Journal of Advances and Scholarly Researches in Allied Education

Vol. VIII, Issue No. XVI, Oct-2014, ISSN 2230-7540

STUDY OF SECURITY AND PRIVACY ISSUES IN SMART PHONES

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

Journal of Advances and Scholarly Researches in Allied Education
Vol. VIII, Issue No. XVI, October-2014, ISSN 2230-7540

Study of Security and Privacy Issues in Smart Phones

Nadeem Khan

Researcher (Information Technology) Devi Ahilya University Indore, Madhya Pradesh, India

Abstract – With the advancement in cellular phone technologies and invention of better and smaller processors, battery and electronic displays. While phones have not been plagued with spywares and viruses like computers but with the myriad connectivity options as well as advent of high speed 3G and 4G networks, the threat cannot be ignored. While enabling interoperation with the internet brings tremendous opportunities in service creation and information access, the security threat of the Internet also dauntingly extends its reach. Users keep lots of important contacts and other private information. Native security like password protection had always existed but what about the naive users who did not set a password for efficiency and ease. Even if phone is password protected a hacker could easily switch memory cards and gain access to confidential data. Not only data but with GPS chips embedded in such phones, the whereabouts of the person are also exposed. Today's Smartphone operating systems frequently fail to provide users with adequate control over and visibility into how third-party applications use their private data .Malware on device can create number of risks which creates problem while connectivity because of security issues. Many honest end users are being successfully hacked on a regular basis. With this research paper I wish to delve into the different security issues that are currently plaguing the Smart Phones, the risk they are posing, as well as the manufacturers are using to handle them.

----------X----------

INTRODUCTION

Smart phones provide you with better processor and memory and it offers enhanced services functionality apart from usual ones like making calls. With the advent of better mobile processors that are not only powerful but also consume less battery has been responsible for the recent flood of Smartphones in the market. Smart phones usually have a complete operating system that allows installation and running of different applications.

Generally Smart phones offer a myriad connectivity options ranging from Bluetooth, GSM, CDMA toWi-Fi that allows easy access on the go. Smart phones boast of touchscreen or mini QWERTY keyboard or stylus for input. Integrated camera coupled with high resolution displays offers live video calling facilities also.

With the rising use of android phone, the security threat has also increased. Huge amounts of critical information and data are nowadays stored on phones and losing phones could lead to losses Smartphones can be subjected to various attack vectors, such as SMS, MMS, Bluetooth, Wi-Fi, Web browsing, applications and emails. Therefore, the standard malicious attacks for PCs (e.g., worms and Trojans) and other infection vectors (e.g. Web browsing, SMS, MMS) are all applicable to smartphones amounting to millions of dollars.

1. Evolution of Smart Phones Malware

Since 2004, malware has spread among smartphones and other mobile devices through wireless networks. In June 2004, the first known smartphone worm was discovered in the SymbianOS, named Cabir. It was propagated through Bluetooth as an infection vector. One of the best known local epid.

2. SMART PHONES MALWARE

There are many different types of malware that takes advantage of many ways to propagate and infect victims. Malware can infect targets by being bundled with other programs or attached as the macros of files. Others are installed by ex- ploiting a known vulnerability of a mobile platform, network device, or other software. For example, malware writers use the vulnerability of a browser, or a smartphone will be infected if the owner uses the smartphone to access a specific web site. However, the vast majority of malware is installed through some action from the user, such as clicking a MMS message or opening an email attachment or downloading an application from the Internet. Google Android Market Modern mobile devices run sophisticated OSs, such as Symbian,

Android, iOS, J2ME, and Windows Mobile. All of these confront similar risks as desktop computers do.

Symbian: Symbian is an open source OS designed for smartphones. With the launch of the Ericsson R380 in the year 2000, Symbian became the first modern mobile OS for smart- phones. From 2004 to 2006, Symbian was the platform frequently targeted by malware writers. Cabir was not only one of the first malware for Symbian, but also one of the first to use Bluetooth to propagate malware. This worm consists of a message that contains an application file, caribe sis, which disguises a security manager utility. If installed, the worm uses the device's native Bluetooth functionality to search for other Bluetooth-discoverable devices. The worm then attempts to send infected SIS files to the discovered devices as well. Mquito became the first Trojan for smartphones and was discovered in August 2004. This Trojan makes infected phones send SMS text messages to other phones resulting in charges to the smartphone owner.

Android: Android is a mobile OS based on a Linux-derived OS backed by Google, along with dominant hardware and software developers (such as Intel, HTC, ARM, Samsung, and Motorola), which form the Open Handset Alliance. An- droid was released on November 5th, 2007 and received praise from a number of developers upon its introduction. A steady rise in the number of threats targeting Android was observed during the first half of 2011. For example, Fakeplayer. A is a Trojan that affects smartphones run by Android. It sends certain SMS messages to specific numbers, which may lead to users being charged for transactions without the consent of the smartphone owner. Base Bridge B. is another Trojan affecting Android-based mobile devices. This Trojan steals sensitive data, sends it to a remote server, and may terminate certain applications.

IOS: IOS is Apple's mobile OS that was derived from Mac OS X. It was originally developed for iPhones, but now has been extended to support other devices, such as iPod Touch, iPad, and second-generation Apple TV. Since the release of iOS 2.0 on July 11th, 2008, it officially began to support third party applications. Ikee is the first self-propagating worm targeting Apple iPhones. This worm attacks only jail-broken iPhones using the installed SSH server and the default root password. Its most notable action involves changing the iPhones background wallpaper. Ikee.B is the second variant of the Ikee worm, and is the first Bonet with a clearly malicious attack. However, unlike iKee, Ikee.B includes command and control logic to render all infected iPhones under the control of a Botnet master.

2.1 Malware Classes

Malware is designed for either damaging or disrupting a computer system. This terminology is used to cover all hostile software, including virus, worm, Trojan, Spyware, backdoor, Rootkit and Botnet.

Virus: A type of malware that enters a computer system via the hardware or software without the user's knowledge, and then attaches itself to a program file. The virus then starts to duplicate itself and commits malicious tasks that it was programmed to do. The severity of viruses includes the effects of data or software damage and denial-of-service (DoS) attacks.

Worm: A type of malware that slips into computer systems without the owner's permission and operates without the owner's knowledge. Unlike viruses, which need human intervention to spread, worms can spread automatically from computer to computer. Worms can replicate themselves and send out hundreds or even thousands of copies from each infected computer, tapping into the user's email addresses to spread the infection. Worms can have a devastating impact on Internet traffic, web sites, and the user's own computer, which may be co-opted by the creator of worm. The infamous Blaster worm in November 2003 was brought to worldwide attention after its devastating impact.

Spyware: A type of malware that collects information for advertising purposes, usually for a secret a third party. The presence of spyware is typically hidden from users, and is difficult to detect. Spyware can obtain credit card numbers, passwords, and email addresses, and can also monitor a user's web activity, scan files, create pop-up ads, log keystrokes, or change the default page of web browsers. Spyware finds its way into computers as programs covertly bundled with downloaded software, through Peer-to-Peer (P2P) file sharing, or as a result of web browsing. For example, spyware with access to a video camera can record video and transmit it using either email or MMS, which enables malicious remote surveillance.

Trojan: A type of malware named after the wooden horse the Greeks used to infiltrate Troy.It is a harmful piece of software that appears legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can attack the host any number of times, from irritating users with popup windows or changing their desktop, to damaging the host by deleting files, stealing data, or activating and spreading other malware, such as viruses. Trojan is also known to create backdoors to provide malicious users access to the host. It is usually user-initiated and does not replicate

Rootkit: A special type of malware that hides itself, specific files and processes, and network links in the compromised devices. It achieves the above goals by loading a special driver program or by modifying the kernel of the OS.

Bonet: A type of malware that allows an attacker to remotely control a set of compromised devices. Attackers often use it to launch large scale network attacks, such as a distributed denial of service attack (DDoS), massive spam mail, or to collect privacy information that can be used for illegal purposes.

Nowadays, the number of mobile malware threats for smartphones has increased dramatically.

2.2 Infection Vectors

There are multiple infection vectors for delivering malicious content to Smartphones. In this survey, we classify infection vectors into four categories: SMS/MMS, Bluetooth, Internet access, and file duplication with USB.

(1) SMS/MMS Cellular services, such as short message service (SMS) and multimedia messaging service (MMS), can be used as attack vectors for smartphones. For example, SMS/MMS messages can be used to deliver malicious content and to maintain communication with an attacker. For example, ComWar is a worm which browses the host's phonebook and then spreads via SMS/MMS messages.

(2) Bluetooth is a short-range radio communication protocol that allows Bluetooth-enabled mobile devices (which could be mobile or stationary) within 10-100 meters to communicate with each other. Bluetooth-based attacks are a method used for device-to-device malware spreading. Once two Bluetooth- enabled devices are in range, the compromised device pairs with its target using default Bluetooth passwords. If the connection is established, the compromised device sends out malicious content. However, Bluetooth is a limited attack vector for injecting malicious content due to several security factors. First, mobile devices are not usually set in the discoverable state by default, and the period during which they can be discovered is limited. Second, the user has to confirm the file transfer and then the malware has to make itself part of the file exchanged via Bluetooth.

(3) Internet access Smartphones can access the Web using Wi-Fi networks or 3G networks, which allows users to use the most common Internet application services, such as surfing the web, sending or receiving emails with attachments, or downloading application software. Although such high speed Internet connections can provide many convenient services, they also expose smartphones to the same threats as personal computers (PCs). In addition, smartphones are constantly switched on, which increases the chance of a successful malicious attack, if they maintain a continuous connection to the Internet.

(4) File duplication with USB Apart from the aforementioned infection vectors, smart-phones could be compromised using other methods, e.g., use of USB. If the files used to synchronize smartphones were compromised, malware can also infect smartphones. As a result, attackers can access the host's private information and install malicious applications on the smartphone.

2.3 Risk of Malware

Once smartphones have been compromised by malware, it may cause interruption to the service of users, such as system damage, economic loss, information leakage, or disruption to a mobile network. We list more details of each category as follows.

(1) System damage

- Battery draining: Some malware commits their attack goal by continuously searching and infecting other phones (i.e., Cabir, Lasco, and Mabir), or continuously sending SMS or MMS messages (i.e., Red Browser). As a result, hosts quickly lose their battery power.
- Disabling system functions: Some malware can make the system unable to operate normally, such as Skulls. Some malware can even block calling functionality, for example, Locknut.
- Change system configurations: Some malware can change the background wallpaper on the device, such as Ikee.

(2) Economic loss

- Sending SMS or MMS messages to premium numbers: A successfully executed attack can force the compromised smartphone to send SMS or MMS messages to premium numbers, such as Mquito, which may cause financial loss to the smartphone owner.
- Dialing premium numbers: A successfully executed at- tack can force the compromised smartphone to dial premium numbers, such as Base Bridge, which may cause financial loss to the smartphone user.
- Deleting important data: Any data stored in the device's memory or on an SD card, e.g., documents, photos or videos, may be compromised and then be deleted by attackers.

(3) Information leakage

- Privacy breach: A successfully executed attack can also empower an attacker with the

ability to browse SMS or MMS messages, emails, call logs, and contact details from compromised smartphones.

- Remote surveillance: An attacker can turn an infected smartphone into a listening device by utilizing the voice recording hardware, and can access the camera of the infected smartphones to take photos or record video clips of the surroundings of the smartphone user.

- Stealing bank account information: Online banking is constantly under attack by using Trojans to steal pass- words, such as ZeuSMitMo.

(4) Disturbing mobile networks

- Denial-of-service (DoS): If compromised smartphones can secretly and continuously send SMS or MMS mes- sages or dial premium rate numbers. It can also result in DoS attacks by occupying network bandwidth. This is a conventional DoS attack, which is flooding-based so an attacker can generate high-rate, high-volume network traffic in order to deplete network resources.

- Signalling channel attack: This is a novel DoS attack and seeks to overload the control plane of a 3G wireless net- work using low-rate, low-volume attack traffic based on some of the aforementioned 3G-specific vulnerabilities. Unlike traditional DoS attacks that focus on the data plane, a signalling attack creates havoc in the signalling plane of a 3G network by repeatedly triggering radio channel allocations and revocations.

3. MAJOR SECURITY FLAWS & PRIVACY THREATS

Everyone has a right to personal data confidentiality. Gone are the days when phones were used merely for making and receiving calls. With Smartphones becoming common and replacing computers & laptops for daily use, the threat to privacy is increasing. The conveniences provided by a Smartphone are innumerable.

Location obtained by GPS installed in every handset allows consumer to update their locations on social networking sites, look for nearby restaurants and cinema halls, and look for friends that are around. Little is known by the user that this data is so crucial for spammers, who steal your location information and throw advertisements. Various cases have been registered where criminals have resorted to geo-location data to perform burglary and kidnapping.

Confidential Data might be stored by businessman, lawyers, etc. on the phone. SMSes, voicemails, photos, music, videos and other downloaded files usually contain lot of information and lure hackers like honey pot. We all are living in a world of Wikileaks and a stolen phone or laptop has often leaded to multimillion dollar losses, government fines and lawsuits.

Address book containing email, phone numbers, address, photo, etc. have always been the target of spyware. By exporting the contact details or modifying email address one can silently monitor the communications from an unsuspected user and steal it too.

Camera & Audio have been known to be tainted with and sent over internet to central server for extracting critical information which can range from interaction with phone banking to revealing of secrets.

Identifiers like SIM card identifiers (IMSI, ICC-ID), and device identifier (IMEI), phone number are very crucial data that could be misused to an unimaginable extent.

The security model in Smart Phones is considerably more locked down than other handset platforms. Each application runs in its own instance of the Dalvik virtual machine. Each instance of the Dalvik virtual machine represents a Linux kernel process; hence each instance is completely isolated from the other memory wise. As such it is not possible for an application to steal information from another running application.

Files and data held by an application are completely isolated from all other applications. This is enforced by the system by the use of the Linux kernel and traditional UNIX file permissions. For applications to access data from another application, it must first be exposed via a content provider and accessed by the message bus by sending “intents” between the two applications.

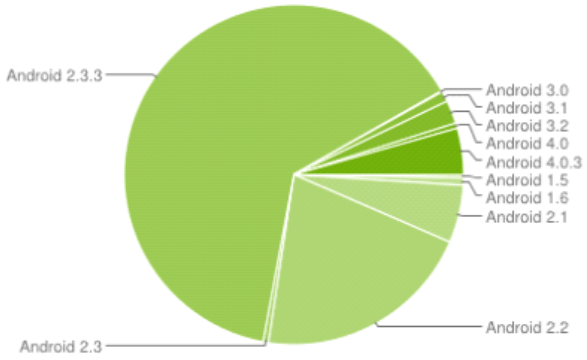
3.1 Malicious Apps

Malicious apps are the most common infection channel and are comparable to trepanised programs on desktop platforms. They provide high convenience for malware developers, as the Android Market and third party app markets potentially give access to all Android users. Malicious code can be packaged and redistributed with popular apps. Furthermore, users can choose to allow installation from websites, which can also be exploited by attackers.

3.2 Infection via Personal Computers

Due to a lack of remote exploits for the Android operating system and its security model, which successfully prevents vulnerable, compromised apps from modifying any operating system components, device to device infections are virtually impossible. This applies for all Android versions prior to Version 3.1., which features USB host mode. USB host mode can be used to infect other Android based

smartphones with USB debugging enabled. Versions prior to Version 3.1 account for around 90% of all Android devices as of May 2012 as shown by Figure



However, to achieve higher infection rates on smartphones, malware authors may turn to desktop computers for smartphone malware propagation in the future. This seems very likely, given the attractiveness of smartphones as a target for malware. Technically, desktop computer malware have to implement the Android Debug Bridge's protocol to install arbitrary software on any device with USB debugging activated.

Rooting To date, vulnerabilities are mainly exploited by users to root their phones, meaning to grant the user full administrative access to their smartphone. Such access is needed for various actions. This includes installation of apps in conflict with the Android security architecture or removing carrier branding, circumventing app or usage limitations (e.g., tethering), or even uninstalling provider installed spyware. An example of such spyware is Carrier IQ, which is deployed by carriers to retrieve detailed data on customer device usage behavior. It uses rootkit technology to keep its activities unnoticed by users. Furthermore, some users may wish to install modified operating systems on their devices, which is also only possible with privileged access. This usage model is not driven by a third party's malicious intent. However, rooting one's smartphone may introduce higher risks of successful malware infection. App markets preconfigured for rooted or modified operating systems are not well monitored and contain many trepanised apps. Furthermore, some modified operating systems are less well maintained than preinstalled ones. They also often provide facilities for any installed software to easily gain root privileges. In this case, malicious apps would no longer need to escalate their privileges themselves through vulnerability exploitation. Thus, rooting a smartphone may pose a high security risk.

3.3 Device to device Infection

As stated in autonomous device to device propagation is currently not possible. With Android versions 3.1 and 4.0, two major changes have been introduced which may serve for device to device propagation

USB host mode (Android 3.1) Android Beam (Android 4.0), an NFC (Near Field Communication) based file and data transmission system with a range of approximately 10 cm.

USB host mode is very likely to be usable for malware propagation. Similar to desktop computer propagation, an Android smartphone may use the Android Debug Bridge to push and install malicious apps to other devices with USB debugging enabled. This may happen both intentionally or unintentionally:

Targeted attacks may be conducted against single persons. A device owner only has to leave their device out of sight for a short moment, and an attacker close by may infect it through plugging a USB cable into it. This requires only few seconds. Unintended device to device infections may occur as well. Given an already infected device, propagation code may run invisibly in background, waiting for other Android devices to be plugged in. Once two devices are connected, the host mode capable device will imitate the Android Debug Bridge's protocol and infect the other device.

Android Beam is of limited utility, as it requires user interaction for installation. For example, a web link to a malicious app can be sent to another Android 4 device via Android Beam, but the user still has to click the link and confirm it. The limited physical distance reduces malware infection risks even further.

As USB host mode has only recently become available, device to device propagation has not yet been reported. However, Android 4 comes shipped with an adb server which allows remote access via shell on other connected Android devices. As a result, malware can use the pre supplied adb program to install apps on other devices. Any difficulties in implementing the adb protocol are thus eliminated. Facilities for device to device infections are provided by the Android operating system.

3.4 Privacy Issues and Classical Malware Threats

Information Leakage through Logging Service

The central Android logging service has proven to be a very rich resource for various personal information. Many apps tend to write status messages to the logging service containing parameters which disclose personal details of their device owners. For example, several GPS based apps were found to write the device's geocoordinatesto the logging service in regular intervals, thus providing full profiles on the device owner's movements to other apps installed. Some apps log web requests or other network communication. Thus, by only reading log files, much sensitive information can be gathered, depending on

the apps installed and their behavior regarding logging.

Online Banking

Online banking transactions are often confirmed and authenticated via the mTAN method. Since the abandonment of printed iTAN lists by many banks, popularity of this method is increasing rapidly, as it is considered easier by customers than TAN generators. In both cases – when a smartphone is only used to receive mTANs or when used to issue transactions as well – the user's bank account is put at high risks, if his device is compromised. On infected phones, login credentials for online banking portals entered by the device owner can be recorded and forwarded easily. This applies when a compromised smartphone is used for receiving mTANs and for issuing transactions, or even when used only to log in to the banking account to check its balance.

Only logging in once is sufficient for an attacker to withdraw all money from an mTAN protected bank account, as ordering a transaction and intercepting the mTAN text message is trivial. Under the Android operating system, an app can register to receive SMS messages before the phone's own messaging application through the RECEIVE_SMS permission. Even without pre-emptive interception, an attacker only would have to react quickly enough to confirm the transaction after parsing the respective SMS message via the READ_SMS permission.

Even when the smartphone is only used to receive mTANs, it may be used to withdraw money from the device owner's bank account under one of the following conditions:

Both desktop computer and smartphone of one person are under the same attacker's control. This scenario seems very likely in the future. A personal computer infected with any common malware can easily infect a plugged in smartphone with USB debugging enabled.

With the information found in a smartphone's messaging application, such as email and SMS messages, targeted phishing or social engineering attacks can be carried out easily. Due to the attacker's knowledge of the owner's communication, such attacks can be conducted in a very sophisticated and convincing way. Hence, infection of the user's desktop computer would not be necessary, compromisation of their smartphone suffices.

Contact Information, Location Data, Credentials and Private Details

Espionage, communication eavesdropping, blackmailing, botnet formation, collecting valid email addresses for spam mailing and recording of sensitive information such as login credentials or credit card data are just some of the classical applications of trojan software. All of these apply for mobile platforms as well. In some cases, they may even be more dangerous on mobile devices: Users are less cautious and store a lot of information and communication centrally. For convenience reasons, app credentials are retained unencrypted or only obfuscated. When encrypted, the corresponding key is usually saved in plain text .

4. CONCLUSION

The importance of Smart phones could be easily understood by the simple fact that for the first time, Smart phone sale exceeded computer & laptop sales. A smart phone has become an important part of our lives and the privacy & security of consumers should be the highest priority of developers as well as manufacturers. Only a few aspects and flaws have been discussed in this paper. And the fact that the flaws have not been discovered does not ensure that they do not exist. There could be several loopholes that are not known and the probability of their surfacing in near future is not ignorable.

Users/Consumers should also be made aware of the threat that lurks using Smart phones. The good old saying "There is no such thing as a free lunch" is apt here too. In present scenario, when even giants like Google are not able to check and curb from their respective App distribution channels (viz Android Market Place), users should take precautions before installing the next free & luring app, as it could well be a spyware. They should not blindly approve any sort of unknown application permission requests as going by the current trends, risk is very high.

The scope of this paper though was limited to smart phones; the generalization that could be inferred, applies to other players as well. Whether it is iPhone, RIM or Symbian, the threat to smartphone security is same. They also follow a similar system for developing and distributing smartphone applications.

It is high time for developers to refine the centralized approach of application distribution as well as analysis. A thorough research should be done before introducing any new OS update or patch. Customer/user security should be made the foremost priority of any manufacturer.

REFERENCE

Android Open Source Project (2013). Publishing on GooglePlay. http://developer.android.com/distribute/googleplay/publish/ preparing.html.

Android Open Source Project (2013). Security and permissions. http://developer.android.com/guide/topics/security/permissi ons.html.

Enck W., Octeau D., McDaniel P. and Chaudhuri S. (2011). A Study of Android Application

Security, The 20th USENIX conference on Security, pp. 21-21.

Guillaume Peersman, Srba Cvetkovic, Paul Griffiths, and Hugh Spear (June 2000). The Global System for Mobile Communications Short Message Service. IEEE Personal Communications Magazine.

K. Niinuma, U. Park, and A. Jain (2010). Soft biometric traits for continuous user authentication. IEEE Transactions on Information Forensics and Security.

Kaur S. and Kaur M. (2013). Review Paper on Implementing Security on Android Application, Journal of Environmental Sciences, Computer Science and Engineering & Technology, 2(3).

Polla M.L., Martinelli F., and Sgandurra D. (2013). A Survey on Security for Mobile Devices, Communications Surveys & Tutorials, IEEE, 15(1), pp. 446–471.

Powar S., Meshram B. B. (2013). Survey on Android Security Framework, International Journal of Engineering Research and Applications, 3(2).

S.J. Vaughan-Nichols (2003) OSs battle in the smart-phone market. IEEE Computer, 36(6).

Tesfay W.B., Booth T., and Andersson K. (2012). Reputation Based Security Model for Android Applications, Trust, Security and Privacy in Computing and Communications, IEEE Computer Society, pp. 896-901.