False Assurance in Smartphone Security for Users

Submitted by
Tung T Nguyen

Lewis University

Submitted to
Dr. Ray Klump

Information Security Project, Spring 2011

TABLE OF CONTENTS

ABSTRACT

Smartphones have been an essential tool for employees who are frequently out of the office. These devices keep them in communication with the office, vendors and customers. It has been shown that "teleworkers work, on average, two hours more per week than office workers. "Access to real applications from anywhere means more work in work places."" (Wailgum, 2010) The ability to access such information outside the office with a portable device such as a smartphone has Information Technology personnel concern about security and the security vulnerabilities that may be inherent with the device.

While there are simple methods to bypass and access the stored data on smartphones if lost or stolen, there are third party applications that can be downloaded and installed for mischievous individuals to access the desired information. (Blake, 2010)

Information Technology personnel have attempted to resolve this issue by purchasing the best application available and deploying these third-party softwares to these devices. These third-party applications allow the client to receive time emails and documents, calendar events and personal contacts of their mailbox on their personal devices. The concern of a smartphone falling into the wrong hand with sensitive and confidential information is a security risk and nightmare for not only the business, but also the insurance company so software from these vendors allows conscious personnel a method to protect the information along with remotely wiping the device.

This paper will demonstrate to individuals that there is no such safeguard for smartphones. There is an abundance of information regarding the security and vulnerabilities of these devices and the effort of this research through the World Wide Web will reveal to owners of smartphones that their devices are not secure as the manufacturers lead them to be. The

results of the findings illustrate how flawed and vulnerable these devices are and the security assurance individuals place in their smartphones are false. This research will demonstrate to smartphone owners that they need to take a more proactive stance with their devices.

CHAPTER 1: INTRODUCTION

The advancement of technology in the realm of PDA/Smartphones has users skeptical of the private information kept on their device. Individuals are protective of their privacy and want to keep the sensitive data from prying eyes. They believe that by encrypting their device(s), the information stored within them is safe. It also has been suggested that smartphones should be encrypted for other reasons as well. In a recent case, the California Supreme Court reached a controversial 5-2 decision in People v. Diaz where they allowed police officers to lawfully search mobile phones found on arrested individuals' persons without first obtaining a search warrant. The court reasoned that these devices fall under the search incident to arrest exception of the Fourth Amendment. (Radia, 2011) This means that not only does a user have to worry about individuals with malicious intent; one also has to worry about the law and if there may be any information that may be incriminating if law enforcement searches their smartphone at the time of arrest.

Manufacturers such as Apple, RIM (Research in Motion), Windows Phone and devices using the Android operating system such as Motorola, HTC (High Tech Computer Corporation), Samsung, etc. have given users false security pretense that the encryption technology for these devices are currently available for some of these devices and there should be no hesitation to implement such policy. "Apple claims that hundreds of thousands of iPhones are used by corporations and government agencies. What it won't tell you is that the supposedly enterprise-friendly encryption included with the iPhone 3GS is so weak it can be cracked in two minutes with a few pieces of readily available freeware." (Chen, 2009) When the owner of a smartphone implements the password setting on the phone, it should not be accessible to others, but it has been documented that this is not the case. (Hill, 2010), (Prince, 2010) Other smartphone that do

not support full-disk encryption have another avenue by purchasing third party applications to encrypt particular types of files such as emails, voice call and text messages. (CheckPoint, n.d.) As with any software, there is not an absolute guarantee that such applications will fully protect the data on the device so enabling the password mode on the smartphone is recommended.

The relevant question of how valuable the data stored within a smartphone may be depends upon the view of the owner whether it is personal data or enterprise data. Whatever the decision may be, the simple fact to securing the smartphone starts with educating the user how to use their device effectively thus making them more secure. This document will provide the necessary information to mitigate security issue(s) for smartphone owners and demonstrate to the owners of these devices the need to update the operating system and install the necessary security patches when made available from the manufacturer.

This paper is organized as follows. Chapter 2 will discuss the history and the direction of the smartphones. In Chapter 3, the focus will be on security exploits of these devices. The security exploits vary from hardware to software and other exploits such as Bluetooth and application downloads. The final chapter, Chapter 4, will discuss recommendations to securing smartphones.

CHAPTER 2: OVERVIEW

The history of cellular devices dates back to the early 1920s. This period established the emergence of radio phones. Radios were emerging as effective communication devices and the first usage of radio phones were in taxi and cars using two-way radio communication. (History of cell, n.d.) The first use of a cell phone was in 1946 by the Swedish police. The Swedish connected a hand-held phone to the central telephone network thus making it the first official cell phone.

The history of smartphones has only been a fraction compared to the history of cell phone. Smartphones have only been around and available since 1993. It has only been recently that smartphones have become popular due to the prohibitively expensive for most consumers because the early smartphones were primarily used as enterprise devices. The IBM Simon was the first attempt of a smartphone that incorporated voice and data services into one device. The price of the IBM Simon in 1993 was $899. Following the IBM Simon, the arrival of the Palm Pilot was released in 1996, but it was not considered a smartphone. In 1998, The Nokia 9110 Communicator was released, but did not have the ability to browse the web. BlackBerry released its smartphone in 2002. This device had the ability to get e-mail and surf the web, but the owner needed to plug in a headset in order to use the device as a phone. Palm's second attempt for a smartphone was in 2003 when they released their first smartphone, the Palm Treo 600. It was not until 2007, when Apple brought the smartphone to a mass consumer market. (Reed, 2010) Apple dramatically increased the popularity of these electronic devices and due to the enormous success of the iPhone, wireless carriers such as AT&T Wireless, Sprint PCS, T-Mobile and Verizon Wireless discovered they could lock in consumers for an extended period

and subsidizing their cost by supporting their customers' purchases of the latest and greatest smartphones.

The advancement of smartphones has exploded to a high demand globally. Manufacturers saw a growth rate of nearly 57% in the first quarter of 2010. (Hamblen, 2010) "2010 was a big year for smartphones. The global market exploded with smartphone shipments totaling 101.2 million units over 2010, almost double that of 2009." (Isaac, 2011) The availability of these phones allows users to be more mobile and available outside of their offices and as such, businesses have seen a need to have smartphones for their employees.

Smartphone Operating Systems

There are six major operating systems for smartphones that are shipped worldwide. These operating systems are Symbian, RIM (Research In Motion), Windows Mobile, Android, iPhone OS (iOS) and other. Figure 1 displays the "Share of worldwide 2010 Q4 smartphone sales to end users by operating system," according to Canalys.

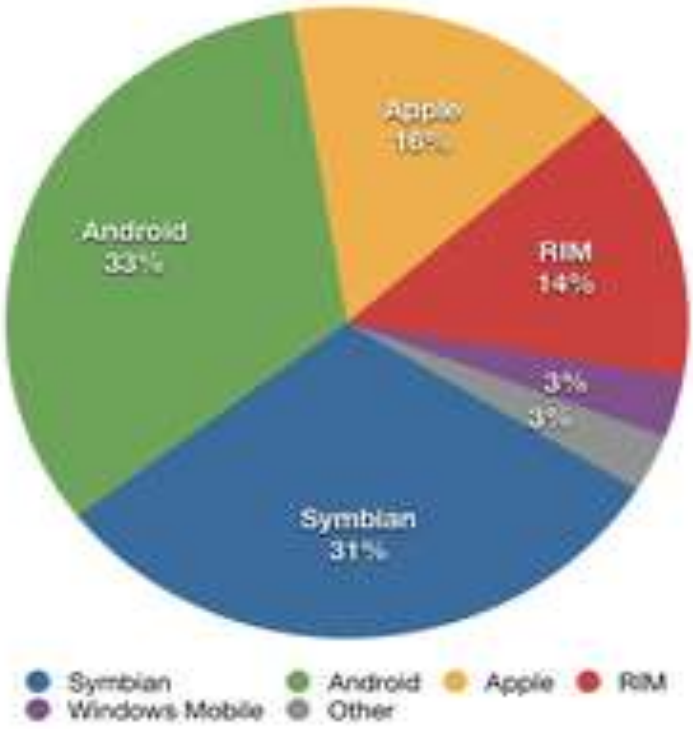

Figure 1. Share of worldwide 2010 Q4 smartphone sales to end users by operating system (Source: Smartphone, 2011)

A recent study by Gartner shows the expected worldwide sales of smartphone will reach 468 million units in 2011. It has been predicted that smartphones with the Android OS will get approximately 50% of smartphone market share by 2012. The same study shows that Microsoft may overtake the market share of Apple's iOS by 2015. (CNXsoft, 2011) Table 1 displays the projection of smartphone sales by operating system through 2015.

Table 1. Worldwide Mobile Communications Device Open OS Sales to End Users by OS (Thousands of Units) (Source: CNXsoft, 2011)

OS	2010	2011	2012	2015
Symbian	111,577	89,930	32,666	661
Market Share (%)	37.6	19.2	5.2	0.1
Android	67,225	179,873	310,088	539,318
Market Share (%)	22.7	38.5	49.2	48.8
Research In Motion	47,452	62,600	79,335	122,864
Market Share (%)	16	13.4	12.6	11.1
iOS	46,598	90,560	118,848	189,924
Market Share (%)	15.7	19.4	18.9	17.2
Microsoft	12,378	26,346	68,156	215,998
Market Share (%)	4.2	5.6	10.8	19.5
Other Operating Systems	11,417.40	18,392.30	21,383.70	36,133.90
Market Share (%)	3.8	3.9	3.4	3.3

Since smartphones are small computers, they have similar characteristics and features such as the processing power and storage capability. The newest smartphone released by AT&T in February 2011, the Motorola Atrix, has a dual core 1 GHz processor with 16 GB of onboard memory storage and another 32 GB of memory storage available on the removable microSD card. Smartphone owners are becoming more familiar with their smartphones so they are comfortable loading and storing information onto these devices. Such information is attracting malicious individuals to target these phones. The information smartphone owners are storing on their phone range from personal contacts to calendars to private messages and even to banking transactions. (BBC, n.d.) A recent survey by InsightExpress shows business users utilizing their smartphones not only for company business, but also personal. These business users are also accessing their web mail, instant messaging, browsing the web, downloading and sharing files over the Internet as well as checking financial account information. (Hicks, 2006) The survey

shows an astonishing 55.7 percent of smartphone users store confidential personal, business or client data on their devices. This same survey shows more than 54 percent use their devices to send and receive e-mails that include confidential personal data; 40 percent access bank accounts using their smartphones; and approximately one-third of the surveyed stated they access credit card accounts.

CHAPTER 3: SECURITY EXPLOITS

The purpose of this study is to show that mobile devices are vulnerable to a range of exploits from plugging the device into a computer and running specialized forensics software to simply bypass the password encryption of the smartphone with the password security feature enabled on these devices. Techniques will be demonstrated and documented for accessing these devices without the need to have any hardware or software that may not be readily available in the field. A second methodology will be shown and documented on the process of accessing the data on these devices with freeware that is available through the World Wide Web. The smartphones can be configured to erase all data after so many password attempts, but the method discussed in this paper will allow an individual to access the device and be able to view all the data intact.

With a little bit of research, an individual can apply and perform simple tasks to access the data on these smartphones with these assistance of available knowledge through the collection of knowledge base articles or publications for these devices through the World Wide Web. The simple steps of showing how effortlessly it may be to break into Apple's iPhone by exploiting the vulnerability of Apple's iOS using only the device. (Withers, 2008) This task can also be performed on the Android OS without the need for any hardware or software. (Kincaid, 2011) The project will also show and demonstrate that applying simple software hack to access the stored data on these devices through software download that is readily available through the World Wide Web for the more difficult devices. (Forgot your iphone, n.d.)

Exploit to Hardware

The advancement of mobile devices such as the iPhone 4, Motorola Droid X, BlackBerry and Windows Mobile 7 phones have made them targets to malicious individuals. As with any technological advancement, the concern of security is an issue. It has been discovered that some of the mobile operating systems for these devices have vulnerabilities that allow malicious individuals to bypass the security settings set by the owner of the device. (Surf4Fun, 2011) Information stored in these devices can quickly be accessed without much effort for these thieves. No matter what wireless devices are available for consumer usage, there are security flaws in these different smartphones. (Ahmed, n.d.) The different vulnerabilities and an explanation of their vulnerabilities are documented for the iPhone OS, Android OS and Windows Phone 7 OS.

When Apple released the original iPhone in January 2007, it was using the OS X. Apple did not official name the OS X to iOS until June 2010. When Apple released the iPhone 2 and the operating system, OS X 1.0, which was shipped with it, it already had security flaws. In fact, when the operating system was released, it was already four months behind in security patches. (Krebs, 2008) The original operating system was designed to have all programs running as root and as such, required no authentication to install applications. The theory behind this vulnerability is that if any program has a vulnerability, then a hacker could exploit the vulnerability by remotely installing malicious code that takes over the phone. (Zetter, 2007) As improvements to the operating system were released (version 1.0 through 4.2), newer versions of the iPhones were also released (iPhones 2, 3G, 3GS and 4G). These improvements were no better due to the fact they too had security vulnerabilities. (Chen, 2009), (Chen 2011) The biggest vulnerability is the exploitation of the operating system to quickly bypass the password

set on the device. (S, 2008) Bypassing the passcode set on the phone is simple as pressing the "emergency call" button from the home screen, pressing the pound key three times and hold down the power button. Apple's attempt to release a newer operating system to encompass their latest model, iPhone 4 that was released in June 2010 also was discovered to have the same vulnerability. (Filho, 2010)

Many wireless device manufacturers from Samsung to Motorola to HTC are using the Android OS as the operating system. The Android OS has quickly become the platform of choice for smartphone manufacturers. (Cormier, 2010) As quickly as these different devices were released to the public, vulnerabilities were discovered in the operating system. The ability to bypass the security password enabled on the device by the owner is a terrifying notion. Bypassing the security passcode only takes a moment. When the smartphone has an incoming call, answering the call allows one to have full access to the device. (Wally, 2010) Depending on the device, there may be another method to bypass the password lock. (Abrams, 2010) It also has been discovered that voice activation in the Android OS has a security flaw allowing calls to be made from the device while the passcode is activated. (Ahmed, n.d.) Smartphones owners using the Android OS may not completely understand the open source software policy. This policy or lack of policy implies that Google does not regulate and monitor their applications that are available for download through the Android Market. The topic of security implications for the open market policy will be discussed in the software exploit section.

Microsoft became the latest company to revamp their operating system for their smartphone device. Microsoft was already in the smartphone market, but its share in the market was small. (Mick, 2010) The predecessor to the Windows Phone 7 was the Windows Mobile 6.5. The security vulnerability of the mobile 6.5 operating system allowed attackers to retrieve

any file on the phone that uses the operating system by connecting to the device via Bluetooth. (Ng, 2009) There have been no reports of security vulnerabilities of the recently released operating system. Although the operating system is new to the market, it already has been jailbroken. (Manninen, 2010) Jailbroken phones are more susceptible to security vulnerabilities because they tend to allow users to download applications from unknown source(s) or not approved by the manufacturer. (Admin, 2009), (Orloff, 2009) When applications are not monitored, anyone developing an application for the operating system can upload their own code, which could be malicious code.

Exploits to Software

Information Technology personnel are constantly worried and concerned about the security of wireless devices such as smartphones. The advancement of technology to make small, portable devices on the go so employees are more mobile and efficient not only has its advantages, but also its disadvantages. These individuals constantly question the validity of security on these devices. These smartphones are just as powerful as or even more so than computers ten years ago. Computers in early 2000 had AMD (Advanced Micro Devices) or Intel processor running at 10 MHz (Choosing a processor, n.d.) with hard drives averaging about 20 GB. (Adimoga, 2010) Smartphone devices these days such as the iPhone 4 are running a 1.0 GHz Apple A4 processor with either 16 or 32 GB hard drives. Being that these smartphones are so robust, it allows users to download applications that may be beneficial to them. With these downloads, hackers are targeting these devices by embedding malware into these applications. Recent discoveries of applications available on the Android Market were malicious. Approximately 50 applications were removed from the Android Market after Google discovered

that these apps secretly installed malware. The applications sent "personal details including the phone's unique IMEI (International Mobile Equipment Identity) number to a US-based server and worse, it exploited security flaws to root the phone and install a backdoor application that allows further software to be installed to the handsets." (Bright, 2011) Third-party mobile software applications provided by Good Mobile Messaging, BlackBerry Enterprise Server or Zimbra Mobile Web Client installed on these smartphones can wipe out the data on the device after so many failed attempts . These applications also allow an administrator to send a command to remotely wipe all data from a device that contains confidential and sensitive business information is the only tool an Information Technology administrator has in his or her arsenal.

Good Mobile Messaging

Motorola Good Technology Group provides Good Mobile Messaging for many of the cell phone providers such as Sprint, AT&T Wireless, Verizon Wireless and T-Mobile. (Good technology, inc., 2011) The Good Mobile Messaging is a client-installed software and uses OTA (over-the-air) transmission to communicate with the smartphone and the server. "Good Mobile Messaging provides end-to-end mobile security with FIPS certified 192 bit AES encryption for data in transit as well as stored on the users' devices." (Good mobile messaging, n.d.) The security policies for users, devices and applications can be remotely locked down by IT along with hardware components including cameras, Bluetooth, and IR ports. The ability to perform such task by IT mitigates the security issues with smartphones.

Motorola Good Mobile Messaging allows an administrator to send a remote wipe command disabling the Good Client on the smartphone. This feature removes and disables the

user's mailbox on the device. In this example, a Motorola Droid X had the Good Mobile Messaging client installed and a remote wipe command was sent to the device. After a few minutes, trying to access the Good Mobile service on the device was disabled and information was cleared. A prompt is displayed informing the user to contact the administrator to resolve the issue. Even though the phone no longer had any enterprise data on it, the application did not completely wipe out all data on the device so text messaging or pictures stored on the device are still accessible. Good Mobile Messaging only promises to wipe enterprise data , which means any data stored on the device's internal storage or secure data card is still retrievable. The only certainty after researching the Good Mobile Messaging client to completely wipe all data on the device is performing a factory reset. This function restores the phone to its factory settings. Resetting the phone to the original factory default state is by holding down the Power and Home buttons for about 5 seconds, then tapping the Search button, scrolling down to factory reset using the volume down button and selecting Yes – delete all user data and tapping the OK on the screen. The security concern is how does one perform such a task when the phone has been lost or stolen?

Even though a company such as Good Technology pride themselves on how secure their mobile application for smartphones may be, there are always vulnerabilities that need to be addressed. While researching for security vulnerabilities, it appears Good Technology has other known issues from previous reports. "A potential vulnerability with one of the third party libraries used by Good Mobile Messaging for converting attachments to text when choosing the "View as Text" option from the Good Messaging client." (Good mobile message, 2009) It was discovered that the vulnerability could be exploited, resulting in the attacker gaining "Good Admin" user privileges because an attacker can send an electronic mail message with a PDF

attachment to a Good Messaging user. As with any security vulnerability, keeping up-to-date with hot fix resolves such issue.

BlackBerry

Another tool besides Good Mobile Messaging for IT personnel to consider is the BlackBerry Enterprise Server provided by Research in Motion (RIM). RIM has stated, "BES (BlackBerry Enterprise Server) is designed to provide peace of mind in mission critical environments. It provides controls and advanced security to help you stay confident that sensitive information is transmitted in a highly protected environment." (Blackberry enterprise server, n.d.) BlackBerry also uses over-the-air transmission to control mobile devices from imposing a device lock-down, wiping data from a lost or stolen device and wirelessly enforcing security setting that includes Bluetooth lockout. BES uses Advanced Encryption Standard (AES) or Triple Data Encryption Standard (Triple DES) to encrypt the data transmitted between the BlackBerry Enterprise Server and BlackBerry smartphones. Information Technology personnel are always looking for any advantage they can gain against mischievous and malicious individuals and having the ability to control smartphones is an excellent way to increase security. The disadvantage of the BlackBerry Enterprise Server is that it is proprietary, meaning the software only works for BlackBerry smartphones.

The BlackBerry Enterprise Server mobile client like any other software does have security vulnerabilities to address, but with diligence from an Information Technology administrator, the security vulnerabilities can quickly be resolved. Security vulnerabilities on the BES were widely published on the World Wide Web, but after researching for specific password vulnerabilities, Research In Motion (RIM) appears to have this feature locked down. If a user

misplaces his or her phone and the password is entered incorrectly after 10 times, all data on the device is completely wiped. An administrator can also send a remote command to perform this task as well. Once the device is wiped, the information that was on the device cannot be recovered. In fact, Research In Motion has been approved and certified for storing and transmitting sensitive data by the North Atlantic Treaty Organization (NATO) and other government organizations such as the United States, Canada, the United Kingdom, Austria, Australia and New Zealand. (Approvals and certifications, n.d.)

The Research In Motion BlackBerry Enterprise Server has a few security vulnerabilities that need to be addressed. A Russian company, Elcomsoft, has recently claimed it has broken the password protection used to secure data backups from BlackBerry smartphones. "The weakness in the way BlackBerry has implemented the apparently secure 256-bit AES encryption allows a successful password recovery attack on the backup archive." (Dunn, 2010) A second vulnerability that was discovered allows a hacker to hijack a connection to the network by exploiting the trust relationship between a BlackBerry and a company's internal server. The program, BBProxy, either can be delivered as a Trojan horse through electronic mail or has to be placed physically on a BlackBerry. (Zetter, 2006) Another security vulnerability allows a hacker to steal the contact list and image database of a BlackBerry. The exploit is through the Javascript in the BlackBerry browser and it has been advised by Research In Motion to disable the JavaScript in the smartphone's browser to block exploits. (Naraine, 2011) After reading websites and blogs of how secure the smartphone was for the past month, it was believed by many that BlackBerry was impenetrable, but these new results show that this is no longer the case.

Zimbra Collaboration Server

Zimbra Mobile Web client provided Zimbra Collaboration Server (ZCS). ZCS provides a mobile web client for smartphones, iPhone and iPad and BlackBerry. (Zimbra collaboration server, n.d.) The software uses over-the-air transmission called Zimbra Server sync. An advantage of this software is that it is the only open source solution for Linux and Mac server supporting access to emails, contacts and calendar through several options such as mobile web browsers, enabled devices, smartphones and BlackBerry. Zimbra security framework applies SSL/TLS encryption to all network communications, authentication tokens containing cryptographically secure representation of the user's individual and machine/network identity and Secure Multipurpose Internet mail Extensions (S-MIME) or Pretty Good Privacy (PGP) which mitigates security issues for the web. The web client security relies on the standard web platform technologies and downloads an Ajax-based application. (Zimbra email and, n.d.) The advantages Zimbra suggest it has over other traditional products are the residual of the software is not left on the client for a malicious person to tamper with, no persistent caching of user data and server-side control of Zimlet mash-ups. A Zimlet is a "zipped" bundle of content that is deployed to the ZCS server by the Zimlet management tool. (What is a, 2009) "Zimlets and other mash-ups are precluded from accessing arbitrary services on the Internet. This means the ZCS server can act as a secure, proxy gateway for accessing intranet applications, and can govern which web services are accessible for mash-up within the Zimbra Ajax web client." (Zimbra email and, n.d.)

The Zimbra Mobile Web client offers the administrator the ability to remote wipe the device in their Zimbra 6.0 version and later. The ability to wipe the device of all emails, contacts and calendar entries synced to a smartphone does not guarantee there is still data on the device.

After researching the software vendor and on the World Wide Web, there was no information available whether information loaded to the device's hard drive is also wiped with the remote command. This is a concern since there was a security vulnerability that "allowed unauthorized, remote access to files that are readable by the "Zimbra user" account on the ZCS Mailbox server." (Sanders, 2009) In addition, another security vulnerability was passwords used to log into email through the Zimbra client were sending clear text rather than encrypted text. (Leffall, 2008) ZCS is an open source application, which means development is abundant so issues are quickly resolved. ""It is commonly believed that more "critical eyes" are examining open source software in its development and debugging"" Security patches are issued in closer time units to the discovery of the vulnerability. (Altinkemer, Rees, & Sridhar, 2005)

There are a number of third-party applications provided by vendors to allow employees of business to be more mobile, but researching and finding the best solution is difficult. Some users want more responsive and friendly smartphones, but these devices are not considered business essential. The best smartphones for business users evaluated to suit the needs of power business users are the LG Expo, Nokia E72, Motorola Droid, RIM BlackBerry Bold 9700 and the HTC Touch Pro 2. The devices users are requesting such as the iPhone 4, Motorola Droid X and the HTC Thunderbolt are known more for social networking and for aesthetic. (Cha, 2010) Individuals requesting these types of devices are not looking for business functionality; otherwise, the phones evaluated for business use would be the device of choice.

The Zimbra Mobile Web client has been shown to have vulnerabilities. The Zimbra Collaboration Suite is an Ajax-based application for messaging and collaboration. "Ajax is a group of interrelated web development methods used on the client-side to create interactive web applications. With Ajax, web applications can retrieve data from the server asynchronously in

the background without interfering with the display and behavior of the existing page." (Ajax (programming), 2011) The Ajax-based application is prone to an HTML-injection vulnerability because it fails to properly sanitize user-supplied input when handling electronic mail attachments. This allows an attacker to steal cookie-based authentication credentials. This exploit also allows an attacker to control how the website is shown to the user. The script injection also allows other attacks to be possible. (Zimbra collaboration suite, 2010) Updating the affected versions of Zimbra Collaboration Suite, 4.0.3 and 4.5.6, may not guarantee a resolution since other versions may also be vulnerable as well.

Bluetooth Exploits

Bluetooth technology has been around since 1994 and was created by the telecom vendor Ericsson. Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances, approximately 30 feet, using low-power wavelength radio transmissions to wirelessly link phones, computers and other network devices. When a Bluetooth capable device is enabled, it "pairs" up with another Bluetooth capable device creating a personal area network (PAN). Some Bluetooth devices can "pair" up with multiple devices. There are two standards for Bluetooth, 1.0 and 2.0. Bluetooth 1.0 has a maximum transfer speed of 1 megabit per second (Mbps) while Bluetooth 2.0 has a maximum transfer speed of three Mbps. Bluetooth 2.0 is backward compatible with 1.0 devices.

A smartphone owner needs to be aware of the security vulnerability with Bluetooth technology. There are several methods used by hackers to obtain information from a Bluetooth enabled device and it is more important these days to turn off the Bluetooth when not in use or in certain public area such as airports and shopping centers. There are different names to these

attacks, BlueJacking, BlueSnarfing, and BlueBugging, but they all have one thing in common, Bluetooth. "Two security researchers created a collection of hacks they called BlueSnarfing that enabled them to stealthily duplicate the address book, call records, photos and text messaging from certain phone models." (Brandt, 2004) In another demonstration, the two researchers forced a targeted phone to call a phone of their own choosing. This attack is called BlueBugging since it transforms the victim's phone into a bugging device. The last Bluetooth attack, BlueJacking, is not as severe. BlueJacking refers to transmission of unsolicited messages to other Bluetooth devices in the network. (Brandt, 2004)

The only assurance to secure Bluetooth is by disabling this feature or using a wired handset for the device when dealing with a personal smartphone. Dealing with the security vulnerability of Bluetooth in the corporate world is much simpler; Information Technology personnel can alleviate such concern by disabling this feature through the management console of the third party application installed on the smartphone.

Download Exploits

As with any owner of a smartphone, the individual will tend to download application(s) that may be beneficial from application stores such as Apple's Apps Store or the Android Market. Some of these applications may be trustworthy while others may not. It was only recently that Google pulled 50 applications from their Android Market. These applications were pulled because they were repackaged versions of an existing Android application that contain virus code. Geinimi, one of the 50 applications that were pulled was a Trojan capable of compromising personal data on users' smartphones and then sending it to a remote server. (Georgescu, 2010) A mobile security company, Lookout Mobile Security, stated they did not

know the real motive of Geinimi, but they believe the most probable use is for either a malicious ad network or an attempt to create a botnet for Android. Although applications for smartphones are regulated by Android Market or Apple's Apps store, it does not mean a user will follow the guidelines.

Apple's iPhone is also not impervious to malicious applications. Even though Apple regulates the development of their applications, iPhone owners that download their applications from the Apple's Apps store may also encounter their fair share of malicious applications. A researcher from the Swiss University of Applied Sciences (HEIG-VD) has discovered Apple's iPhone app review process is inadequate to stop malicious apps from being distributed to the millions of iPhone users. The malicious application could be hidden within an innocent app such as a game that has the ability to access the stored data on the device. The researcher, Nicolas Seriot, proved this concept by creating an open-source proof-of-concept spyware he called "SpyPhone". This application had the ability to access the 20 most recent Safari searches, YouTube history and e-mail account information such as username, e-mail address, host and login of the device. The malicious application also displayed detailed information about the phone that can be used to track users even if they change devices. (Mills, 2010)

There is also the question of jailbroken iPhones. IPhone users who download applications from websites other then the Apps store such as Cydia (http://cydia.saurik.com) are also susceptible to malicious applications. Website such as Cydia has apps that were rejected by Apple for one reason or another.

CHAPTER 4: INCREASING SECURITY AND SECURING SMARTPHONES

Despite the sad state of mobile device security, informing users of these potential flaws will educate the owners of these devices of the vulnerabilities that may compromise their privacy. Performing such tasks will demonstrate to the users of these devices that it may be more prudent for them that other measures for security should be implemented. Technology is advancing at a rapid rate that it only invites individuals who are looking to make an immediate impact to their bank account will spend time to think of unscrupulous ways of defrauding individuals. Since smartphones are becoming a dime a dozen, everyone who owns a device may store pertinent information such as pin number to their ATM card or possible their bank account number or even their credit card number. Owners of devices who store such data should be more paranoid with their devices and it is wise to be on the side of error by considering a third party application be installed where if the phone was ever lost, the data on the device can be remotely erased. (Pinola, n.d.)

Security is always a huge concern for any company. Information Technology personnel bear many responsibilities on their shoulder and as technology advances, organizations face an increased number of threats from hackers, Trojans, viruses and malwares. As with any Information Technology personnel, the concern of unauthorized access to one's network is a nightmare and being that smartphones are an integral part of a business in today's world, network security now extends to the company's smartphones. The demand for employees to be mobile and have the ability to stay connected to the company; companies have implemented security policies to protect their network infrastructure and information store on these devices by installing software applications such as Good Mobile Messaging, BlackBerry Enterprise Server and Zimbra Collaboration Server to protect enterprise data. It has been shown there is more of

an urgent need for mobile security these days because a recent poll shows 44 percent of 6,000 smartphone and tablet users use their devices for both personal and business purposes. (Shukla, 2010) Even though security policy has been deployed to these smartphones, the first line of defense falls upon educating and training the users regarding security.

As smartphones become more popular, they become more of a target for hackers. Smartphones are essentially small computers so they also are vulnerable to Trojans, viruses, spywares and malwares. Just as an operating system on a server or workstation, smartphones operating systems need to be updated in a timely fashion. When security vulnerabilities are discovered, manufacturers quickly patch the issue by releasing an update for the operating system. The need for security has become a top priority since smartphones are an extension of a company's network containing enterprise data. It is necessary in today's world that Information Technology personnel do whatever it takes to secure these devices and mitigate the damage that can be done due to unauthorized access.

Recommendations

There is no guarantee that the data on a smartphone will not ever fall into mischievous and malicious hands. In order to secure the data on smartphones, users need to be more diligent in protecting their devices. As with any company asset, the directives of the company's policies and consequences of violating those policies are reviewed, agreed and signed by the user. The following are recommendations to improve the security risk(s) and vulnerabilities companies face with smartphones.

The first recommendation is to review all the features of the smartphone and disable any feature on the device deemed not critical to complete the company's mission. This means

blocking SMS (Short Message Service), application downloads, and disabling the Bluetooth and infrared, etc.

The second recommendation is to mandate training to all users prior to being issued a company smartphone. A thorough training session will educate the user how to use the device efficiently and effectively. This is the first step in protecting the company's asset and the securing the network from unauthorized access.

The third recommendation is to inform users that these phones are company assets and as such, there will be no unauthorized download and installation of application without written approval from senior management. Informing and emphasizing to the user that the smartphone is company asset, the mindset of using the device for personal will not be an issue.

A final recommendation is to inform users that these smartphones will need to be returned back to the company on a regular basis, possibly every three months, so an audit team may review and audit the device for unauthorized applications and any stored enterprise data. A complete format of the device may be necessary to remove any unauthorized applications and/or stored enterprise data.

As with any recommendations, policies need to come from senior management. Policies may be recommended, but without the support of senior management, it is futile.

References

Ajax (programming). (2011, March 12). Retrieved from http://en.wikipedia.org/wiki/Ajax_(programming)

Approvals and certifications. (n.d.). Retrieved from http://us.blackberry.com/ataglance/security/certifications.jsp

Blackberry enterprise server features. (n.d.). Retrieved from http://us.blackberry.com/apps-software/business/server/full/features.jsp#tab_tab_security

Choosing a processor. (n.d.). Retrieved from http://www.build-a-computer-guide.com/Chosingaprocessor.htm

CheckPoint Software Technologies LTD. (n.d) Pointsec Mobile Security. Retrieved from http://www.checkpoint.com/products/datasecurity/mobile

Forgot your iphone passcode? learn to bypass it.. (n.d.). Retrieved from http://www.machoe.com/110/forgot-your-iphone-passcode-learn-to-bypass-it.html

History of cell phones. (n.d.). Retrieved from http://www.historyofcellphones.net

Good mobile message - security bulletin. (2009, February 13). Retrieved from http://www.good.com/faq/18431.html

Good mobile messaging. (n.d.). Retrieved from http://www.good.com/products/good-mobile-messaging.php

Good technology, inc.. (2011, February 19). Retrieved from http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=438185

Mobile services. (n.d.). Retrieved from http://www.mirapoint.com/index.php?id=mobile

Smartphone. (2011, April 27). Retrieved from http://en.wikipedia.org/wiki/Smartphone

What is a zimlet. (2009, July 15). Retrieved from http://wiki.zimbra.com/wiki/What_is_a_Zimlet

Zimbra collaboration server mobility. (n.d.). Retrieved from http://www.zimbra.com/products/mobility.html

Zimbra collaboration suite html injection vulnerability. (2010, November 15). Retrieved from http://www.juniper.net/security/auto/vulnerabilities/vuln28134.html

Zimbra email and collaboration server. (n.d.). Retrieved from http://www.zimbra.com/products/secure-email-anti-spam.html

Abrams, Randy. (2010, August 25). The strange case of the droid 2 password lock [Web log message]. Retrieved from http://blog.eset.com/2010/08/25/the-strange-case-of-the-droid-2-password-lock

Adimoga, . (2010, September 17). Comparison computer storage space. Retrieved from http://www.warepin.com/comparison-computer-storage-space

Admin. (2009, November 9). Security vulnerability on jailbroken iphone in Australia. Retrieved from http://iphone.1800pocketpc.com/2009/11/09/security-vulnerability-on-jailbroken-iphone-in-australia.html

Ahmed, Mansoor. (n.d.). Security flaw found in motorola droid 2. Retrieved from http://www.worsttech.com/bug-report/droid2-security-flaw-bypass-passcode-1105360.html

Altinkemer, Kemal, Rees, Jackie, & Sridhar, Sanjay. (2005). Vulnerabilities and patches of open source software: an emperical study. Unpublished manuscript, Krannert Graduate School of Management, Purdue University, West Lafayette, Indiana. Retrieved from http://www.krannert.purdue.edu/academics/mis/workshop/ars_092305.pdf

BBC. (n.d.). Is your smartphone safe enough? Retrieved from http://www.fellowgeek.com/a-Is-your-Smartphone-Safe-Enough.html

Blake. (2010, November 10). Spoofed android apps can bypass security permissions. Retrieved from http://www.intomobile.com/2010/11/10/android-security-bug-spoof-app

Brandt, Andrew. (2004, October 29). *Privacy watch: cell phones get chatty with hackers*. Retrieved from http://www.pcworld.com/article/118236/privacy_watch_cell_phones_get_chatty_with_hackers.html

Bright, Peter. (2011, February 28). Malware in android market highlights google's vulnerability. Retrieved from http://arstechnica.com/open-source/news/2011/03/malware-in-android-market-highlights-googles-vulnerability.ars

Cha, Bonnie. (2010, January 28). *Best smartphones for business users*. Retrieved from http://reviews.cnet.com/4321-6452_7-6544038.htm

Chen, Brian X. (2009, July 31). Apple patches iphone sms security hole with software update. Retrieved from http://www.wired.com/gadgetlab/2009/07/apple-patch-sms

Chen, Brian X. (2011, April 7). Creepy bug gives some iphones unwanted face time. Retrieved from http://www.wired.com/gadgetlab/20011/04/creepy-iphone-bug

Cormier, Kristin. (2010, May 10). Android popularity passes apple iphone. Retrieved from http://www.examiner.com/online-marketing-in-dallas/android-popularity-passes-apple-iphone

CNXsoft (2011, April 11). Android to get 50% of smartphones market share by 2012. Retrieved from http://www.cnx-software.com/2011/04/11/android-to-get-50-of-smartphones-market-share-by-2012

Dunn, John E. (2010, October 4). Blackberry backup encryption broken by russians. Retrieved from http://www.pcworld.com/article/206854/blackberry_backup_encryption_broken_by_russian.html

Filho, Salomao. (2010, October 25). Bypass password on a locked iphone ios 4.1 "security problem". Retrieved from http://www.ihelplounge.com/ihelplounge/2010/10/bypass-password-on-a-locked-iphone-ios-41-security-problemvideo.html#axzz1D2onWNWI

Georgescu, Iohana. (2010, December 31). Android trojan recently discovered. Retrieved from http://www.metrolic.com/android-trojan-recently-discovered-154803

Hamblen, Matt. (2010, May 9). Brace for smartphone explosion. Retrieved from http://www.pcworld.com/article/195832/brace_for_smartphone_explosion.html

Hicks, Sarah. (2006, April) Mobile and malicious: security for mobile devices – best practices and technologies. Retrieved from http://www.enterprisenetworksandservers.com/monthly/art.php?2153

Hill, Kashmir. (2010, February 9). Yet another reason to password-protect your smartphone. Retrieved from http://trueslant.com/KashmirHill/2010/02/09/yet-another-reason-to-password-protect-your-smartphone

Isaac, Mike. (2011, January 31). Android os now world's leading smartphone platform. Retrieved from http://www.wired.com/gadgetlab/2011/01/android-os-leading-smartphone

Kincaid, Jason. (2011, January 11). Security flaw makes it easy to bypass verizon droid screen lock. Retrieved from http://techcrunch.com/2010/01/11/verizon-droid-security-bug

Krebs, Brian. (2008, July 2). Apple iphone four months behind os x in patches. Retrieved from http://voices.washingtonpost.com/securityfix/2008/07/apple_iphone_four_months_behin_1.html

Leffall, Jabulani. (2008, October 6). Yahoo fixing zimbra bug, integrating with exchange. Retrieved from http://campustechnology.com/articles/2008/10/yahoo-fixing-zimbra-bug-integrating-with-exchange.aspx

Manninen, JP. (2010, November 26). First windows phone 7 jailbreak tool released. Retrieved from http://venturebeat.com/2010/11/26/first-windows-phone-7-jailbreak-tool-released

Mick, Jason. (2010, June 25). Microsoft spills windows phone 7 release month. Retrieved from http://www.dailytech.com/Microsoft+Spills+Windows+Phone+7+Release+Month/article18845.htm

Mills, Elinor. (2010, February 3). Researcher warns of risks from rogue iphone apps. Retrieved from http://news.cnet.com/8301-27080_3-10446402-245.html

Naraine, Ryan. (2011, March 15). Rim: disable javascript in blackberry browser. Retrieved from http://www.zdnet.com/blog/security/rim-disable-javascript-in-blackberry-browser/8445?tag=content;selector-blogs

Ng, Alan. (2009, July 15). Htc windows mobile smartphones: bluetooth vulnerability. Retrieved from http://www.product-reviews.net/2009/07/15/htc-windows-mobile-smartphones-bluetooth-vulnerability

Orloff, Jeff. (2009, December 14). Jailbreak shows iphone apps vulnerability. Retrieved from http://www.revenews.com/jefforloff/jailbreak-shows-iphone-apps-vulnerability

Pinola, Melanie. (n.d.). Install or enable remote wipe on your smartphone now. Retrieved from http://mobileoffice.about.com/od/mobilesecurity/qt/smartphone-remote-wipe.htm

Prince, Brian. (2010, August 12). Smartphone security vulnerable to touch-screen smudges, researchers report. Retrieved from http://www.eweek.com/c/a/Security/Smartphone-Security-Vulnerable-to-Touch-Screen-Smudges-Researchers-Report-446273

Radia, R. (2011, January 17). Why you should always encrypt your smartphone. Retrieved from http://arstechnica.com/gadgets/guides/2011/01/why-you-should-always-encrypt-your-smartphone.ars

Reed, Brad. (2010, June 18). A brief history of smartphones. Retrieved from http://www.pcworld.com/article/199243/a_brief_history_of_smartphones.html

S, Jason. (2008, August 29). How to easily bypass iphone 3g screen lock password [Web log message]. Retrieved from http://jsbi.blogspot.com/2008/08/how-to-easily-bypass-iphone-3g-screen.html

Sanders, K. (2009, July 1). Zimbra critical security update [Web log message]. Retrieved from http://blog.letushostu.com/tag/zimbra

Shukla, Anuradha. (2010, October 31). Security becomes 'top priority' for smartphone users. Retrieved from http://www.pcworld.com/article/209346/security_becomes_top_priority_for_smartphone_users.html

Surf4Fun. (2011, January 19). Can iphones, androids or windows phone 7 have security vulnerabilities? [Web log message]. Retrieved from http://blogs.msdn.com/b/devschool/archive/2011/01/19/can-iphones-androids-or-windows-phone-7-have-security-vulnerabilities.aspx

Wailgum, Thomas. (2010, January 04). Smartphones: corporate shackles or tool for work-life balance?. Retrieved from http://www.cio.com/article/512486/Smartphones_Corporate_Shackles_or_Tool_for_Work_Life_Balance_

Wally, Initials. (2010, January 11). Security flaw makes it easy to bypass verizon droid screen lock. Retrieved from http://droidexperts.com/forum/general-discussions/347-security-flaw-makes-easy-bypass-verizon-droid-screen-lock.html

Withers, Stephen. (2008, August 28). Whoops! iPhone password bypass a cinch. Retrieved from http://www.itwire.com/your-it-news/mobility/20273-whoops-iphone-passcode-bypass-a-cinch

Zetter, Kim. (2006, August 5). Blackberry a juicy hacker target. Retrieved from http://www.wired.com/science/discoveries/news/2006/08/71548

Zetter, Kim. (2007, November 16). Hacked iphone no longer just a theory: demo turns iphone into spy device. Retrieved from http://www.wired.com/threatlevel/2007/11/hacked-iphone-n