iOS Security vs. Android Security

Xiaoyi Zhou

Purdue University

Nov 29, 2014

iOS Security *VS* Android Security

The competition between iOS and Android has increasingly drawn people's attention, in terms of security, user interface, eco-system, and structure design. A lot of forums even launch the discussion between iOS and Android about which operating system is the most user friendly; which operating system supports more functions in general? With the trend that mobile users pick a team and cannot change their choice anymore because of the incompatibility in eco-system of the two systems, a comparison and analysis of iOS and Android should be made early. Therefore, users are able to choose a suitable system for themself rather than blindly rely on advertisement or a salesman's suggestion which is normally frustrating after you purchase the product. Since both of the mobile operating systems have been developed and improved for many years, the functionality of the two systems is compatible. So, we cannot make a judgment on which operating system is better than the other. The only thing we can analyze is the difference between iOS and Android.

As for a normal user, on the condition that iOS and Android are high quality, iOS is more reliable and stable for them. However, most students who major in technology or science will choose Android because of the flexibility of the Android system that provides various way to modify the functions. In other words, users can hack their Android mobile phone more conveniently than iOS system. Some users might argue that the Android system is inferior to iOS in the aspect of security while the less security feature exactly caters to the interest of programmer user who is particularly dedicated to writing programs and developing their own applications on the mobile phone.

Security is the most significant issue when it comes to analyzing the pros and cons of an operating system. With the development of science and society, nowadays the protection of and attention on private information gradually has become more important than past time. If the confidentiality cannot be promised, if the sensitive data is hacked, the loss is far more than the cost of a secure mobile device, which is also the main reason why should we get familiar with security.

iOS does not provide many privileges for users in case their users cause damage to the mobile phone by accident, or on purpose. The manufacture should not accuse the user of being unprofessional when problems occur. However it is a well-known phenomenon that some users do not have enough knowledge of technology and information security. Therefore the manufacturer cannot predict how many issues would happen assuming they provide the full privilege to user. The locking-privilege policy does guarantee the security to a normal user. But the existence of backdoor becomes an intractable problem these years since the staff involved in iOS development announced the backdoor embedding at iOS. Even worse, the backdoor almost gives permission to the manufacturer to spy on users' behavior. Once the user opens an application or makes a phone call, it is possible for backdoor programs to record the activity within the mobile device. After the exposure of the backdoor, Apple Inc. has to confess that there is an unpublished secret technology skill mastered by employees at Apple Inc. called the backdoor. And the secret technology skill planted in iOS could result in the revealing of documents, photos, contact numbers and other personal information. The original purpose of preparing the backdoor if not for the hackers of course, but designed for the investigation and mobile diagnosis (Greenberg, 2014). For instance, when the phone owner got involved into criminal case or other legal issue, the backdoor might contribute to digging out the strong evidence at the critical moment. Although the current forensics skill could figure out the truth preserved on the mobile device, retrieving evidence directly from the manufacturer not only saves time but also assures the confidentiality and integrity. For security sake, the investigator can take the benefits of backdoor meanwhile applying the forensics skill.

Considering the advantages and disadvantages of backdoor, somehow the backdoor is necessary especially in the field of cyber forensics. However realizing that the manufacturer can monitor the behavior and habit of a user without any notification is still uncomfortable.

The suggestion aimed to business and government users is strengthening the security of passwords or encrypting the private data instead of deprecating the iOS system completely. None of the mobile systems could be flawless. Comparing to other operating systems, iOS is more secure and highly functional. For example, in the summer of 2014, a scandal occurred to a celebrity whose mobile got hacked. The incident actually results from two factors consisting of the weakness of password and the security issue of iOS itself. Here we are not going to guess the password but we can assume that the password is easy to crack by brute force attack. Both the iOS vulnerability and user's carelessness should be blamed on the photo-surfaced incident. Passing the responsibility is not beneficial for fixing the bug caused by security issue. In order to maintain the secure environment on the mobile device, the user group and software developing team ought to work together and then improve the mobile security level to an advanced phase.

The other security risk of iOS lies in the battery of the mobile device. The adversary could eavesdrop on the mobile device via malicious programs if the malware is launched and the phone is operating normally. And triggering a mobile device remotely is feasible in terms of modern technology methods. To avoid that risk, the only effective method is unpacking the battery, which is also impossible in the iPhone. Fortunately only a small group is capable of the skill that controls the electronic device to start remotely. General users still support iOS even though the security issue arose. The unprofessional group is unlikely to take advantages of backdoor to steal sensitive information. Due to the restriction on mobile applications, normally, it is reasonable that users insist that iOS is the most secure mobile system.

On the contrary, the security issue of the Android system is always satirized by the public. Android, relatively to iOS, releases more privilege to users so that they are able to make modifications to the phone even if they are not experienced enough to do it. Despite the criticism, a lot of people still join in the team of Android. Before we study the security issue hidden in Android, firstly we should realize the difference between a backdoor and a loophole. A backdoor is implanted into the system intentionally by the software developing team while a loophole is considered as a mistake during the developing process. It is an unintentional bug. Because of the characteristic of loopholes, they are easy to discover and fix (Reid, 2014). A lot of advanced programmers are eager to find and report the loopholes of the Android system, which is also the factor that helps improve Android security.

Similarity

Both Android and iOS provide read access and partial write access. For the purpose of security, write access should be restrained. System programs can set the level of write access by calling Application Program Interface (API). Thus the security of API and the reliability of application could determine how secure the system is. Opening users' access to write is the only way to cause disruption to system functionality. Therefore it is wise for mobile operating systems to provide partial write access instead of full write access.

Difference

At the beginning when users intend to install an application, Android will provide the access that the application requires. Users can choose if they will accept or deny the installation of program. Once the user accepts it, the read access and write access cannot be modified unless the program is reinstalled. In other words, the Android system does not allow users to change the access to a program or accept partial access. Unlike Android, iOS constrains the installation for some programs. Users can only download and install applications from the official store provided by Apple. Additionally, all applications installed on iOS were examined and verified by the official institution so that the malicious applications could be filtered out. At the first time when users install an application, the iOS system will pop out a message box asking for access permission. Users can either give permission or deny it. But no matter what the choice is, users are able to change the access permission after installing the application.

iOS is more reliable than Android when it comes to examining the malicious programs. Although Android devices are supported by the official Google store, there are still some applications from third party stores that have the potential to damage the system integrity. To be more specific, Android users undertake the risk of being infected by malware. Some applications from third party stores have a higher security level, such as Amazon store. However many applications from third party stores will not be verified. A third party could re-implement the paid application program and then put the new free version at the store for downloading. As we known that paid applications contain codes that help verify the digital certification authentication, third party purposely rewrite it and compile the program again to break the certification authentication. Therefore the paid application got updated to free version meanwhile it might be implanted with malicious code in order to steal the credential information from users. Thus users privacy is under threat because of the malicious program. Users are supposed to consider the similar situation that their personal information might be when they plain to install applications from third party.

Additionally, some third parties lack the ability to verify the security of applications. A lot of programs seemingly function but the included malicious code is run in background. For instance the Douban broadcasting station, a music application originated in China, has a background program that scans recent browser history when users are listening to a broadcast from the application. The scanning background program is designed to upload users' browsing preferences to Baidu. The massive data is used to analyze the page view to the Baidu website. Therefore the security level of Android devices will decrease due to the third party applications. The third party normally doesn't acknowledge that the scanning program is malicious because it doesn't cause real damage to the system of the device. But the program tries to access users' privacy information like browsing history first and then send the information to other institutions without consent. Here we should consider how to define a malicious program. Any software or program that intends to disrupt computer operation, break confidentiality, or gain access to a computer system should be regarded as malware (Nash, 2005).

Another risk to Android systems lies in the access to the developer mode. Users do not need any authorization to open the developer mode to gain access to the operating system such as read and write files or install untested programs, etc. If a system supports any program written by users, the security level should be doubted. On the contrary, any users willing to gain access to the developer mode at iOS requires official authentication from Apple Inc. People without official accounts cannot manage to implement at developer mode. Therefore iOS users do not have to worry that the disruption to the operating system would happen at developer mode.

The Android system is initially generated from Google and then distributed to other mobile enterprises from the open handset alliance. Those enterprises will improve and customize the original generation of the Android system before launching it to market. Compared to the original generation, the derived generation might have more interesting features. The problem is if the original version has security risks, Google will launch a patch as soon as possible for upgrading. Users with the original version of Android can receive the patch instantly. But the enterprises from the open handset alliance should wait for the patch distributed by Google. Users cannot measure how long it takes for enterprises to customize and launch the patch. The upgrading process would be postponed so that the security risk might extend for one to three months minimum.

Due to the fierce competition in mobile marketing, both users and developers would like to get more access to mobile systems. Under pressure from massive amount of customers and competitors, iOS becomes more open while it cannot guarantee one hundred percent security. The mistake could appear during the verification procedure for applications. iOS used to launch an application named "Find and Call" that contains malicious code to get access to information credentials (Maslennikvo, 2012). This application is designed to simplify contact lists. The Apple store and users failed to detect the Trojan hidden in the application. The Trojan program resulted in a great number of downloads within 48 hours while part of downloads is automatically triggered by malware rather than users. The malware steals the contacts list and address book from users' device and upload the information to a remote server. The server then sends an email containing the information of "Find and Call" to the other email addresses retrieved from a users device. So the malware could spread to more people (Cheng, 2012).

Although Apple Inc. immediately launched a patch to fix the mistake after the accident, they claimed that "Find and Call" was the first malware found at iOS, causing users to be skeptical of security level at iOS. Another example reflecting iOS security is WireLurker invented by iTools which is the first third party iOS store in China. Security sources said that as long as the laptop is infected by this malware, all iOS devices connected to the laptop have a potential risk of being infected. When WireLurker infects an iOS device, it will automatically generate malicious application or download malware from a third party without permission from users. In the last year and half, WireLurker has infected more than 467 applications (Xiao, 2014). Apple has taken action to fix the problem. It released an XProtect update to detect if the programs running on OS X contain the malware, and removes the developer certification for compromised applications that are being used as vectors to spread the malware (Kessler, 2014). To protect system security, users cannot always expect the launched patch to work. Apple Inc. suggests users download the application only from the official App store. Admittedly third party stores might provide more interesting programs with affordable prices, but few users want to take the risk of being attacked by malware.

Until February 2014, security analysts categorized and summarized the main features of Android malware into seven categories: the ability to gain root or convince the user to root his phone, sending paid or malicious SMS messages, stealing location information, information stealing to a remote server, installing other applications or binaries, potentially unwanted application ("Hacker"-Tools), banking Trojan which is able to intercept and modify banking authentication codes (mTAN messages), and infecting a connected Windows PC with a Trojan (Forensics blog, 2014). So far most Android malwares have combination features of those seven types, even if they were downloaded from official Google-Play markets such as Android.FakeBank, a Trojan horse for Android devices, which opens a backdoor and steals information from the compromised device. Additionally, the malware is able to infect a connected Windows PC and tricks the user into exchanging legit banking apps against malicious ones (Forensics blog, 2014). Android systems have suffered from being attacked by malware for a long period. However, iOS seems more secure because if the users stick to the official App store, malware can hardly infect on their iOS device. Eleven malwares have been detected on iOS machine up until the present day. Eight of them only worked functionally on jailbroken devices. In this paper we have already mentioned iOS/FindCall.A!tr.spy known as Find and Call. The other two are Adware/LBTM and iOS/Toires.A!tr.spy aiming to retrieve personal information and generate unexpected high bills due to calling premium numbers of ads, respectively (Apvrille, 2014). iOS is not immune to malware. The malware targeted to iOS does exist regardless if the device is jailbroken. But the occurrence of malware with iOS devices is significantly less than with Android.

We can also analyze the security risk of iOS and Android from investigating their respective user group. According to the data gathered from the mobile markets, Android users take 80.2% of today's market while iOS users take 14.8% (Edward, 2014). So Android devices are the majority of today's market. At first glance of the data, some users might argue that iOS is far less developed than Android. But people should realize the act that mobile enterprises from all over the world carry on manufacturing Android devices, which create a great superiority over the Android device market. However, only Apple Inc. develops and manufactures iOS. Without the alliance from other enterprises and initial marketing advantages, iOS still takes nearly 15% at mobile market. iOS devices target the specific customer group in a mature market, while Android is used everywhere, by every type of customer (Bolluyt, 2014). Besides, a larger amount of user groups could also indirectly cause security risks. Mobile enterprises should not expect that every user has professional technical knowledge to deal with issues related to their devices. Hence, users at various levels of technical knowledge might have misuse of their device thereby some unexpected mistakes occur.

Android users insist that Android brings more pleasure than iOS. Indeed, Android devices provide a lot of functions and flexibility. It is more versatile compared to iOS.

Misuse might cause system corruption. Users with professional technology and computer knowledge are advised to use Android systems because they are able to protect credential information and system security. The flexibility of Android could be an added bonus because users could technically interact with their device; for example, they can write a program and implant the program into their own Android device. Some Android users possessed with computer programming knowledge are even eager to hack their Android device only for fun.

General users without enough technical knowledge are advised to try iOS. We can assume most users are looking for the system platform that is functional enough for life. Users worry about the system security and the confidentiality of sensitive information. Lack of technical knowledge can possibly result in personal loss. Therefore in the aspect of security, iOS is superior to Android.

iOS and Android are brilliant mobile systems despite the flaw of security. They make great contributions to modern technology and society. Mobile markets would suffer rapidly without Android and iOS. Users should understand that there is no absolute security in mobile operating systems. Even mobile manufacturers cannot define what is the most secure system. So, to keep sensitive data secure, the good way is to consider carefully what you need and why you need it.

Reference

Apvrille, A. (2014). Security Research: Threat Landscape and Analysis. iOS Malware Does Exist.

Bolluyt, J.(2014). The CheatSheet. Android vs. iOS: How We Are the Biggest Difference. Retrieved from http://wallstcheatsheet.com/technology/apple/android-vs-ios-how-users-are-the-biggest-difference.html/?a=viewall.

Cheng, J. (2012). The Apple ecosystem. “Find and Call” app becomes first Trojan to appear on iOS App Store. Retrieved from http://arstechnica.com/apple/2012/07/find-and-call-app-becomes-first-trojan-to-appear-on-ios-app-store/

Current Android Malware. (2014). Forensic blog: mobile phone forensics and mobile malware. Retreived from http://forensics.spreitzenbarth.de/android-malware/.

Edwards, J. (2014, May 31). The iPhone 6 Had Better Be Amazing And Cheap, Because Apple Is Losing The War To Android. *Business Intelligence Market*. Retrieved from http://www.businessinsider.com/iphone-v-android-market-share-2014-5.

Greenberg, A. (2014). Forbes. Android Upgrades Open A Backdoor To Malware, Researchers Show.

Kessler, T. (2014). MacIssues. How to protect yourself from ‘Masque Attacks’ that replace iOS apps with malware. Retrieved from http://www.macissues.com/2014/11/10/how-to-protect-yourself-from-masque-attacks-that-replace-ios-apps-with-malware/.

Maslennikov, D. (2012). The SecureList. Find and Call: Spam and List. Retreived from http://securelist.com/blog/incidents/33544/find-and-call-leak-and-spam-57/

Nash, T. (2005). An Undirected Attack Against Critical Infrastructure: A Case Study for Improving Your Control System Security.

Reid, B. (2014). iOS Backdoor Loopholes Let Apple And Government Agencies Collect Private Data. Retrieved from http://www.redmondpie.com/ios-backdoor-loopholes-let-apple-and-government-agencies-collect-private-data/.

Xiao, C. (2014). WireLurker: A New Era in OS X and iOS Malware.