensive analysis of automated dynamic malware analysing techniques and tools [10]. The advantage of this process is that it is immune to polymorphic viruses which evade static analysis successfully. A similar tool is CrowdDroid which could be used to detect the presence of the malware discussed in the paper [11].

B. Anomaly Detection

This technique takes recourse to machine learning algorithms to learn behaviour of applications and then can classify them as known or new malware. Author Shabtai et al proposed “AndroMaly”, a similar tool which continuously monitors the smart devices and the events generated [12]. They are intelligently examined using machine learning algorithms to flag applications as normal or malicious. Researchers have developed VirusMeter which identifies malwares by analysing power consumption of applications [13].

V. Conclusion

This paper introduces a novel malware which operates based on individual usage patterns of the smart devices. As a proof-of-concept, malicious codes are attached to Power Monitor which collects usage information to propose power saving profiles to the users. The remote server in this case can act as a C&C server. It is discussed that direct attacks can be launched on hardware resources like CPU, battery and display hardware. As a consequence, the battery dies very quickly forcing users to charge the device very frequently. More attack scenarios include 3G network usage, SMS, other malware download and screenshot based information leakage. These malicious behaviours are closed tied up with actual usage patterns of devices and are performed less frequently. Thus the malware becomes stealthy and difficult to detect by human or anti-malware applications. Further research is being carried out to develop novel algorithms to detect and remove such malwares from Android powered devices.

Acknowledgment

The authors would like to thank the consortium of the French research project Smart 4G Tablet Pole SCS.

References

[1] S. K. Datta, C. Bonnet and N. Nikaein, "Personalized power saving profiles generation analyzing smart device usage patterns," 7th IFIP Wireless and Mobile Networking Conference (WMNC), 20-22 May 2014.

[2] S. K. Datta, C. Bonnet and N. Nikaein, "Power monitor v2: Novel power saving Android application," Consumer Electronics (ISCE), 17th IEEE International Symposium on Consumer Electronics (ISCE), pp. 253-254, 3-6 June 2013.

[3] C.C. Lin, H. Li, X. Zhou and X.F. Wang, “Screenmilker: How to milk your Android screen for secrets,” 21st Annual Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, February 23-26, 2014.

[4] Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner, “A survey of mobile malware in the wild,” Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (SPSM '11). ACM, New York, NY, USA, 3-14.

[5] Yajin Zhou; Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution," *IEEE Symposium on Security and Privacy (SP),* pp. 95-109, 20-23 May 2012.

[6] J.M. Kang, S. Seo and J. Hong. “Usage pattern analysis of smartphones.” In 13th Asia-Pacific Network Operations and Management Symposium, 2011, pp. 1-8.

[7] Q. Xu, J. Erman, A. Gerber, Z. Mao, J. Pang, S. Venkataraman. “Identifying diverse usage behaviors of smartphone apps.” In Proc. of ACM SIGCOMM conference on Internet Measurement Conference, 2011, pp. 329 – 344.

[8] H. Falaki, D. Lymberopoulos, R. Mahajan, R. Govindan, S. Kandula, and D. Estrin. Diversity in Smartphone Usage.In *Proc. ACM MOBISYS*, 2010.

[9] http://threatpost.com/google-removes-bitcoin-mining-android-malware-from-play [accessed on 17-Jun-14].

[10] Egele, Manuel et al. "A survey on automated dynamic malware analysis techniques and tools." ACM Computing Surveys (CSUR) 44.2 (2012): 6.

[11] Burguera, Iker, Urko Zurutuza, and Simin Nadjm-Tehrani. "Crowdroid: behavior-based malware detection system for android." Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices 17 Oct. 2011: 15-26.

[12] Shabtai, Asaf et al. "“Andromaly”: a behavioral malware detection framework for android devices." Journal of Intelligent Information Systems 38.1 (2012): 161-190.

[13] Liu, Lei et al. "Virusmeter: Preventing your cellphone from spies." Recent Advances in Intrusion Detection 1 Jan. 2009: 244-264.

[14] Blasing, Thomas et al. "An android application sandbox system for suspicious software detection." Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on 19 Oct. 2010: 55-62.