Malicious Android Applications in the Enterprise: What Do They Do and How Do We Fix It?

Xuetao Wei, Lorenzo Gomez, Iulian Neamtiu, Michalis Faloutsos

Department of Computer Science and Engineering, University of California, Riverside
{xwei, gomezl, neamtiu, michalis}@cs.ucr.edu

***Abstract*— Android applications are used in a variety of domains, including business, social, media, health, scientific, and even military. On one hand, enterprises can take advantage of the richness of Android applications to support their business needs. On the other hand, Android devices contain rich sensitive data—e.g., GPS location, photos, calendar, contacts, email, and files—which is critical to the enterprise and unauthorized access to this sensitive data can lead to serious security risks. In this paper, we describe the nature and sources of sensitive data, what malicious applications can do to the data, and possible enterprise solutions to secure the data and mitigate the security risks. The purpose of this paper is to raise employees' and enterprises' awareness and show that a suite of easy-to-implement measures can improve both employee and enterprise security.**

I. Introduction

Android applications (*apps*, for short) are well-known for their ability to exploit the rich information and capabilities of Android devices and the immense resources of the Internet, which have exciting potential for a variety of business, game, media, social, health, scientific, and military purposes. The main source of Android apps is the Android Market, which as of December 2011, lists more than 550,000 apps [4].

The danger lies in the usefulness combined with the ease of access of the apps, which leads most users to have a mixture of both personal and enterprise apps installed on the same device. As a consequence, the properties that give Android apps the potential to improve our lives, also pose a serious threat to enterprise privacy and security. Apps can collect sensitive data from the user (e.g., user names and passwords), access personal data stored on the device (e.g., calendar and contacts list), and use sensitive device capabilities (e.g., the GPS, camera, or microphone) [9], [8]. Moreover, Android hardware and software platforms are evolving rapidly and apps are being developed every day that use Android device's capabilities in new and unexpected ways.

In this paper, we first discuss the sensitive data on Android devices (Section II). Next, we reveal what malicious apps can do with this data (Section III). Aside from malicious apps, we show that there are security risks in benign apps (Section IV) as well. In Section V, we present the possible threats these apps pose to the enterprise, e.g., financial loss and loss of competitive advantage. Finally, to address potential problems brought by Android apps to the enterprise, we propose several approaches (Section VI).

	Premium Services			**Install New Apps**		**Data Exfiltration**				
	Phone calls	SMS messages		With intervention	Without intervention	Phone info	GPS location	SMS messages	External storage
DroidDream					✓	✓			
DroidDreamLight				✓		✓			
Zsone		✓						P	
Geinimi	✓	✓			✓	✓	P	P	P

TABLE I
MALICIOUS APP BEHAVIOR. 'P' INDICATES PERMISSION WAS GRANTED.

II. Security-sensitive Data on Android

Each Android device contains a wealth of security-sensitive information associated with the user's identification, whereabouts, and his/her official business in the enterprise. We now provide a brief overview of this information.

IMEI, IMSI, and phone number. The IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), and phone number are unique numbers that identify the physical device and the user's mobile subscription, respectively.

Contacts list. This list identifies all contacts which may include names, phone numbers, addresses, and emails.

Location. This information, provided by the GPS and the Network Location Provider, allows apps to determine the user's geographical location.

SMS messages. These include the private text, picture, and sound messages contained in the phone's message Inbox.

External SD card. The SD card (external storage) may contain a variety of personal files including photos, music, and documents. The card may also contain application-specific data.

Physical sensors. These sensors include the accelerometer, compass, light sensor, pressure sensor, proximity sensor, and temperature sensor. The sensor data is generated by hardware components directly measuring changes in the physical properties in the environment of Android devices.

III. What do Malicious Android Apps do?

We now proceed to presenting the various methods that malicious apps employ against users. Understanding these methods is particularly important for enterprises as the bring-your-own-device (BYOD) model gains more traction in the

enterprise [6]. Our characterization is based on a study we conducted on malware samples (malicious Android apps) [7].

A. Download and Install New Apps

When given Internet access permissions, malicious apps are able to download and install third-party apps in two ways: with and without user intervention. With user intervention, the malicious application will be able to download an application from an external site to the device. However, without gaining root (superuser) access to the phone, they are forced to install the covertly-downloaded app via the standard installer, which will prompt the user for authorization before continuing. For example, the malware DroidDreamLight is not able to gain root access and prompts the user when trying to install additional third-party apps.

When an app is able to gain root access to the phone, it connects to an external site, downloads an Android application install file (.apk), and installs the application onto the device without any notification or authorization from the user. The newly-installed application then shows up in the user's launch list (malware DroidDream and Geinimi had this capability). Downloading and installing new apps can be a serious threat against the enterprise, since the malware can analyze the enterprise environment and download specific apps to pose enterprise-specific, targeted threats.

Users have a hard time discerning between malicious and benign apps based solely on the app's name. Of the malicious apps we examined, all bore names of seemingly harmless tools and games, e.g., Scientific Calculator and Monkey Jump 2. Therefore, even if the user is prompted to install an app triggered by malware, the user could still believe it is safe to do so. To conclude, while installing third-party apps can seem more of an annoyance at first, it can lead to serious security threats, as explained in the following sections.

B. Monitoring and Exfiltration of Data

Once malicious apps make their way onto a device, they can monitor and send away certain categories of data, depending on the app's permission and control; this includes the security-sensitive data explained in Section II: phone information, contacts list, GPS location, SMS messages, and files stored on external storage. Although users may not be concerned much if their personal data is leaked, this issue is particular acute in enterprises, that stand more to lose from their data being exposed or leaked. Enterprise data on the device may be confidential and/or harmful to the enterprise if released into the wrong hands.

Using the IMEI, IMSI, and phone number, an app can identify the mobile phone down to the physical device and the subscriber. The data retrieved from the phone can then be sent away to external websites by the malicious app. These external sites could potentially build a blacklist of phone information to be sold to the highest bidder. This could be very dangerous to enterprises, because it could put employees at risk for future attacks against their devices.

Malicious apps that have access to SMS messages are able to read the message Inbox and send a log of the messages away to external websites. This could potentially be harmful if enterprise interactions are conducted via the messaging services of the phone. For example, if confidential information or orders are transmitted via SMS, this data can be harvested and exfiltrated from the phone.

Another dangerous ability of malicious apps is the power to access data stored on the phone's external storage. Most smartphones contain some sort of external storage in the form of flash cards such as SD cards. The data stored on these cards is dependent on the usage of the phone, but can contain user document files or saved settings of installed apps. Herein lies the biggest Android threat to enterprises: exfiltration of confidential files. If enterprise files are stored on the device, they are potentially available for extraction if the phone contains a malicious app with the capability to access external storage. This is a very startling possibility, given that it is very convenient to carry enterprise files on a phone, e.g., to permit working-on-the-go. All the malware categories we tested (DroidDream, DroidDreamLight, Zsone, and Geinimi) had the ability (permission granted) to extract at least one type of sensitive data.

C. Premium Services

Malicious apps can also incur charges when they have permission to make phone calls and send SMS messages. Those apps with the ability to make phone calls come bundled with a list of premium (1-900) numbers that charge the user per-phone call. The app can make these calls without the user opening the dial pad interface of the phone and can do so anytime the app is used on the phone.

Sending and receiving SMS messages is another way to accrue charges. The malicious apps can accomplish this in two ways, by either sending many SMS messages out from the phone or subscribing the phone to "premium" SMS services that charge the user a hefty per-message price. Once the phone is subscribed to a service, it may be difficult for the user to cancel the service even after they are aware of the intrusion.

The costs accumulated from the premium service charges are problematic for both personal and enterprise users, though they can be especially damaging to enterprises if the malware spreads to other phones within the enterprise. Among the malware categories we studied, Zsone and Geinimi have the capability to accrue such charges. We summarize the malicious behavior of each malware category in Table I.

IV. Are Benign Android apps Safe For Enterprises?

In this section, we show that even benign Android apps still pose risks and vulnerabilities.

A. Permission Abuse

In order to install an Android app, the user must grant certain permissions to the app. Permissions to access personal, location, and contact information are abused by most apps that request such permissions. In particular, apps constantly

gather personal data and send it to remote servers. Once the data is collected, using it for benign or malicious purposes is up to the discretion of the developer and the remote servers' administrators.

Even when apps do not have certain permissions, permission re-delegation (a more privileged app acting as a deputy) could let malicious apps seek permissions from other apps to access sensitive enterprise data, which could lead to a serious security risk [5].

B. Unencrypted Account Information

The account name and password combination is the most standard authentication approach to accessing personal sensitive data. Unfortunately, in benign apps such as LinkedIn, Foursquare, and Netflix, user names and passwords are stored in an unencrypted form on Android devices. The security situation becomes even worse if people use the same user name and passwords to manage their different apps. A hacker could use malicious apps to easily access the information of user accounts and passwords, then log into the user's apps to modify or steal sensitive enterprise data, which is a serious threat to enterprise security [2].

C. Preinstalled Apps

Even when users are judicious about the apps they install, pre-installed apps that ship with the phone can wreak havoc. For example, in a recent incident, users of certain HTC phones were exposed via the pre-installed app HTCLogger [3]. HTCLogger was designed to log device information for the development community in order to debug device-specific issues; as such, the app collects account names, call and SMS data, GPS location, etc. Unfortunately, the app stored the collected information without encrypting it and made it available to any application that had the Internet permission.

V. What is the Impact on the Enterprise?

Android devices are carried by users when they are at home or in the enterprise and are put to business and personal use in both environments. This mixed, personal/enterprise usage could raise security and privacy concerns due to the security-sensitive data available on the Android devices.

A. Loss of Privacy

When malicious apps are running on Android devices, they can track and leak personal information without notice or legal authorization. When provided with enough tracking information, hackers can infer the role and conduct of users, e.g., who the user is, what their position is, and when and where they conduct meetings. Even benign apps, when not used properly, could be used for malicious purposes, e.g., using the camera without permission to take a photo or record video in the enterprise. All these scenarios can lead to privacy leaks.

B. Enterprise Data Loss

Android devices often store sensitive enterprise information in the calendar, contact list, media library, etc. Sensitive enterprise data could include conference call numbers and passwords, passwords for enterprise logins, key codes for alarms and secure enterprise offices, employee names and phone numbers, sensitive audio or video content from senior management. All of this data can be obtained by malicious apps and sent off the devices, over the Internet, without the user's knowledge.

C. Data Integrity Loss

Malicious apps could easily delete or modify the user's enterprise data, e.g., official business documents, client contact methods and calendar entries, to break the integrity of enterprise data. The modified enterprise data could confuse employees of the enterprise, which could mar critical enterprise operations. This could lead to serious impairments to the functionality of enterprises.

D. Monetary Loss

As mentioned before, malicious apps could sign users up for premium-rate services, hence using such apps can have negative impacts: (1) financial loss due to charges and (2) time and money spent on remedial measures.

E. Loss of Competitive Advantage

The rich and sensitive data associated with enterprise apps can be modified or stolen by malicious apps in order to undermine a company's competitive advantage. For example, malicious apps could read the contact lists which includes many important, even confidential, official business emails, SMS messages between clients and the enterprise, and documents that include sensitive transaction records. When such information is exposed to competitors, the business vitality of the enterprise could be seriously damaged. Competitors could construct counter strategies based on the leaked confidential information to build a competitive edge against the exposed enterprise.

VI. What Can Enterprises Do?

With the security risks brought by using Android apps in enterprises, it is pressing for the research community to propose defensive strategies. In this section, we will discuss potential approaches to protect enterprise data resident on Android devices and mitigate the risks associated with using malicious Android apps.

A. Educating Users

Even though Android has a well-defined security model, problems can still arise if users are not well-informed about the risks posed by their devices. Educating the users is a simple and efficient way to provide a basic security background for Android users in the enterprise, e.g., only download apps from the official Android Market and don't jailbreak devices. Informing users how to install safe apps, what the important permissions are, and the consequences of granting permissions are, can go a long way. More importantly, once one user finds suspicious malicious behaviors of an application, they should report the problem to the security administrators in the enterprise as soon as possible. This would help the administrator distribute the alerts before others are affected by, or infected with the same malware.

B. Building An Enterprise Marketplace

Most apps are distributed via the official Android Market. However, the Market does not vouch for application security, hence enterprises cannot expect that arbitrary apps on the Market are safe [1]. For instance, hackers could possibly make a fake copy of their application with the exact same UI, while adding malware functions that run in the background of the app. In order to avoid such security risks, the enterprises can be more secure by building their own marketplaces. The advantages of building their own marketplaces are two-fold: (1) employees can easily and securely install the correct apps provided by the enterprise, and (2) the enterprise can remotely manage the apps on employees' devices. For example, if an app is found to have a security risk, the enterprise could push a security fix onto employees' devices before damage is done. If an enterprise doesn't have the capability to build and maintain its own market, they could affiliate their marketplace within the official Android Market.

C. Strict Enterprise Content Management Policy

Since the content of enterprise app data is critically important to enterprises, a strict framework of policies about its own enterprise content management should be specified. The enterprise should first identify what data should be considered as sensitive enterprise content. For example, files on the external storage, GPS location, or SMS messages should be secured. Further, the sensor data from the accelerometer, compass, light sensor could also be included into the enterprise content to prevent misuse. Then, the enterprise-sensitive content should be placed in a restricted storage on the Android device. Only the enterprise apps will have the rights to access the secured content. In other words, the enterprise content-blocks any access from non-enterprise apps. Furthermore, this policy framework has to differentiate between network destinations, i.e., enterprises should specify trusted outgoing destinations where enterprise data can be sent from the device.

D. User Monitoring

The enterprise could also implement a monitoring scheme for enterprise users with access to sensitive enterprise content. This would include monitoring on both the network and on the device. A log could be constructed to keep track of what the user and apps do within these two channels. An example of data to be collected could include a list of hosts that apps have interacted with when handling confidential data. A probing system can then parse the collected data and determine whether the data for each user is consistent with the policy in the enterprise's content management policy, mentioned above. Administrators could then separate suspicious users from critical assets of the enterprise.

E. User Profiling

We can not predict when Android devices will be used by someone other than the original owner in cases where the device is lent out or lost. One fundamental recommendation is to have the enterprise require that employees enable password-protected logins on their Android device. However, this simple and efficient method is ignored by most people, because it is inconvenient for users to unlock the phone between uses. A more integrated approach could involve creating an application profile of the enterprise apps based on the device owner's interactions with the application. For example, a profile could be built from patterns of the user's interaction with the GUI. By profiling the application's behavior in benign situations, a profile of safe use will be created. Therefore, in case the Android device is lost, an unfamiliar use pattern would be detected and the sensitive data can be protected or wiped.

F. Snapshotting Smartphone Software and Data

The enterprise should set up an incremental backup system to periodically snapshot each smartphone's software and data. That way, if a phone is infected or if malicious apps modify or delete sensitive data, users can revert to a pre-infection version stored in the backup system. The backup system can be set up in enterprise data centers, or in the Cloud.

VII. Conclusion

In this paper, we have presented the nature, sources, and implications of sensitive data on Android devices in enterprise settings. We have characterized malicious apps and the risks they pose to enterprises. We have also presented the security risks associated with benign Android apps. All these findings have confirmed that Android apps are posing potential threats to the security and privacy of enterprises. Finally, we have proposed several approaches for defending against security risks for enterprise and mitigating the consequences of smartphone-based security breaches.

Acknowledgements

We would like to thank Lookout Labs for providing the malicious applications to analyze. This work was supported in part by National Science Foundation awards CNS 1064646, CNS 1143627, by a Google Research Award, and by ARO CTA W911NF-09-2-0053.

References

[1] C. Albanesius. Google pulls more malware-infected apps from android market. *PC Magazine*, June 2011. http://www.pcmag.com/article2/0,2817,2386806,00.asp#fbid=bL8XwFNB1ic.

[2] Android Guys. Popular Android Apps Pose Security Risks for Users. http://www.androidguys.com/2011/06/09/popular-android-apps-pose-security-risks-users, June 2011.

[3] Android Police. Massive Security Vulnerability In HTC Android Devices. http://www.androidpolice.com/2011/10/01/massive-security-vulnerability-in-htc-android-devices, October 2011.

[4] Androlib. Number of New Applications in Android Market by month, December 2011. http://www.androlib.com/appstats.aspx.

[5] A.P. Felt, H. Wang, A.Moshchuk, S.Hanna, and E.Chin. Permission Re-Delegation: Attacks and Defenses. In *USENIX Security Symposium*, 2011.

[6] A.P.Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A Survey of Mobile Malware in the Wild . In *ACM SPSM*, 2011.

[7] L. Gomez and I. Neamtiu. A Characterization of Malicious Android Applications. Technical report, University of California, Riverside, August 2011. http://www.cs.ucr.edu/~neamtiu/pubs/MaliciousAppsTR.pdf.

[8] W. Enck. Defending Users Against Smartphone Apps: Techniques and Future Directions. In *ICISS*, 2011.

[9] 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*, 2010.