Mobile Security: An Analysis of Android and iOS

by

Team 27: Security Force

Alex Li
Derek Wilson
David West
David Johnson
Mentor - Ridhima

Mahajan http://securityforcei399.com

Abstract

Through research, it is clear that 3rd party applications are ineffective in protecting a user on each operating system due to the way each OS is set up. Due to this, it is primarily up to Apple and Android to provide virus fixes and protection when needed. Apple and Android offer two similar ways of combating attacks on their respective phones. Using cloud computing Android is able to run each program uploaded to Google Play. Although the specific means is unclear due to the closed source approach Apple uses, Apple also has means to scan and remove destructive programs. However, the permissions model that is in place for both iOS and Android is ignored due to vagueness in what programs are allowed to do if installed on a phone. This is the easiest way in which a mobile phone can be infected. This is especially true if the app is downloaded away from Apple's App Store, and the Google's Play Store.

Introduction

Team Security Force is formed with the purpose of finding, and evaluating research for our research question:

> "Compare and evaluate Android and iOS with respect to mobile security" such as Web-based attacks, Malware, Denial of resource and service, Data Integrity attacks and Social engineering

attacks, Study how these are addressed in Android and IOS."

The first goal is to find preliminary research on both Android and Apple's operating systems (OS). We used Google, Wikipedia, IUCAT, and other credible sources. To collaborate and compile all of our research we are using Google Drive. This decision allows us to update with each member being able to see changes in real time. It also syncs nicely with our website. Our goal with our research was to determine the steps each OS uses to prevent a mobile attack on their phones.

Background and Related Work

Our research began with the question why? Is this really something worth pursuing? Consider the research we found from the 2011 report Lookout provides every year.

> Mobile devices are the fastest growing consumer technology, with worldwide unit sales expected to increase from 300 million in 2010, to 650 million in 2012
>
> Mobile applications are likewise booming. In June 2011, for the first time ever people on average spent more time using mobile applications (81 minutes) than browsing the mobile web (74 minutes).
>
> While once limited to simple voice communication, the mobile device now enables us to also send text messages, access email, browse the Web, and even perform financial transactions. Even more significant, apps are turning the mobile device into a general-purpose computing platform. In just three short years since introducing the iPhone SDK in 2008, Apple boasts over 425,000 apps available for iOS devices. Seeing similarly explosive growth, the Android Market now contains over 200,000 apps after only a short period of time.
>
> As mobile devices grow in popularity, so do the incentives for attackers. Mobile malware, for example, is clearly on the rise, as attackers experiment with new business models by targeting mobile phones. Recently over 250,000 Android users were compromised in an unprecedented mobile attack when they downloaded malicious software disguised as legitimate applications from the Android Market
>
> The emergence of mobile payments is another key driver of mobile threats. The value of mobile payment transactions is projected to reach almost $630 billion by 2014, up from $170 billion in 2010. Vendors, retailers, merchants, content providers, mobile operators, and banks are all actively establishing new payment services. Mobile payments create an attractive target for attackers, as they allow direct monetization of attacks.
> In addition to financial information, mobile devices store tremendous amounts of personal and commercial data that may attract both targeted and mass-scale attacks.

With so many users using what are essentially pocket computers, we decided to focus more research on how a virus or an attack could occur on each OS. We needed to find how a phone can be attacked. This means more research on the different attacks. As with PCs, there are a variety of security threats that can affect mobile devices. We split mobile threats into several categories: application-based threats, web-based threats, network-based threats and physical threats. For the sake of brevity, this list is intended to be a general overview of the most important mobile threats, not an exhaustive treatment of all possible threats.

Application-Based Threats

Downloadable applications present many security issues on mobile devices, including both software specifically

designed to be malicious as well as software that can be exploited for malicious purposes. Application-based threats generally fit into one or more of the following categories:

Malware

Malware is software that is designed to engage in malicious behavior on a device. For example, malware can commonly perform actions without a user's knowledge, such as making charges to the user's phone bill, sending unsolicited messages to the user's contact list, or giving an attacker remote control over the device. Malware can also be used to steal personal information from a mobile device that could result in identity theft or financial fraud.

Spyware

Spyware is designed to collect or use data without a user's knowledge or approval. Data commonly targeted by spyware includes phone call history, text messages, location, browser history, contact list, email, and camera pictures. Spyware generally fits into two categories: it can be targeted, designed for surveillance over a particular person or organization, or untargeted, designed to gather data about a large group of people. Depending on how it is used, targeted spyware may or may not be considered malicious, such as in the case of a parent using a text messaging or location monitoring application on a child's phone.

Privacy

Privacy Threats may be caused by applications that are not necessarily malicious (though they may be), but gather or use more sensitive information (e.g., location, contact lists, personally identifiable information) than is necessary to perform their function or than a user is comfortable with.

Vulnerable Apps

Vulnerable Applications contain software vulnerabilities that can be exploited for malicious purposes. Such vulnerabilities can often allow an attacker to access sensitive information, perform undesirable actions, stop a service from functioning correctly, automatically download additional apps, or otherwise engage in undesirable behavior. Vulnerable applications are typically fixed by an update from the developer.

Web-based Threats

Because mobile devices are often constantly connected to the Internet and used to access web-based services, web-based threats that have historically been a problem for PCs also pose issues for mobile devices:

Phishing Scams

Phishing Scams use web pages or other user interfaces designed to trick a user into providing information such as account login information to a malicious party posing as a legitimate service. Attackers often use email, text messages, Facebook, and Twitter to send links to phishing sites.

Drive-by Downloads

Drive-By Downloads automatically begin downloading an application when a user visits a web page. In some cases, the user must take action to open the downloaded application, while in other cases the application can start automatically.

Browser Exploits

Browser exploits are designed to take advantage of vulnerabilities in a web browser or software that can be launched via a web browser such as a Flash player, PDF reader, or image viewer. Simply by visiting a web page, an unsuspecting user can trigger a browser exploit that can install malware or perform other actions on a device.

Network Threats

Mobile devices typically support cellular networks as well as local wireless networks. There are a number of threats that can affect these networks:

Network Exploits

Network exploits take advantage of software flaws in the mobile operating system or other software that operates on local (e.g., Bluetooth, Wi-Fi) or cellular (e.g., SMS, MMS) networks. Network exploits often do not require any user intervention, making them especially dangerous when used to automatically propagate malware.

Wi-fi Sniffing

Wi-Fi Sniffing can compromise data being sent to or from a device by taking advantage of the fact that many applications and web pages do not use proper security measures, sending their data in the clear (not encrypted) so that it may be easily intercepted by anyone listening across an unsecured local wireless network.

Physical Threats

Since mobile devices are portable and designed for use throughout our daily lives, their physical security is an important consideration.

Lost or Stolen Device

Lost or Stolen Devices are one of the most prevalent mobile threats. The mobile device is valuable not only because the hardware itself can be re-sold on the black market, but more importantly because of the sensitive personal and organization information it may contain.

Afterwards, we focused our research on how these attacks can occur. This led us to the applications that run on each OS. By and large these programs are safe. However, cases of stolen identities, fraudulent phone calls, and stolen bank account numbers started circulating throughout the tech world. This was especially prevalent in

Android phones, but also occurring in Jailbroken iPhones.

Jailbreaking is a coined term, which essentially means that the device is out of its jail. Jailbreaking allows the user to gain root access to the operating system with the intent of overcoming limitations set by hardware manufacturers and carriers. Once a phone is jailbroken the phone has the ability to alter, replace system applications, change system settings, and downloading additional apps.

Although jailbreaking can be performed on the Android and the IOS it's much popular on IOS because it gives a user access to additional apps, extensions, and themes (located in Cydia), that aren't available in the Apple App Store. This isn't as popular on Androids phones because users already have the freedom to download any application they desire, from any location. The main security threat with a jailbroken device is that it installs a remote connection service, known as SSH. The SSH allows the user to manage and transfer files off the phone remotely from another computer. However the problem arises when the user installs SSH without changing the default password. This means essentially anyone can access their phone and all data.

One example of this security hack occurred in the Netherlands where F-secure reported on an iPhone SSH worm compromising bank transactions from jailbroken phones. Another example of security problems that arise after jailbreaking is the installation of 3rd party apps. These apps aren't verified by apple and therefore can leak user data to unwanted sources.

Research Methodology

Once we conducted our preliminary research, we determined two things. First and foremost, there is a significant threat to mobile security. Secondly, we found that both phones are equally vulnerable given the same conditions. An app can easily cause havoc on both iOS and Gingerbread if installed. From there, we needed to find out if this information is common knowledge between the public. Also we wanted to find what steps Apple and Google are taking to protect the user. This information was found using a survey, and an interview with a knowledgeable PH.D student in Security.

To gather even more research we decided to distribute a survey to the Facebook community and our class. We used an online survey software, Qualtrics, that enables users to do any kind of online data collection and analysis. We setup our survey with 15 questions that essentially asked our survey takers basic questions like what kind of OS they were currently using, if they thought there was phone was secure enough, if they had ever had a security breach, and etc. We got great results from our survey that are displayed below.

Initial Report
Last Modified: 11/05/2012

1. Do you currently use iOs, Andriod, or Other

#	Answer	Response	%
1	iOS	32	56%
2	Android	19	33%
3	Other	6	11%

Total	57	100%	

Do you think your phone is secure enough?

#	Answer		Response	%
1	Yes		40	70%
14	NO		14	25%
21	I		3	5%
	Total		57	100%

5. Are you currently aware of access permissions that applications have on your phone?

#	Answer		Response	%
1	Yes		30	53%
2	No		26	46%
3	I don't care		1	2%
	Total		57	100%

7. Have you ever experienced a security breach on your phone?

#	Answer		Response	%
1	Yes		4	7%
2	No		42	74%

3	No clue		11	19%
	Total		57	100%

:

After we conducted the survey, it became apparent that mobile security isn't taken nearly serious enough. The next step was to conduct an interview with someone more familiar with security. Kevin Benton, a PhD student, agreed to interview our group. In addition, he provided us with research he previously did that dealt with app permissions. The entire interview is available on our website. However, the main points are:

- Most security breaches are self-inflicted. Almost every attack comes from an app that was downloaded from a dangerous site. Even if the app is from the Play Store, or the App store most people simply ignore what the app has permission to do once installed.
- iOS and Android have similar permissions when it comes to their respective app stores.
- The focus should be on the prevention of breaches, not containment.
- Traditional viral programs won't be popular (at least currently) because of the strain it causes on a smartphone (slowdown, crashes, etc). In addition, since each application is sandboxed, a virus program (in essence, an app) cannot affect another application in any significant way. That includes the root of the phone. If that should somehow be affected, a virus program won't be able to do much to stop it.

Conclusions

Both companies have relatively rare occurrences of attacks on their operating systems. The ones that do are mostly due to circumventing the security measures already implemented (Jailbreaking, and ignoring permissions when downloading apps being the most typical offenders).

Although both iOS and Android operating systems are different from a design standpoint, as well as their stance on the development of their OS (Open vs Closed Source). Both are similar in their approach to security. Keep it secure from the beginning, so that a fix does not have to be released later.
On paper, it appears that Apple's iOS is the more secure system as it only allows you to download apps through their store. In addition the low amount of changes allowed to the system (and only by Apple no less) due to their closed source mentality means that it's pretty difficult to find a security breach in the code for iOS that can't be easily patched up. Compare that to Android that has hundreds, if not thousands, of devices (some up to date, some decidedly less so) that each run unique versions of their OS.

However, Android's OS main advantage is that it's way more forthcoming with information. A malware program, Bouncer, scans all apps on the Google Play store for malicious apps. There may be a similar program in the Apple store, based on research found on their website, but nothing concrete has be said on the matter. In addition, if an attack should occur, it is more likely that the open source community will have a solution available quickly. This ability to work together simply isn't possible under Apple's current stance on the changes of iOS.

Both Android and Apple have an inferior permissions model that allow malicious apps masquerading as legitimate apps to transmit undesired information to third parties. Although avoidable, these are often the most common way a security breach can occur on your phone. Once a malicious app has been downloaded, a user can be subject to numerous breaches, both minor and major.

Our recommendations are twofold. First and foremost, public awareness must be increased. As prevention

is the easiest way to prevent an attack from harming a phone in the first place, it would be more helpful if people were more aware of what their downloading and why. IU has emails about security that are sent out nearly weekly. In addition, there is a website, http://protect.iu.edu/cybersecurity/mobile , that can instruct users on the steps that need to be taken to secure a phone.

Secondly, a more helpful permissions app would allow people to protect themselves as well. If an app could lay out exactly what functions it will carry out if downloaded, a person could make a better decision as to whether or not it should be downloaded. The generic definitions that are provided are not defined enough. A person should also be able to turn off certain aspects of an app if they believe they do not need that particular function of an app. An example of this would be turning off the GPS tracker on a game that has no critical need for a GPS tracker.

Benton, Kevin. "Studying the Effectiveness of Android Application Permissions Requests." N.d. MS. Indiana University, n.p.

Mobile Threat Report!!
https://www.mylookout.com/mobile-threat-report

How secure is your phone:
http://bringyourownit.com/2012/04/04/safe-smartphone-android-ios-blackberry-windows-phone-attack/

Security flaw of iOS:
http://www.phonearena.com/news/5-year-old-SMS-security-flaw-in-iOS-has-finally-been-discovered...-by-a-hacker_id33409

Security flaw of Andriod:
http://mashable.com/2012/02/10/google-wallet-security/

http://blogs.computerworld.com/19035/htc_android_massive_security_flaw_leaks_private_info_like_a_sieve

Android improving security with new apps
https://www.mylookout.com/

http://developer.android.com/guide/topics/security/permissions.html