Smart Phone, Dumb Security

Chris Rose, Ph.D., Walden University, USA

ABSTRACT

Over one-third of Americans use a smartphone daily and recently there has been a substantial increase in the incidents of malicious software on these devices. Smartphones, being just miniature computers, suffer from the kinds of hacker exploits that were prevalent in the early days of the proliferation of the PC. However, the differences in the ecosystem of these phones with Android being open, Apple which is closed but can be opened and BlackBerry which is completely closed and encrypted, has a profound effect on the security of these devices.

Keywords: Smart Phone; iPhone; Android; Malicious Software

INTRODUCTION

The Pew Internet Project found that 83% of all adults in the USA own some kind of cell phone and of those, 42% own a smartphone. This means that 35% of all US adults own a smartphone, which can be defined as a phone that operates on a smartphone platform including iPhones and Blackberry devices, and the numerous devices running the Android, Windows or the Palm operating systems. Of these 87% use their smartphone to access the Internet or email and 25% say they mostly use their phone to go online, rather than use a computer (Smith, 2011). But because smartphones can access other devices, networks and the Internet, they are in reality just mini computers, therefore just like computers, it is the responsibility of the user to keep them secure but few users actually do.

As smartphones grow in usefulness whereby people organize their digital life on a mobile device, their attractiveness to criminals also increase. Smartphones are now notebooks, wallets, email repositories, photo albums, organizers and mobile banking devices and since mobile phone owners are directly billed for phone services, this makes it more attractive to criminals. Hackers have attacked computers for years and now that smartphones are becoming a central part of daily life, they are becoming more attractive to criminals. "As more and more people use phones and keep data on phones, and PCs aren't as relevant, the bad guys are going to follow that. The bad guys are smart. They know when it makes sense to switch" (Robertson, 2011). A very large percentage of mobile apps are storing the user's sensitive account information unencrypted on their smartphones, according to a new survey. "Some 76 percent of the apps tested stored cleartext usernames on the devices, and 10 percent of the tested applications, including popular apps LinkedIn and Netflix, were found storing passwords on the phone in cleartext" (Isaac, 2011).

The root of this security problem is a result of the evolution of the device itself. PCs trace their origins to complex, home-built devices that took advanced technical skills to program, but the smartphone is a byproduct of a very simple and straightforward device, the home telephone which required no special skills to operate. Therefore PCs went in the direction of complex to simple whereas smartphones went in the opposite direction from very simple basic communication devices into miniature computers, rivaling the functionality of a PC. And as the capabilities and functionality of the smartphone grows, so does the exposure to hackers of the devices, thus mirroring the threats already present on a PC (Marko, 2011).

MALWARE

Lookout, the Android security specialists, says it is seeing more unique strains of Android malware than it did in all of last year.

- Lookout says it now detects thousands of attempted infections each day on mobile phones running its security software. In January, there were just a few hundred detections a day. The number of detections is nearly doubling every few months. As many as 1 million people were hit by mobile malware in the first half of 2011.
- Google Inc. has removed about 100 malicious applications from its Android Market app store. One particularly harmful app was downloaded more than 260,000 times before it was removed. Android is the world's most popular smartphone operating software with more than 135 million users worldwide.
- Symantec Corp., the world's biggest security software maker, is also seeing a jump. Last year, the company identified just five examples of malware unique to Android. So far this year, it's seen 19. Of course, that number pales compared with the hundreds of thousands of new strains targeting PCs every year, but experts say it's only a matter of time before criminals catch up (Robertson, 2011).

In the case of Droid Dream Light which was downloaded 260,000 times, the hackers took an existing app and modified it "to send details (including IMEI and IMSI info) about the infected handset to a remote server upon receiving a call. The code can also download and cue new package installations" (Gorman, 2011). Juniper Networks Inc. (JNPR) has estimated there is a 400% increase in Android malware since summer of last year (Jaroslovsky, 2011).

APPS

The Apple iOS security model has a rigorous certification process whereby Apple verifies the identity of each author of an app and therefore offers strong protection against malware. However, in early July a previously unknown security hole in Apple Inc.'s iPhones and iPads was discovered. Users downloaded a program that allowed them to basically jailbreak (remove Apple restrictions) their phone and run programs on their devices not authorized by Apple. But this jailbreaking software also allow hackers to take over the user's phone and it was the second time this year that the iPhone's security was breached.

Android doesn't offer this type of certification and this is the reason behind the proliferation of Android malware. Google lets anyone create and release apps, anonymously and without inspection and they could be downloaded from many different sites. "When Angry Birds first came to Android, you could only get it through a third party. This is called 'sideloading' or, installing apps using an .APK file....Most of the time you won't know what the file contains until you install it. By then it's too late" (Snyder, 2011). The Android Market allows anyone to submit any app for download, without it being tested for quality or security. This makes it extremely easy for hackers to sneak malware into the Android market. "Three out of ten Android users will encounter a web-based threat on their device this year, according to recent findings from Lookout Mobile Security" (Isaac, 2011).

Researchers have also discovered a design flaw in Android which could lead to pop-up ads for phones. For example, a hacker could create malware that appears genuine and could, for example, display a fake login page while the user is using the legitimate bank app since there is basic code in Android that allows a developer to override the standard for pushing the back button on the phone (Mills, 2011). In fact, a recently discovered piece of malware for Android not only logs details about incoming and outgoing phone calls, it also records those calls (Robertson, 2011).

Recent security testing on Apple and Android in multiple categories, ranging from social networking applications to mobile banking software found that Apple's iOS-based apps consistently scored higher marks than Android apps in security tests. This is because Apple's Keychain security architecture for storing user credentials is stronger than Android's Account Manager system (Isaac, 2011).

SECURITY

Unlike at a PC, a mobile phone user is always on and users instantly respond to email so they are more exposed to phishing sites. However, mobile phone users have one advantage over PC users and that is that the years of experience combating malware on PCs which has exposed the flaws which made the PC insecure, has served as a guide to creating a secure environment for the mobile platforms. But since there is such a heavy demand for

smartphones, (the market research firm IDC predicts that about 472 million smartphones will be shipped this year, compared with 362 million PCs) this isn't likely to be enough to keep hackers away (Robertson, 2011).

And hacking is relatively easy. A 10-year-old California girl who uses the pseudonym "CyFi," made a presentation at a recent hacker conference in Las Vegas demonstrating a new zero-day exploit in iOS and Android (zero-day means, instantly, before generally known to the program developer). Apparently she was playing a game, got bored with how long it was taking and manually advanced the clock on the device to force the game ahead. Some games stop this from happening but she demonstrated workarounds such as by disconnecting the wi-fi and making small incremental clock adjustments. She didn't reveal which games were affected (DesMarais, 2011).

There is also a new type of attack called the "upgrade attack" whereby hackers get around the scrutiny of newly released apps. What they do is produce a good, functioning app and then later they offer an update. but it is the update that is infected. And since most people set their phones to automatically update, there is less chance of the malware being discovered. "Hackers are experimenting with different distribution models...Mobile malware is now in the experimental stage, where attackers try innovative techniques to distribute their malware, and are engaging in experimental monetization" (Keizer, 2011). Another common technique is what is called "repackaging." This is the very common technique of taking a legitimate app, modifying it to include malicious code and then republishing it to the app market or alternate sites. This usually works because the average user cannot tell the difference between the legitimate app and the modified malicious version. Sometimes the hackers will even take a paid app, modify it to include malicious code and then offer it for free. The user, thinking it is the legitimate trusted app will grant the app permission to access various system resources which allows the malicious code free reign over your device (Marko, 2011).

Google's Android Market is now the premier place for hacking attacks since it developers don't have to submit their apps for pre-approval. Some of these schemes are impossible on a PC such as:

- An app that subscribed persons up to a service that sends quizzes by text message with the pay service charged to the victim's phone bill. Since malware can intercept text messages it is very possible the user didn't even see the text messages, only the charges.
- Another logs a person's incoming text messages and replies to them with spam and malicious links.
- Some even set up a connection between the phone and a server under a criminal's control, which is used to send instructions (Robertson, 2011).

THE ECOSYSTEMS

The ecosystems, or the environment in which the smartphone operates, has a profound effect on the general security of the device. Windows Phone 7 would, at first glance, appear to be a strong alternative for business because of Windows' dominance in the enterprise. But that's not the case. It is heavily integrated with Microsoft's consumer offerings such as the Xbox and it also requires Zune for multimedia file management. Windows Phone 7's target is clearly the consumer (Lyn, 2011). It doesn't command a large market share of users.

However, if a mobile device was originally designed with connectivity in mind, then it will be more secure than PCs (which were well established before the proliferation of the Internet). For example, the Canadian manufacturer Research in Motion (RIM) built its BlackBerry business around security and encryption, that is why it is used extensively in government and secure corporate environments. It is so secure that many foreign governments have either wanted to ban the devices outright, or have asked for some backdoor into the network, so that they can monitor the transmissions on RIM BlackBerry devices (Jaroslovsky, 2011).

The other two major operating systems used in smartphones, iOS developed by Apple and the open-source Android, developed by Google, vary greatly in their approaches to security. Apple mainly believes that security is their business whereas Google believes the security of Android is your responsibility. Both limit what third party applications (apps) can do to the core functions of the respective operating systems and force sandboxing, which is a system of restrictions preventing programs from doing anything to the core functions of the OS, or opening a hole in the system to allow other things to happen.

Apple however, just like BlackBerry, reviews every app which is to be used on their devices before allowing it to be downloaded. All downloads are controlled by them and have to be approved by them. Android, on the other hand, has no pre-approval process, if you create an app you can place it on the Android market for download and in addition, the Android Market is not the only place for Android apps, there is the Amazon Android market and many other smaller markets and there is no quality assurance with these apps and they have not been checked for malware or functionality (Jaroslovsky, 2011).

ANDROID

Android smartphones have a dedicated following perhaps because the openness of the system allows customization and modifications that are not possible on other systems. It is currently the most popular OS used on smartphones yet support, updates and apps all depend on a variety of people, from Google itself, to the smartphone carriers such as AT&T or T-Mobile and also much depends on the third-party app developers. This alone is a major reason why business IT departments are skeptical about adopting Android in the corporate environment. There are also so many variations between Android phones whereby a phone on a certain carrier will have a different version of software than the identical phone on another carrier, makes Android an extremely challenging proposition. For example, some carriers offered a recent Android 2.2 update which extended functionality and addressed some prior issues with the OS. Some phones got the update while other had to wait months to get it. In fact, at one time Sony Ericsson stated outright that one of their phones wouldn't get the update, but after customers complained they relented and even offered updates beyond the Android 2.2 (Lyn, 2011).

However, this fragmentation causes tremendous support problem s and if an IT department was to allow their users to bring various types of Android phones with various versions of the OS into their network, the problems could be catastrophic. Even if only one type of phone running one version of the OS was allowed, problems would arise if that particular phone/version combination never got upgraded by the provider. Android supports Exchange, but again the fragmentation results in no uniformity therefore security support is almost impossible. In addition, third-party apps that are supposed to enhance Android and Exchange can sometimes cause problems if a certain phone/version combination is upgraded and another is not (Lyn, 2011).

APPLE

Apple does not need to focus on the enterprise because its consumer base is so huge but Apple's iPhone and iPad in particular are used in some clever and creative ways by smaller business. Apple does makes business products such as the Mac mini server and the OS X Lion Server. However, those products are for the small and medium business sector or businesses that are all-Apple shops and are not suited to large enterprise networks. For example, Apple recommends the Mac mini server for workgroups of only up to 50 people. Apple's real efforts are squarely behind the Mac mini (Lyn, 2011).

Apple has improved the compatibility of iOS with Exchange servers but there are still problems especially when the iPhone's OS gets updated. When iOS4 was introduced those iPhones running that OS had problems communicating with Exchange Active Sync and recently more problems have been discovered with iOS5 and Exchange Active Sync policies (Lyn, 2011).

Apple phone can also be jailbroken, that is, the restrictions that are built into the device by Apple can be circumvented and this allows the users to get root access to the very heart of the operating system. When this is done, custom software can now be installed on the devices and there is no longer any restrictions or limitations on what can be done or which apps can be installed. But even without jailbreaking, Apple iOS is vulnerable to malware, and a site such as JailBreakMe which can modify the iOS kernel is one such example (Marko, 2011). Recently, also researchers discovered a security hole in Apple Inc.'s iPhones, which prompted the German government to warn Apple about the urgency of the threat (Robertson, 2011).

BLACKBERRY

BlackBerry phones can't be jailbroken, and it is not for a lack of trying. Hackers have tried for years and have never succeeded. In addition, unlike other smartphones a BlackBerry does not directly connect with the Internet, it only connects indirectly through the BlackBerry Network Operations Center (NOC). If a Blackberry user opens a browser and goes to a web site, that information is passed to the NOC and the NOC then retrieves the Internet information, encrypts it and then sends it encrypted and compressed to the BlackBerry user. It is the only totally encrypted smartphone system and the user can even encrypt the media card which internally stores information. It is because of this encryption process that BlackBerry has had problems with the governments of Dubai, India, Saudi Arabia among others, because it is impossible to intercept BlackBerry communications without the assistance of the BlackBerry NOC, but these governments wanted access to the phone communications within their country (Walid & Karam, 2010).

"Blackberry is losing status as a cool and sexy device, but cool and sexy is not what IT needs. The constant attention on the enterprise that RIM delivers is what business needs" (Lyn, 2011). RIM's BlackBerry Enterprise Server has long worked with Exchange and BlackBerry Enterprise Server 5.0 is fully certified to work with Exchange 2010 and comes with full technical support services, which is critical for IT. With full support, IT has an almost guarantee of faster turnaround time for solution of any BlackBerry problems, and RIM can be held accountable if they don't deliver as promised (Lyn, 2011). In addition, the only tablet device to receive Federal Information Processing Standards (FIPS) certification is the BlackBerry PlayBook and only if a device receives FIPS certification can it be used by the US government. The PlayBook is also HIPAA compliant and a Blackberry is the only mobile device that the President of the United States is allowed to carry, which again further reinforces BlackBerry's security pedigree.

BlackBerry Enterprise Server (BES) gives control to the IT department to individually control and set policy for each BlackBerry device and even to perform remote wipes. iOS and Android just can't match this natively but there are apps that offer varying degrees of security controls over iPhones and Androids but even these apps can be a security risk if they are poorly coded. Since BES offers all these security controls out of the box, RIM remains the only solid choice for businesses."For IT infrastructures, particularly those who must adhere to rigid corporate or government-mandated compliance requirements, the BlackBerry ecosystem is unmatched in security and manageability for smartphones" (Lyn, 2011). BlackBerry also recently introduced BlackBerry Balance which securely partitions a BlackBerry into two separate partitions so that one device can be used for both business and personal uses and the data on one side can't interact in any way with the data on the other.

CONCLUSION

In August 2011, McAfee recently stated that malware for Androids phones jumped 76% since the last quarter which makes it the most heavily attacked mobile OS. McAfee has also found 12 million unique types of malware in the first half of 2011, a 22% increase from a year ago, and expects that by the end of the year they will have 75 million samples of malware in their database (Cheng, 2011). In addition, a gadget advice site Retrevo found that users of Android devices are "significantly less security-conscious than owners of devices made by Research in Motion (RIM). Android users take insufficient steps to reduce their vulnerability ... to theft of confidential information, e-mail addresses and other files they thought were secure" (Jaroslovsky, 2011). Since "attackers can spoof legitimate applications with high accuracy, suggesting that the risk of phishing attacks on mobile platforms is greater than has previously been appreciated" (Robertson, 2011).

Apple has the leading consumer-oriented smartphone strategy, but BlackBerry has had great success with its focus on the enterprise. BlackBerry does not have a very appealing user experience, however, what BlackBerry does best is security and IT management and that just works seamlessly in the background. "BlackBerry is considered stodgy, and so it should remain.... RIM can't beat Apple at its own game. But that's fine. We can love our Androids and iPhone when we're off the clock, but, in the office, BlackBerry is still tops" (Lyn, 2011).

AUTHOR INFORMATION

Professor Chris Rose, Ph.D., teaches at Walden University USA. E-mail: christopher.rose2@waldenu.edu.

REFERENCES

1. Cheng, R. (2011, August 23) News.com. McAfee says Android plagued by the most malware. Retrieved 9/8/2011 from http://news.cnet.com/8301-1035_3-20095965-94/mcafee-says-android-plagued-by-the-most-malware/#ixzz1Y3vFwoTz
2. DesMarais, C. 2011, August 7) PCWorld. Hacker, 10, Exposes iOS and Android Games Exploit. Retrieved 9/3/2011 from http://www.pcworld.com/article/237467/hacker_10_exposes_ios_and_android_games_exploit.html
3. Gorman, M. (2011, June 1) Engadget. More malware in the Android Market: Google removes 26 deleterious app doppelgangers. retrieved 9/3/2011 from http://www.engadget.com/2011/06/01/more-malware-in-the-android-market-google-removes-26-deleteriou/
4. Isaac, M. (2011, August 8) Wired. Survey Finds Smartphone Apps Store Too Much Personal Data. Retrieved 9/4/2011 from http://www.wired.com/threatlevel/2011/08/smartphone-local-data-storage/
5. Jaroslovsky, R. (2011, August 31) Bloomberg. Clueless Android Users Make Enticing Targets. Retrieved 9/6/2011 from http://www.bloomberg.com/news/2011-08-31/android-s-insecure-users-top-all-malware-targets-tech-by-rich-jaroslovsky.html
6. Keizer, G. (2011, August 3) Computerworld. Spike in mobile malware doubles Android users' chances of infection. retrieved 9/7/2011 from http://www.computerworld.com/s/article/9218831/Spike_in_mobile_malware_doubles_Android_users_chances_of_infection
7. Lyn, S. (2011, August 5) PCMag.com. BlackBerry Still Tops for IT. Retrieved 9/5/2011 from http://www.pcmag.com/article2/0,2817,2390526,00.asp
8. Marko, K. (2011, August 8) Information Week. Mobile Malware: Protect Yourself Against Evolving Threats. Retrieved 9/7/2011 from http://www.informationweek.com/news/231300437
9. Mills, E. (2011, August 6) News.com. Android could allow mobile ad or phishing pop-ups. Retrieved 9/6/2011 from http://news.cnet.com/8301-27080_3-20089123-245/android-could-allow-mobile-ad-or-phishing-pop-ups/#ixzz1Y3YJfPD0
10. Smith, A. (2011, July 11) Pew Research Center. Smartphone Adoption and Usage. Retrieved 9/3/2011 from http://www.pewinternet.org/Reports/2011/Smartphones.aspx
11. Snyder, B. (2011, August 30) PCWorld. Android Devices Exposed: 7 Ways to Thwart Hackers. Retrieved 9/8/2011 from http://www.pcworld.com/article/239162/android_devices_exposed_7_ways_to_thwart_hackers.html
12. Robertson, J. (2011, August 7) MSNBC.com. Your smartphone: a new frontier for hackers, Retrieved 9/2/2011 from http://www.msnbc.msn.com/id/44050631/ns/technology_and_science-security/#.TnJiIs0xaHs
13. Venkatesan, D. (2011, August 1) TotalDefense.com A Trojan spying on your conversations. Retrieved 9/2/2011 from http://totaldefense.com/securityblog/2011/08/26/A-Trojan-spying-on-your-conversations.aspx
14. Walid T and Karam, S. (2010) BlackBerry users in UAE, Saudi may have services cut. reuters. retrieved 5/11/2011 from http://www.reuters.com/article/2010/08/01/us-uae-blackberry-idUSTRE6700C920100801

