Mobile Malware Threats and Defenses for Homeland Security

Seung-Hyun Seo, Kangbin Yim, Ilsun You

Mobile Malware Threats and Defenses for Homeland Security

Seung-Hyun Seo[1], Kangbin Yim[2], and Ilsun You[3]

[1] Korea Information and Security Agency (KISA),
IT Venture Tower, 78 Garak, Songpa, Seoul, 138-950 Korea
seosh@ewhain.net
[2] Dept. of Information Security Engineering, Soonchunhyang University,
646 Eupnae, Shinchang, Asan, 336-745 Korea
yim@sch.ac.kr
[3] School of Information Science, Korean Bible University,
214-32 Dongil, Nowon, Seoul, 139-791 Korea
isyou@bible.ac.kr

Abstract. As the population of mobile users grows rapidly, mobile malware targeting smartphones are becoming a new threat to homeland security. So far, many kinds of malicious malwares including monetizing, stealing credentials or rooting have emerged. The latest mobile malwares are especially posing a serious threat to homeland security, because they can zombify phones to be controlled by their command and conquer servers. In this paper, we survey the threats and malicious behaviors of current mobile malwares. Then, we study the defense mechanisms of mobile malware and introduce a cooperative system for mobile security in South Korea. We also discuss the possible future of mobile malware and attack techniques.

1 Introduction

Recent large scale acts of terror such as the September 11, 2001 attacks have awakened national governments to the needs for supporting homeland security[10]. The original scope of homeland security includes: Emergency preparedness and response (for both terrorism and natural disasters), emergency management, Critical infrastructure and perimeter protection, Border security, Transportation security, Biodefense, etc. However, due to dramatic advances in IT technology, most *Supervisory Control And Data Acquistion* (SCADA)[18] systems and other official forms of networked computer system have been utilized over the last decade to control power grids, gas and oil distribution, water supply, telecommunications and etc. These computer-controlled and network-connected systems can be potential targets for hackers or hacking groups with malicious intent such as a crime or terrorist organization. As the government's

critical systems increasingly rely on IT technology, the threats of cyber attacks increase. So far, hackers have performed cyber attacks using information exploitation tools including computer viruses, malwares, worms, or eavesdropping sniffers.

As the population of smartphone users rapidly increases, hackers are converting their target systems of choice towards smartphones. Smartphones have a wide variety of feature-rich applications, commonly referred to as "apps". These apps include user-friendly content such as *Social Network Service* (SNS), navigation, banking and stock trading based on accessibility to public networks at anytime and anywhere.

Unlike computer applications, the smartphone platform vendors provide centralized marketplaces such as Apple's App Store or Google's Android Market in order to allow for smartphone users to conveniently browse and install their smartphone apps. However, some markets such as Google's Android market or the third-party app markets deal with illegitimately modified free versions of paid apps. This allows some apps to be posted without proper security checks, and allows the distribution of mobile malware at an increasing rate within these markets. Moreover, most users without security expertise install these apps unaware of its vulnerability. This has lead to the explosive growth of mobile malwares numbering at about 12,000 malicious apps in 2011 since the appearance of the mobile malware Cabir in 2004[13]. Especially, since the smartphones store sensitive data, if hackers infect a user's smartphone with mobile malware, they can steal sensitive data. If the infected smartphone were to be used at work in a company, hackers can obtain corporate secrets. Governments and public service offices which actively introduce the technology "Mobile Office" where employees are all equipped with smartphones connected to company servers and Intranet, have a greater security risk.

In order to prevent a cyberwar through mobile malware, *Korea Internet & Security Agency* (KISA)[15] of South Korea has organized a cooperative mobile security defense group. KISA also operates a hot line for response and defense against a mobile cyber war. In this paper, we first present the threats of mobile malware and attack scenarios against homeland security. Then, we show countermeasures for mobile security and introduce KISA's cooperative system against mobile cyber war. The remainder of this paper is organized as follows: In Section 2, we present threats of mobile malware. In Section 3, we present countermeasures for mobile security and introduce response and defense systems against mobile cyber war. We expect the possible future of mobile attack technique in Section 4 and conclude in Section 5.

2 Threats of Mobile Malware

In this section we first discuss about mobile malware threats and attack scenario for homeland security. Then, we give some examples of mobile malwares which recently emerged.

2.1 Threat Model and Infection Techniques

In order to obtain sensitive financial information, hackers have recently developed and spread mobile malwares. Mobile malwares achieve their malicious goals or profits by infecting the Operating System (OS) of smartphones. Usually, mobile malwares steal information stored on users' smartphone or send SMS to premium numbers for hackers' monetary profit. Stolen information can include *International Mobile Equipment Identity* (IMEI) numbers, *International Mobile Subscriber Identity* (IMSI) numbers, *Subscriber Identity Module* (SIM) serial number, user credentials for future misuse, contacts or *Global Positioning System* (GPS) location. Some mobile malware changes the infected phone into a bot that can be remotely controlled by the *Command and Conquer* (C&C) server.

We can categorize the infection techniques of mobile malware into Repackaging, Malvertising, and Browser Attacks[13]

- **Repackaging**: Repackaging is one of the most popular techniques to deceive users into installing malware. Hackers repackage legitimate apps after embedding malicious code and upload the modified apps to an unregulated market. These repackaged apps are distributed via the marketplace and downloaded by unwary users. The repackaged apps not only feature the same functionality as the original apps, but also include malicious code to collect sensitive information or to obtain monetary profit.
- **Malvertising**: Malvertising uses genuine looking advertisements that link back to fraudulent websites that can download malware to users' smartphones. Originally malvertising was one of the hacking techniques used on the Internet for many years. Now it is beginning to target mobile devices.
- **Browser Attacks**: There are two types of smartphone apps such as web apps and native apps. Mobile users fall for a hacker's browser-based malware, the hacker can trick a mobile user into visiting one of their URLs and essentially control any content they receive. This type of attack is far more dangerous and pervasive because it is not limited to strictly the unregulated Android marketplace.

2.2 Mobile Attack Scenarios against Homeland Security

Cyberthreat presents a real risk in loss of property and could threaten the lives of people. Recently, threats to industrial infrastructure networks such as SCADA systems have increased because of the lack of information security. So, in this section, we present the mobile attack scenarios against industrial SCADA systems using mobile malware.

The overview of an attack scenario is shown in Fig.1. It is supposed that employees can connect to a SCADA operating server using their smartphone. The employees can check the status of the SCADA system and control the SCADA server by inputting commands through their smartphone.

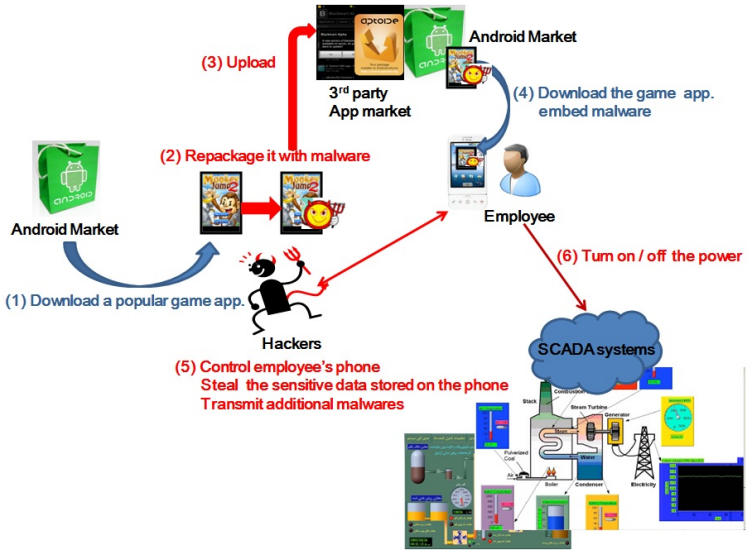

Fig. 1. Overview of Mobile Attack Scenario to the SCADA system

We also assume that hackers have repackaged a popular game app by including a malicious root exploit code and uploaded the repackaged game app both to the official Android market and unregulated third party market. Some of the employees download the repackaged apps from the market. Once these game apps are successfully installed, their malicious code can obtain root privileges while allowing hackers to control the infected smartphone. This attack can be divided into two types: (i) sending command to control the SCADA system and (ii) transmitting additional malware to steal sensitive data. For example, if hackers send the command

of "turn off the power" of a hypothetical SCADA system such as a national water utility, the employee's infected phone will shut off the power. If the SCADA system is compromised, a serious disaster could occur. If hackers send an additional malware which steals sensitive information, they could gather all the information about monitoring and controlling. Afterwards, they could launch more attacks towards the SCADA system using this stolen information. For instance, with stolen usernames and passwords, the hacker can access the remote network to gain access to the utilities network and cause the system to turn on and off repeatedly, until the water pump burned out.

2.3 Recent Mobile Malware

The mobile malware has many types of malicious behaviors such as leaking sensitive data or stealing credentials for unauthorized users, sending SMS to premium numbers for monetary loss, restricting device usage, mobile *Distributed Denial of Service* (DDoS) attacks and etc. These types of damages tend to appear in a complex manner in actual mobile malware incidents. Recent mobile malwares include root exploits(or jailbreak exploits) that gain extra privileges and execute commands from the C&C server. These mobile malwares can convert the infected smartphone into a bot. Once a exploit malware obtains root-level access, its powers are potentially unlimited. So, if these malwares are distributed and downloaded in the smartphone apps market place, hackers can remotely control users' smartphones. Root exploit malwares are especially dangerous compared to other types of malware.

DroidDream[3] in March, 2011, GingerMaster in August, 2011 and RootSmart in Feburary, 2012 are major root exploits malware for Android OS. DroidDream uses the "rageagainstthecage" and "exploid", and is functional for Android OS versions 2.2 and older. More than 50 apps have been found to contain DroidDream in the official Android Market. DroidDream can root a users phone and send sensitive information (IMEI and IMSI) from the phone to a remote server. DroidDream-infected phone can download additional malwares without a user's knowledge as well as open the phone up to control by hackers.

GingerMaster[8] and RootSmart[17] using "GingerBreak" run on Android OS versions 2.3 and older. Once the GingerMaster is installed, it creates a backdoor root shell and gains root privileges. It silently runs a service in the background which gathers information about the infected phone and transmits it to the C&C server. It is also able to download and install further malwares.

Unlike "GingerBreak", RootSmart does not directly include the root exploit inside the app. Instead, it dynamically fetches the GingerBreak root exploit from the C&C server and then executes it to escalate its privilege. RootSmart-infected phones register system-wide receivers and lie dormant until a system event activates it. After being activated, malicious actions run in the background. Then, RootSmart-infected phone connects to the C&C server with various information collected from the phone such as the Android OS version number, IMEI number, as well as the package name.

3 Countermeasures for Mobile Security

In this section, we present countermeasures for mobile security. Firstly, we discuss various detection mechanisms proposed in academic research and security mechanism for smartphone platform. Then, we introduce KISA's collaborative defense system against mobile cyber war.

3.1 Mobile Malware Detection Mechanism

Enck et al.[4] proposed TaintDroid system. It is an information flow tracking system for realtime privacy monitoring on smartphone and demonstrates potential privacy threats from third-party apps in Android platform. Chin et al.[2] proposed Comdroid system that analyzes the vulnerability in inter app communication in Android apps and finds a lot of exploitable vulnerability. Grace et al.[9] presented Woodpecker which exposes capability leaks on stock Android phones by analyzing preloaded apps in the phone firmware. Stowaway tool by Felt et al.[6] detects whether an app is overprivileged. Stowaway identifies the set of API calls used in an app and then maps it to the corresponding permissions. It examines 940 apps and finds that one-third apps are overprivileged.

Xie et al.[19] proposed pBMDS, a behavior-based malware detection system for cellphone devices. pBMDS utilized a probabilistic-based approach that correlates a user's input with system call events to detect abnormal behaviors in smartphones. Liu et al.[12] proposed virusMeter that detects mobile malware based on abnormal power consumption caused by mobile malware. Burguera et al.[1] presented Crowdroid that collects ststem calls of running apps on smartphones and applies clustering algorithms to differentiate between normal and malicious apps. Zhou et al.[20] proposed DroidMOSS that detects repackaged apps in unregulated third-party Android markets. Zhou et al.[21] presented DroidRanger that

performs offline analysis to detect mobile malware in current Android Markets.

3.2 Security Mechanism for Smartphone Platform

ScanDroid by Fuchs et al.[7] is an automated security certification of Android apps. It extracts app specific security specifications and applies data flow analysis for their consistency in the app code. Enck et al.[5] proposed Kirin that is lightweight mobile phone app certification. The goal of Kirin is to block the installation of potential unsafe apps if they have certain dangerous permission combination. Nauman et al.[14] revised the current Android framework. Apex by Nauman et al. provides fine-grained controls of resources accessed by third-party untrusted apps. L4Android by Lange et al.[11] isolates smartphone OS for different usage environments in different virtual machines.

3.3 KISA's Collaborative System

In South Korea, KISA has organized a cooperative mobile security defense group which is consisted of Korea government office, telecommunication company, security research institute, virus vaccine company, smartphone device vendors and etc. KISA has also organized the response and defense process for mobile security and operates a hot line for response and defense against a mobile cyber war. KISA's collaborative response and defense process for mobile security is divided into 5 steps: the monitoring, beginning response, analysis and information sharing, recovery, and improvement steps.

1) Monitoring step: In this step, each member of the cooperative mobile security defense group monitors infection routes of mobile malwares and gathers the information of mobile security issues and report of smartphone users' damages.
2) First action step: In this step, KISA blocks the distribution sites of mobile malwares to prevent additional damages and notifies the security threat of mobile malwares. Then, each member of the cooperative group collects the mobile malware sample.
3) Analysis and information sharing step: In this step, malware analysts of the cooperative group analyze the collected malware sample and grasp malicious functions of the malware. Then, they classify the types of the mobile accident and share the analysis information.

4) Recovery step: According to the analysis results, in this step, KISA blocks IP addresses of hacker's C&C servers and virus vaccine companies update vaccine patterns. Service centers of smartphone device vendors recover the users' infected smartphones.
5) Improvement step: In this step, the cooperative group analyzes the features and trends of mobile accidents and forecasts the possible future mobile security accidents. Then, they try to improve the response and defense process.

4 Future of Mobile Attacks and Defenses

Most malwares were usually organized in a static code frame and they could not change their patterns. Because these malwares were packaged with the whole body, it was deterministic whether they would have vulnerabilities or not and a security assessment outside the mobile platform was effective to find malicious patterns or behaviors and save its computing resources. Therefore, it was reasonable to prepare the lab-based security framework to analyze mobile apps. This type of framework may consist of massive multicore servers and provide an enough performance to analyze a number of malwares in parallel. Two common functions of this framework are abstracting signatures from new malwares through a dynamic analysis and scanning the existing malwares to find the signatures through a static analysis.

On the other hand, recent malwares have become facilitated with the ability to root the kernel and started placing a backdoor to download additional codes to extend themselves. Because the initial base code of these malwares may have no differences with that of normal apps, it is difficult for the lab-based framework to decide if they are malicious. The downloadable part can also make themselves highly polymorphic, thus confusing the security framework. Furthermore, they will incorporate the ability to hide themselves from or make immune to analysis by manipulating the kernel structures similarly to the self-defensive malwares in the stationary PC environment.

Due to these reasons, another security framework inside the mobile platform is getting focused as a counterpart of the lab-based framework to neutralize the self-defensive malwares. Because a sequence of a dynamic analysis and the signature-based vaccination are performed in a virtualized environment of the lab-based framework, the main objective of the mobile security framework is to disinfect the kernel. The objects targeted are various kernel structures such as the task structure, which

should be repeatedly investigated. The disinfection also should be performed out of the scheduling to make sure these kernel structures are exclusively accessed by the security framework.

5 Conclusion

Due to the advent of mobile device technology such as smartphones, the threat to homeland security using mobile malware is rapidly expanding. Motivated by this, we studied the possible securuty threats of mobile malwares as well as the infection techniques. In addition, we presented a feasible serious attack scenario against SCADA systems through mobile malware, and then focused on the existing countermeasures, one of which KISA has organized as a mobile cooperative security systems against mobile cyber war. Finally, we provided the possible attack techniques of mobile malwares in the future.

References

1. I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, Crowdroid:Behavior-Based Malware Detection System for Android, In Proceedings of the 1st Workshop on Security and Privacy in Smartphones and Mobile Devices, CCSSPSM 11, 2011.
2. E. Chin, A. P. Felt, K. Greenwood, and D. Wagner, Analyzing Inter-Application Communication in Android, In Proceedings of the 9th Annual Symposium on Network and Distributed System Security, MobiSys 2011, 2011.
3. DroidDream, http://blog.mylookout.com/blog/2011/03/01/security-alert-malware-found-in-official-android-market-droiddream/.
4. W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. Mc- Daniel, and A. N. Sheth, TaintDroid: An Information-Flow Tracking System for Realtime Privacy-Monitoring on Smartphones, In Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation, USENIX OSDI 10, 2010.
5. W. Enck, M. Ongtang, and P. McDaniel, On Lightweight Mobile Phone Application Certification, In Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS 09, 2009.
6. A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, Android Permissions Demystied, In Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 11, 2011.
7. A. Fuchs, A. Chaudhuri, and J. Foster, SCanDroid: Automated Security Certification of Android Applications, http://www.cs.umd.edu/avik/projects/scandroidascaa.
8. GingerMaster, http://www.csc.ncsu.edu/faculty/jiang/GingerMaster/.
9. M. Grace, Y. Zhou, Z. Wang, and X. Jiang, Systematic Detection of Capability Leaks in Stock Android Smartphones, In Proceedings of the 19th Annual Symposium on Network and Distributed System Security, NDSS 12, 2012.
10. Homeland Security, http://en.wikipedia.org/wiki/Homeland_security.

11. M. Lange, S. Liebergeld, A. Lackorzynski, A. Warg, and M. Peter, L4Android: A Generic Operating System Framework for Secure Smartphones, In Proceedings of the 1st Workshop on Security and Privacy in Smartphones and Mobile Devices, CCS-SPSM11, 2011.
12. L. Liu, G. Yan, X. Zhang, and S. Chen, VirusMeter: Preventing Your Cellphone from Spies, In Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection, RAID09, 2009.
13. McAfee, Threats Report: Second Quarter 2011, 2011.
14. M. Nauman, S. Khan, and X. Zhang, Apex: Extending Android Permission Model and Enforcement with User-Defined Runtime Constraints. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS 10, 2010.
15. KISA, Korea Internet and Security Agency, http://www.kisa.or.kr.
16. H. Kim, J. Smith, and K. G. Shin, Detecting Energy-Greedy Anomalies and Mobile Malware Variants, In Proceeding of the 6th International Conference on Mobile Systems, Applications, and Services, MobiSys 08, 2008.
17. RootSmart, http://www.csc.ncsu.edu/faculty/jiang/RootSmart/.
18. SCADA, Supervisory Control and Data Acquisition, http://en.wikipedia.org/wiki/SCADA.
19. L. Xie, X. Zhang, J.-P. Seifert, and S. Zhu, pBMDS: A Behavior-based Malware Detection System for Cellphone Devices, In Proceedings of the 3rd ACM conference on Wireless Network Security, WiSec 10, 2010.
20. W. Zhou, Y. Zhou, X. Jiang, and P. Ning, DroidMOSS: Detecting Repackaged Smartphone Applications in Third-Party AndroidMarketplaces, In Proceedings of the 2nd ACMConference on Data and Application Security and Privacy, CODASPY12, 2012.
21. 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 Proceedings of NDSS '12, 2012.