Proactive and Reactive Measures Used to Secure Your Smartphone and Its Data and Smartphone Basics

Dwayne Shaffer

68-595

Security Project

Table of Contents

Chapter 1: ABSTRACT

Cellular smartphones and their associated networks are always under constant attack and the valuable data that is stored on these smartphones is often subject to being compromised by a variety of individuals every single day. Today, malware for mobile devices can delete or steal confidential information, send mass SMS and MMS messages from infected devices, dial premium-rate numbers without a user's knowledge, and transfer malicious code to a PC once a connection is established.[5] Encrypting the data on a smartphone can help to prevent your data from being compromised. Last week, California's Supreme Court reached a controversial 5-2 decision in People v. Diaz (PDF), holding that police officers may lawfully search mobile phones found on arrested individuals' persons without first obtaining a search warrant.[4] The attacks that are waged against smartphones and their associated networks can bring down an entire network, infect a smartphone with a virus, erase all the data on a smartphone and provide access to the sensitive data that is stored on a smartphone.   Numerous organizations have worked individually and collectively to secure the smartphone networks and the smartphones themselves. Privacy purists and people who worry about sensitive data on their smartphones being stolen now have a new reason for concern: Hackers have cracked the security codes for two of the world's most popular cell phone transmission standards. [3] Unfortunately, in the United States there are two major network types, several smartphone operating systems and multiple smartphone manufacturers. The major carriers in the U.S. are split between the two standards, with AT&T and T-Mobile using GSM and Verizon and Sprint Nextel using CDMA for their phones and, more recently, wireless peripherals. [1]

Regarding network types in the United States, there are GSM networks and CDMA networks, and these networks impose different types of security. The United States has several smartphone operating systems. The smartphones operating systems in the forefront include the iPhone operating system iOS, the BlackBerry 6.0 operating system, the Android operating system and the Windows Phone 7 operating system. As of January 2010 BlackBerry operating system accounted for 43%, iOS operating system accounted for 25.1% of the smart phone market, Microsoft 15.7 and Android holds 7.1%. [2] There are multiple smartphone manufacturers which include BlackBerry, Apple, HTC, Samsung, LG and Nokia just to name a few. To understand the vulnerabilities of smartphones you have to take into consideration the network, the operating system, the smartphone and the encryption algorithm used by the smartphone. Each of these factors will be dissected and explain to provide a thorough understanding of the vulnerabilities that exist and how to secure your data with the best available options. Despite the tools and techniques that will be explained people should understand that security has to be both proactive and reactive to ensure that the smartphone users, network providers, operating system publisher, and smartphone manufacturers are prepared to handle existing vulnerabilities and yet-to-be created zero day vulnerabilities. In addition, they must also continue to create new and more complex networks, operating system, smartphone devices and encryption algorithms. This will make the hackers work harder and longer to defeat existing security implementations.

Chapter 2: Introduction

This project will outline proactive and reactive measures that can be implemented to ensure that smartphones and their associated data are protected from vulnerabilities and loss of data. Measures that can be implemented to ensure your smartphone and its associated data are not compromised and can be recovered include:

- CDMA and GSM Basics
- Smartphone Wiping
- Smartphone Password Protection and Encryption
- Smartphone Data Backup
- Smartphone Locating/Tracking
- Smartphone Anti-Virus Protection
- Smartphone Software and Firmware Updates
- Smartphone Voice Encryption

Each of these topics will be discussed in relation to the smartphones operating systems in the forefront include the Android 2.2 operating system, the BlackBerry 6.0 operating system, the Apple iOS operating system and the Windows Phone 7 operating system.

Chapter 3: CDMA and GSM Basics

In the United States, there are two major network types that are used by all the cellular telephone providers. These networks are Code Division Multiple Access (CDMA) and Global System for Mobile telecommunications (GSM). These networks need to be protected at all times. If these networks are not protected the consumers of smartphones are at risk as well as the networks of the mobile service providers. According to a White Paper published by Verizon Wireless, some of today's top security issues and concerns are unauthorized systems and network access, auditability and compliance, customer data breaches, internal and external sabotage, theft of intellectual property and confidential business information and cost of mobile device administration. [31] GSM has the same security issues that are listed above for CDMA mobile networks.

3.1 CDMA

Launched commercially in 1995, the first CDMA networks provided roughly ten times more capacity than analog networks, and far more than TDMA or GSM. Besides supporting more traffic, CDMA brought mobile carriers and consumers better voice quality, broader coverage and stronger security, among other benefits. CDMA now has over a hundred million subscribers worldwide. [32] CDMA networks have some advantages and disadvantages. The advantages of CDMA include increased mobile security, concurrent conversations, CDMA can handle a large number of mobile users per MHz of bandwidth, has lower power requirements and has a larger range between cell towers than GSM networks. CDMA also has some disadvantages which include the fact that CDMA has not been around as long as GSM and CDMA does not provide international roaming.

3.2 GSM

In 1982 there was a need for a new digital mobile network because the European mobile network market was growing at a high-speed pace. Nordic Telecom and

Netherlands PTT made a proposal to the CEPT (Conference of European Post and Telecommunications) to satisfy this need with GSM. More than 700 GSM mobile networks have been established in Europe, the North America, South America, Iceland, Asia, Africa and Australasia up until now, woven together by international roaming agreements and a common bond called the "Memorandum of Understanding" (MoU) which defines the GSM standards and the different phases of its world-wide implementation. [33] GSM networks have some advantages and disadvantages. The advantages of GSM networks include international roaming, longevity, and simultaneous data and voice communications. The disadvantage of GSM include a fixed maximum cell tower range of 22 miles, users share the same bandwidth which can cause transmission interference and GSM can interfere with pacemakers and hearing aids.

Chapter 4: Smartphone Wiping

Smartphone wiping methods are used to totally remove the data from a smartphone if the smartphone is lost or stolen. This can be very important for individuals who have sensitive or classified information stored on a smartphone. Some smartphones have built-in wiping software while some smartphones do not come with such software. The smartphones that do not come with built-in smartphone wiping software can still be wiped. However, third- party software needs to be installed to perform this activity. Smartphone wiping can be completed remotely and is a very effective way of ensuring that data on the smartphone is not accessed since remote wiping a smartphone will restore the device to the condition it was in when it was first purchased. Remote wiping will wipe the data on your phone and restore all the factory settings.

When smartphones are lost or stolen, the information contained on these devices can be accessed by the individuals who find lost or stolen smartphones. When your smartphone is lost or stolen you need to be able to react quickly to ensure the data on the device is not accessed. One way to ensure that the data on your smartphone is not accessed after you determine that the smartphone is lost or stolen is to remotely wipe the smartphone. Some smartphones have wiping software installed, and some smartphones require third-party software to perform this function. The various smartphone operating systems have unique smartphone wiping software.

4.1 Wiping Android Smartphones

Android smartphones are unique in that they do not come with remote wiping software or commands installed. Therefore, if you own an Android smartphone you will have to obtain third-party software. One third-party Android wiping software application that is available via Android Market is Mobile Defense. Setting up Mobile Defense is very simple and the steps are listed below.

There are prerequisites to installing Mobile Defense. The first prerequisite is to setup a Mobile Defense account. The second prerequisite is to have root access to your Android smartphone. The third prerequisite is to have a SuperUser whitelist app installed. The forth prerequisite is to have a working knowledge of Android Debug Bridge (adb).

Once you have completed the prerequisites you can begin to start the setup of Mobile Defense. Some of the steps listed below are not required depending on how you want to setup Mobile Defense. However, if the additional steps listed below are completed the installer will not encounter and issues with the install.

Step 1: If Mobile Defense was previously installed the uninstall procedure should be followed to remove the current install.

Step 2: Download the Mobile Defense software to your computer from the following link: com.neevo.mobiledefense.apk.

Step 3: Ensure that the SHA1 and MD5 from the downloaded file match the SHA1 and MD5 listed below.

SHA1 9cc864ad705e73539f1739818e07e55b173db71e

MD5 ecb22a931016df21ee93ee31d9ac4bff

Step 4: Open a command prompt or terminal window and start a remote shell. This can be done with the following command: adb shell.

Step 5: Enable or start a root user. This can be completed with the following command: su.

Step 6: Ensure the system partition is remounted as read-write. The command to do this is: mount -o remount,rw -t yaffs2 /dev/block/mtdblock3 /system.

Step 7: Alter the permissions on the system app directory , this will allow you to add new APKs. The following command will allow you to complete this task: chmod 777 /system/app.

Step 8: Exit from root. The exit command will take you out of root.

Step 9: Get out of the remote shell. The exit command will get you out of the remote shell.

Step 10: Install Mobile Defense. Ensure that the path for the APK file is correct. Here is an example of installing Mobile Defense if you are sure you are in the directory where you downloaded the APK in Step 2: adb push com.neevo.mobiledefense.apk /system/app

Step 11: Open a command prompt or terminal window and begin a remote shell. The command to begin a remote shell is: adb shell

Step 12: Enable a root user with the su command.

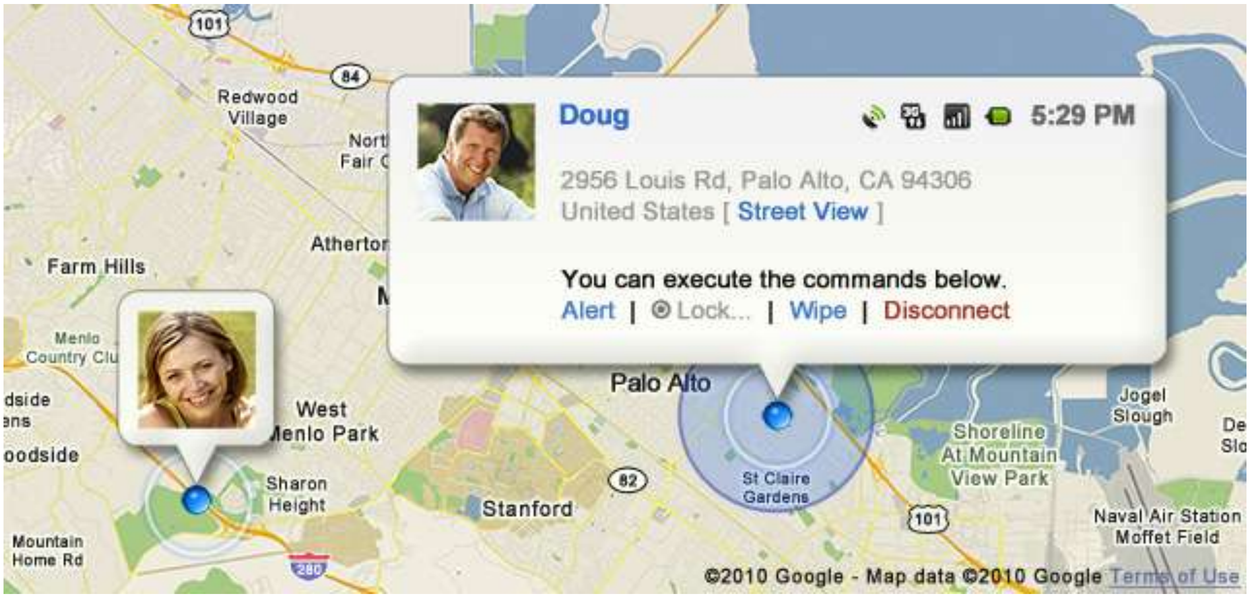
Step 13: Modify the permissions on the system app directory and change it back to the default. The command is: chmod 755 /system/app

Step 14: Ensure the system partition is remounted as read-write. The command is mount -o remount, ro -t yaffs2 /dev/block/mtdblock3 /system

Step 14: Exit from root directory. The command is exit.

Step 15: Exit from the remote shell. The command is exit

After the software has been installed and you execute the Mobile Defense software you will get a screen like Figure 2, which has a wipe button that will enable you to wipe an Android smartphone.



Doug 5:29 PM

2956 Louis Rd, Palo Alto, CA 94306
United States [Street View]

You can execute the commands below.

Alert | Lock... | Wipe | Disconnect

Figure 2: Wipe Button

4.2 Wiping BlackBerry Smartphones

BlackBerry smartphones have the ability to wipe if you have an Enterprise smartphone however; if you have an individual BlackBerry you will need third-party software to perform wiping. BlackBerry smartphones, being very enterprise-friendly devices, have a specific policy that IT administrators can turn on to enable remotely wiping a BlackBerry to factory defaults.[10] The IT administrator needs to change a default value to wipe a BlackBerry and this value is explained below.

4.2.1 Wiping Enterprise BlackBerry Smartphones

This rule specifies whether a BlackBerry® device resets to the default settings when it receives the Erase Data and Disable Handheld IT administration command over a wireless network. The default value is False. Change this rule to True to require a BlackBerry device to delete its stored IT policy permanently, to delete all third-party applications, and to delete all user data.

4.2.2 Wiping Individual BlackBerry Smartphones

For individual BlackBerry owners there is a software program that performs wiping and that software program is Smrtguard. With Smrtguard installed on a BlackBerry, the owner can remote wipe a BlackBerry which will prevent individuals from accessing personal data if the device is lost or stolen. Smrtguard does not provide details on the install of their software on the www.smrtguard.com website. Smrtguard is not free and the cost varies depending on how you pay. Smrtguard rates are $3.99 a month, $22.99 for six months or $44.99 for a year.

4.3 Wiping iPhone Smartphones

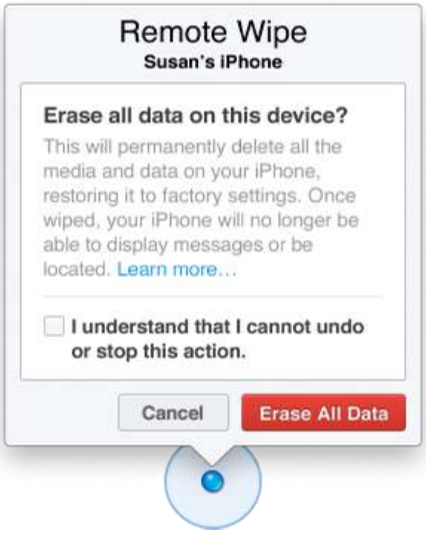
Apple smartphones have wiping software and commands installed. However, you must sign up for and activate a MobileMe account with your Apple smartphone. In addition, you must have iPhone operating system iOS 3.0 or higher installed. Should you ever lose your iPhone, you can log in to your MobileMe account on the Web and issue a remote command to securely wipe the phone's data, making it unrecoverable.[16] Setting up a MobileMe account is very simple and the steps are listed below.

Setting up Find My iPhone requires several steps:

- You must set up a MobileMe e-mail account in the iPhone Mail app.
- You must enable Push for that MobileMe e-mail account.

- You must enable Find My iPhone for that MobileMe e-mail account (Settings: Mail, Contacts, Calendars): [MobileMe account name].
- Your iPhone must be connected to the Internet whether via EDGE, 3G, 4G or Wi-Fi.

After the MobileMe is setup you can log into the MobileMe account and wipe the iPhone. You will see a screen like Figure 1 below when you want to wipe and iPhone.



Remote Wipe

Susan's iPhone

Erase all data on this device?

This will permanently delete all the media and data on your iPhone, restoring it to factory settings. Once wiped, your iPhone will no longer be able to display messages or be located. Learn more…

□ I understand that I cannot undo or stop this action.

Figure 1: Apple Remote Wiping

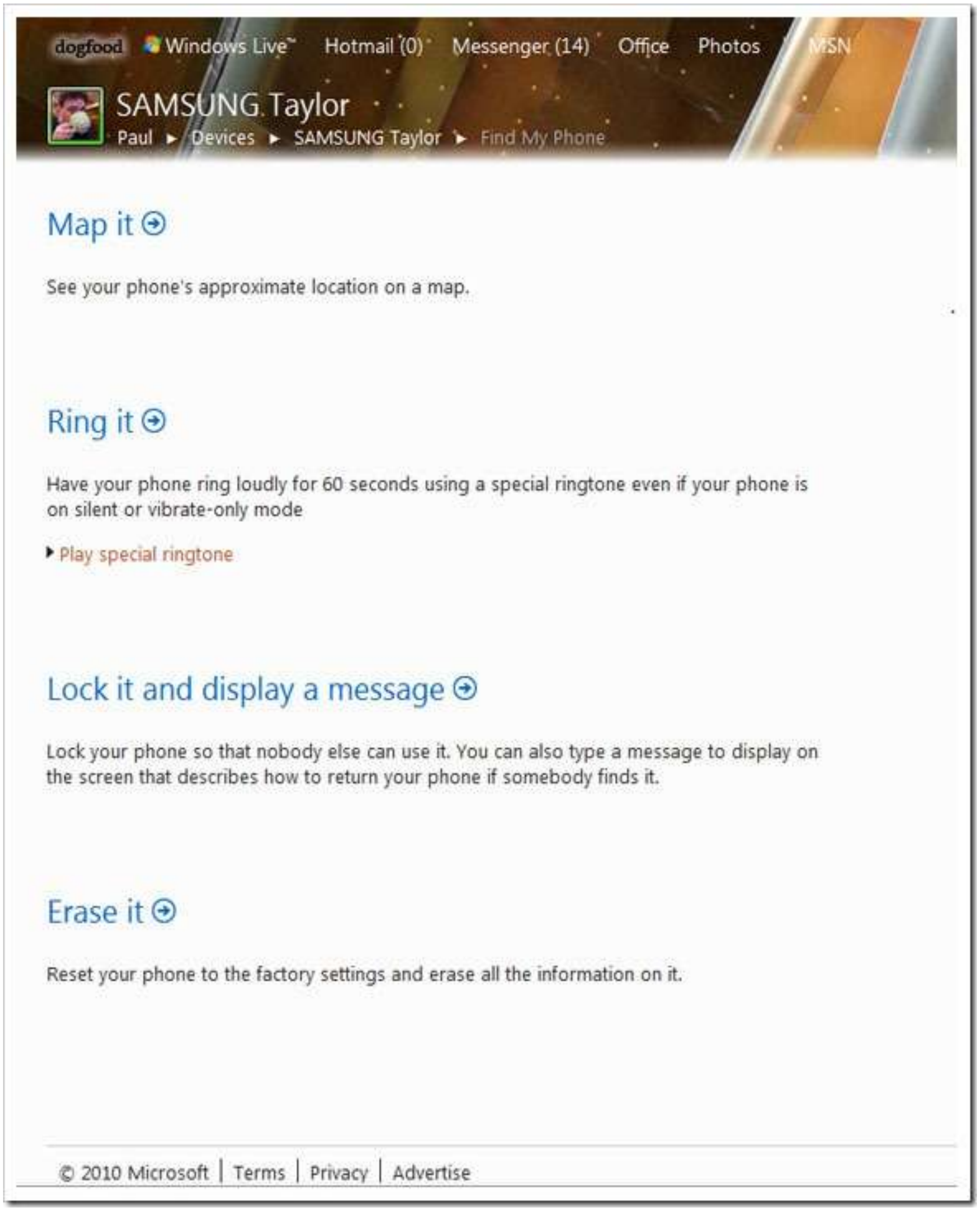
There are a couple of things to consider when wiping an iPhone. The first thing to consider is if you complete a wiping of your iPhone you will not be able to use the Find MY iPhone application to locate an iPhone. The second thing to remember is if you recover your iPhone after a wiping it will only restore your iPhone to the last time the device was synced and backup. Therefore, frequent backups and syncs are recommended.

4.4 Wiping Windows Smartphones

Windows smartphones come installed with wiping software that enables smartphone with Windows operating systems to remotely wipe the phones of any data. Windows Phone 7 can wipe Windows Phone 7 devices via Microsoft Business Productivity Online Standard Suite (BPOS) which can be used for Enterprise smartphones. However, individual smartphone will require a third-party software suite like Smrtguard. To setup Enterprise remote wiping the following setups need to be followed. The steps were received from the video link below.

- Install Outlook Web Access and login to Outlook Web Access
- Go to options on Outlook Web Access, Mobile Devices.
- Wipe all data from device
- Remove the wiped device from the list after the wiping or it will continue to wipe the device over and over again.

The device also needs to be setup for wiping and this is done by signing in to Windows Live ID, going to settings, email account and Outlook user account. This is where you sync and enable the wiping function for this particular device. The link below provides a video of how to wipe a Windows smartphone. Figure 3 below is a screen-print of what you will see when you complete a wiping of a Windows smartphone.



Map it ⊕

See your phone's approximate location on a map.

Ring it ⊕

Have your phone ring loudly for 60 seconds using a special ringtone even if your phone is on silent or vibrate-only mode

Lock it and display a message ⊕

Lock your phone so that nobody else can use it. You can also type a message to display on the screen that describes how to return your phone if somebody finds it.

Erase it ⊕

Reset your phone to the factory settings and erase all the information on it.

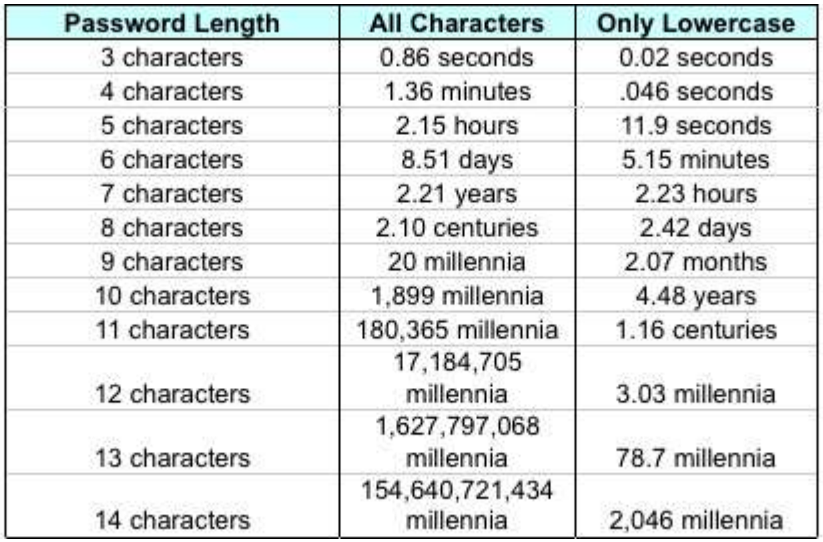
Figure 3: Windows Phone Wiping

Chapter: 5 Smartphone Password Protection and Encryption

Password protecting a smartphone is very important. Once a smartphone is lost or stolen, the first thing the thief or finder of the smartphone will try to do is access the data on a smartphone. This can be for nefarious reasons or to simply try and locate the owner of the smartphone. The owner of the smartphone never knows the reason why the thief or finder of the smartphone wants to access the information and is best suited password-protecting the smartphone. This is usually the first defense against gaining access to the data on a smartphone. Some passwords encrypt the data on a smartphone and provide a way to prevent most individuals from accessing the phone data and functions without knowing the password.

If the owner of a smartphones values the information that is in the smartphone, then the owner should password protect the smartphone. The various smartphones that are being discussed in this paper have different password requirements and different ways to set the passwords and each type of smartphone will be discussed. The passwords that are used to login to a smartphone can encrypt the data and add a layer of protection to prevent unauthorized individuals from access the data on a smartphone. The longer and more complex the password, the harder it will be to determine the password. However, the easier the password, the faster it can be determined. And how fast could this be done? Well, that depends on three main things: the length and complexity of your password, the speed of the hacker's computer, and the speed of the hacker's Internet connection.[21] The data below in

Figure 4 is for passwords that are not in the dictionary and a basic computer was used not a super computer.

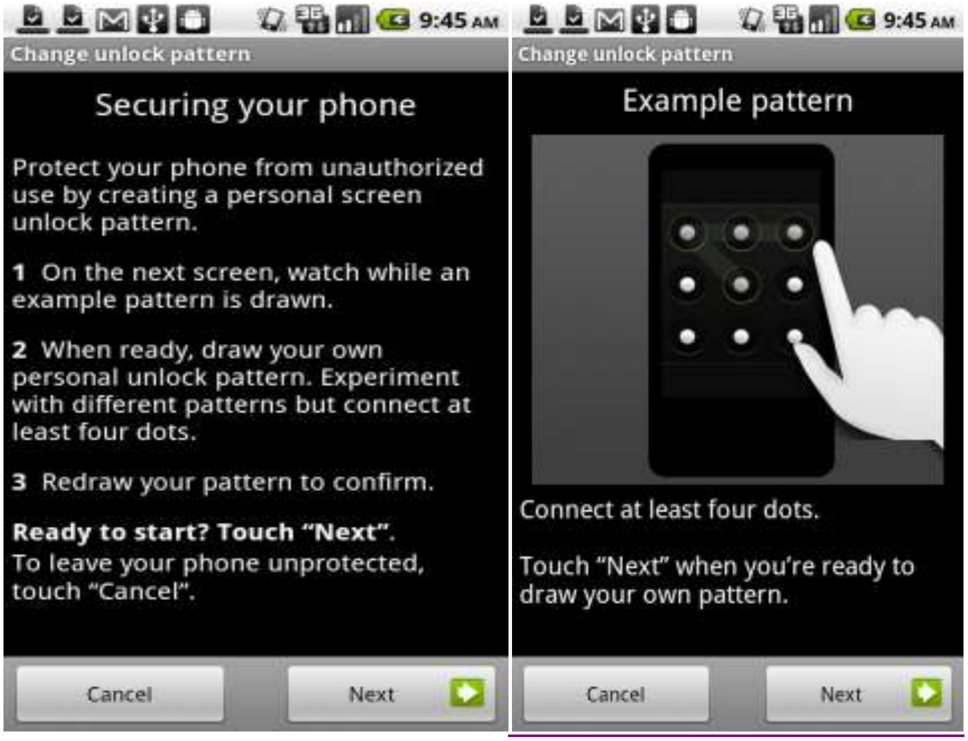


Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Figure 4: Time to Crack Passwords

5.1 Android Smartphone Password Protection and Encryption

Android phones can also be password-protected. Android phones can be password-protected by two methods. One method is a pattern lock which allows the user to draw a pattern on the touch screen by connecting at least four dots. The other password protection method is by inputting a password. To set a password with an Android phone the user needs to do the following steps. To get to the security options, tap the menu button from the home screen, then choose Settings>Security>Screen lock.[20] The Android phones allow for locking interval of immediately, five minutes or ten minutes. Android phone can setup password by going to security settings and set up screen lock. The Android smartphone password can be set with up to 16 characters that can include numbers, letters and special characters. Figure 5, displays the procedure for password protecting an Android smartphone. The password does not provide any encryption and if you want to encrypt the data on your Android you need to use a third-party application. AnDisk is an application that will encrypt the data on an Android smartphone however; there is a cost of $3.99 for this application that can be found in the Android Market.



Change unlock pattern

Securing your phone

Protect your phone from unauthorized use by creating a personal screen unlock pattern.

1 On the next screen, watch while an example pattern is drawn.

2 When ready, draw your own personal unlock pattern. Experiment with different patterns but connect at least four dots.

3 Redraw your pattern to confirm.

Ready to start? Touch “Next”.
To leave your phone unprotected, touch “Cancel”.

Change unlock pattern

Example pattern

Connect at least four dots.

Touch “Next” when you’re ready to draw your own pattern.

Figure 5: Android Password Options

5.2 BlackBerry Smartphone Password Protection and Encryption

BlackBerry phones can likewise be password-protected. The BlackBerry Tour can have a password that is as long as 32 characters. BlackBerry passwords can use numbers, letters and special characters. The minimum password has to be at least four characters. There are two interesting things with regard to BlackBerry smartphone passwords. One is that you cannot use certain patterns. If you try to use the password 1111 it will not allow you to use this password because of the repeat pattern of ones. This was attempted on a BlackBerry Tour unsuccessfully. The second is that you can have the password protection enabled by holstering the phone. This means that you can lock your BlackBerry by holstering a BlackBerry smartphone in a BlackBerry smartphone holster. The magnet in the BlackBerry smartphone holster enables the locking of a BlackBerry smartphone. To set the password you need to go to Options, Password and Change Password. You can also set the number of password attempts to 10. If you do not get the password right after 10 tries the device will delete all the data. Therefore you need to remember the password and do frequent backups. The security timeout can be set to 1, 2, 5, 10, 15, 20, 30 and 60 minutes. This is the amount of time before the BlackBerry smartphone automatically locks itself. Blackberry smartphones can encrypt data with AES and Triple DES to protect the data on a smartphone.

5.3 iPhone Smartphone Password Protection and Encryption

Apple iPhones can be password protected and the steps to protect an iPhone will be explained. iPhones can have passwords however, they also need to have the password feature enabled. The iPhone can be set to auto lock at intervals which range from one to five minutes or never. In addition, the iPhone can have a simple or complex password**.** Simple Passcode**.** As noted above, the iPhone 4 relies on a simple four-digit numeric passcode by default. For better security, turn off the Simple

Passcode option. Once the Simple Passcode option is disabled, the iPhone will request a new password which can be significantly longer than four characters, and can be comprised of uppercase and lowercase letters, numbers, and special characters.[19] The iPhone does accept more complex passcodes which can use special characters and letters however, this function must be enabled in passcode locking. Apple documentation did not state how complex the passcode can be, however passcodes as long as 20 characters were attempted without an issue. To enable the passcode feature you need to go to Settings, General and turn passcode lock on. There is an additional passcode feature that iPhones have that some individuals may or may not want to use. This feature can erase all the data on an iPhone if there are ten failed passcode attempts. That being said you need to remember your password and complete frequent backups. Once the passcode is used on an iPhone the data is encrypted with 256-bit AES and the full disk is encrypted.

5.4 Windows Smartphone Password Protection and Encryption

Windows smartphones also have password protection. Windows smartphones can use any combination of letters, number or special characters to setup a password. There is a four character minimum limit regarding passwords. You have the option of setting the lock timeout to the following values, 30 seconds, 1 minute, 3 minutes, 5 minutes, or never. This is the amount of time before the Windows smartphone automatically locks itself.

Below are the steps to setup or change a password on a Windows smartphone.

Step 1: From the start move to the left to the Applications list and then press Settings.

Step 2: Once in Settings press the Lock & Wallpaper button.

Step 3: Do one of the following to setup an initial password:

A: Turn on Password and enter a new password. Use a password that you can remember, however, you should not use your marriage date, family members' birthdays or easy passwords. Then enter your new password in the New Password text box and then re-enter it in the Confirm Password text box. You have just setup a new password and that password will be required every time your Windows smartphone is locked.

Changing a Windows smartphone password is slightly different. If your phone already has a password and you want to change it use the following steps.

Step 1: From the start move to the left to the Applications list and then press Settings.

Step 2: Once in Settings press the Lock & Wallpaper button.

Step 3: Press the Change Password button and then enter your phone's current password in the Current Password text box before entering your new password.

Step 4: Then enter your new password in the New Password text box and then re-enter it in the Confirm Password text box.

Step 5: Press Done to save your changes

You have just changes your password on a Windows smartphone.

Something I found interesting was that Windows Phone 7 allows certain smartphone functions while the phone is locked. These functions include changing the ringer volume, operating the camera and playing media files. Allowing these functions basically makes your lost phone an advanced MP3 player and may discourage someone from returning the device. When Windows smartphones are password protected they also encrypt the data and the encryption methods employed can be AES, HMACSHA1, HMACSHA256, Rfc2898DeriveBytes, SHA1 and SHA256.

Chapter 6: Smartphone Data Backup

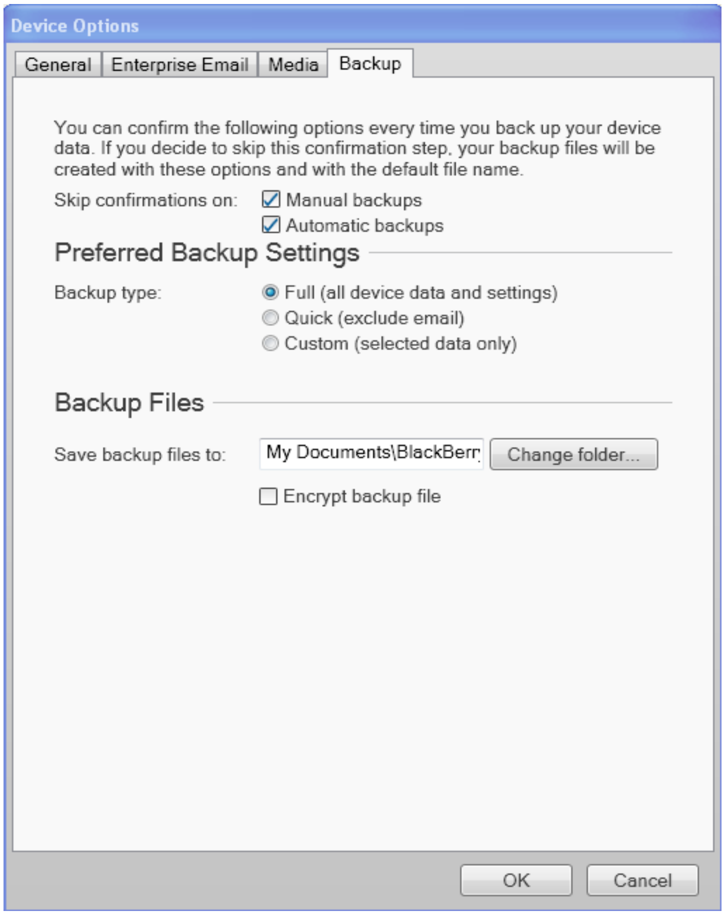
Data on a smartphone tends to be very important to the owner of the smartphone. If a smartphone needs to be reset to the original settings or is lost or stolen, a backup is required to ensure the data that existed before the smartphone was reset, lost or stolen is retrievable. Smartphone backups are a reactive way of protecting the data on a smartphone. Backups must be performed frequently and the backup interval depends on how often you add data to your smartphone and how important the data is to the smartphone owner. Backups vary based on the smartphone type. Some smartphones have backup software that comes with the device and some backups can even be encrypted. Other smartphones require third-party backup software. The backups for the following type of smartphones will be detailed: Android, BlackBerry, iPhone, and Windows.

6.1 Android Smartphone Backup

The HTC EVO is an Android smartphone from Sprint that is their first 4G smartphone. The EVO comes with HTC sync software. However, the sync software only backs up the contact information on the Evo. HTC Sync allows the Evo to backup multiple times a day, daily and weekly or specific days of the week. Android backups come in two varieties that are all-in-one and piecemeal. The all-in-one backups are not free and one of these applications is Smrtguard. The Smrtguard application starts at $2.99 a month with a one year contract and can be as high as $4.99 a month with a month to month purchase. Currently, Smrtguard for Android supports the data backup and restore of Contacts, Call Logs, SPAM Blacklist, Bookmarks, and SMS [24]. There are free piecemeal alternatives however, this requires three separate applications. Download these three apps: SMS Backup and Restore, Call Logs Backup & Restore, and APN Backup & Restore. Each one backs up its respective data to your microSD card (in /sdcard/*appname*BackupRestore/) for easy restoration on another phone. [12] In addition, you need one more application to backup the applications on your Android and the application that can do this is Astro File Manager. However, it required you to have a microSD card installed in your Android device to perform a backup. Another thing that needs to be done is to backup the data on the microSD card to a computer or portable hard drive because if the smartphone is lost or stolen with the microSD card inserted in the device there goes your backup. Regarding encryption, you have to use third-party encryption software like Bitlocker that comes with certain versions of Windows 7 or you can encrypt the entire sd card so all backups to the sd card are encrypted.

6.2 BlackBerry Smartphone Backup

BlackBerry smartphones come with backup software that is included with the BlackBerry Desktop Software. BlackBerry smartphones allow you to backup all the data and settings on the BlackBerry smartphone or specific data that is selected by the user. You can skip confirmations for manual and automatic backups. This means that once you start a backup, you will not have to click yes to confirm a backup. The location of the backup can be the default location which is My Documents/BlackBerry/Backup or a folder of the user's choosing. The frequency of the backup can be manually, daily, weekly, bi-weekly or monthly. With BlackBerry smartphones the backups can be encrypted or non-encrypted. If the backup is encrypted, the backup will require the user to input a password before the encryption and during the installation of the backup. If you forget the password associated with the backup, you will not be able to restore that encrypted backup. It is important to be mindful of the number of backups you keep in your backup folder. Previous backups are not deleted from the backup folder when new backups are added to the folder. Therefore, if you backup frequently and the backups are large you can quickly run out of hard drive space. Figure 6 shows the BlackBerry smartphone backup setting.



You can confirm the following options every time you back up your device data. If you decide to skip this confirmation step, your backup files will be created with these options and with the default file name.

Skip confirmations on: ☑ Manual backups
☑ Automatic backups

Preferred Backup Settings

Backup type: ● Full (all device data and settings)
○ Quick (exclude email)
○ Custom (selected data only)

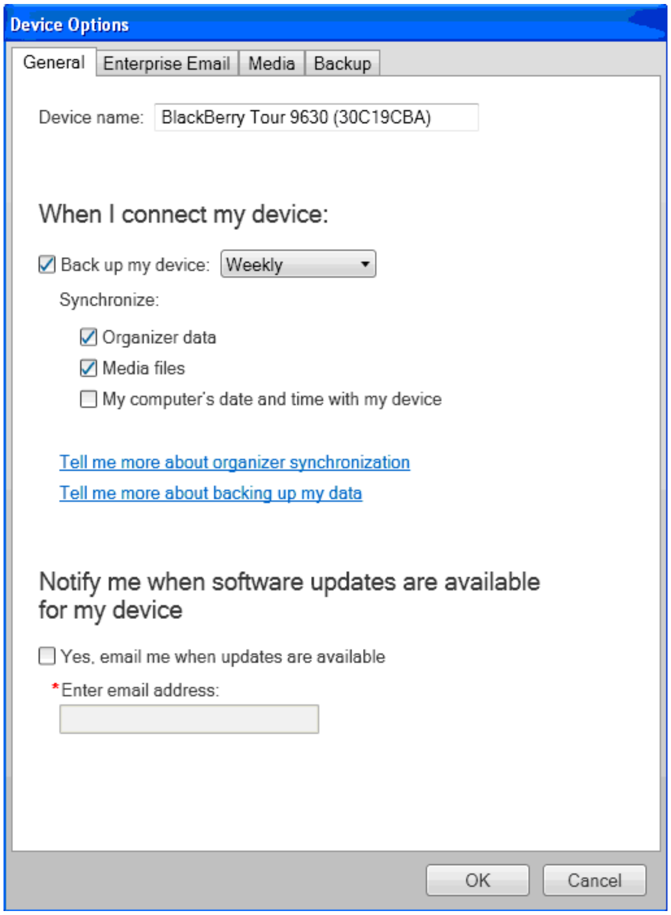
Backup Files

Save backup files to: My Documents\BlackBerr

☐ Encrypt backup file

Figure 6: BlackBerry Backup Settings

Figure 7 shows the BlackBerry smartphone Backup Frequency settings.



Device Options

Device name: BlackBerry Tour 9630 (30C19CBA)

When I connect my device:

☑ Back up my device: Weekly

Synchronize:

☑ Organizer data

☑ Media files

□ My computer's date and time with my device

Tell me more about organizer synchronization

Tell me more about backing up my data

Notify me when software updates are available for my device

□ Yes, email me when updates are available

*Enter email address:

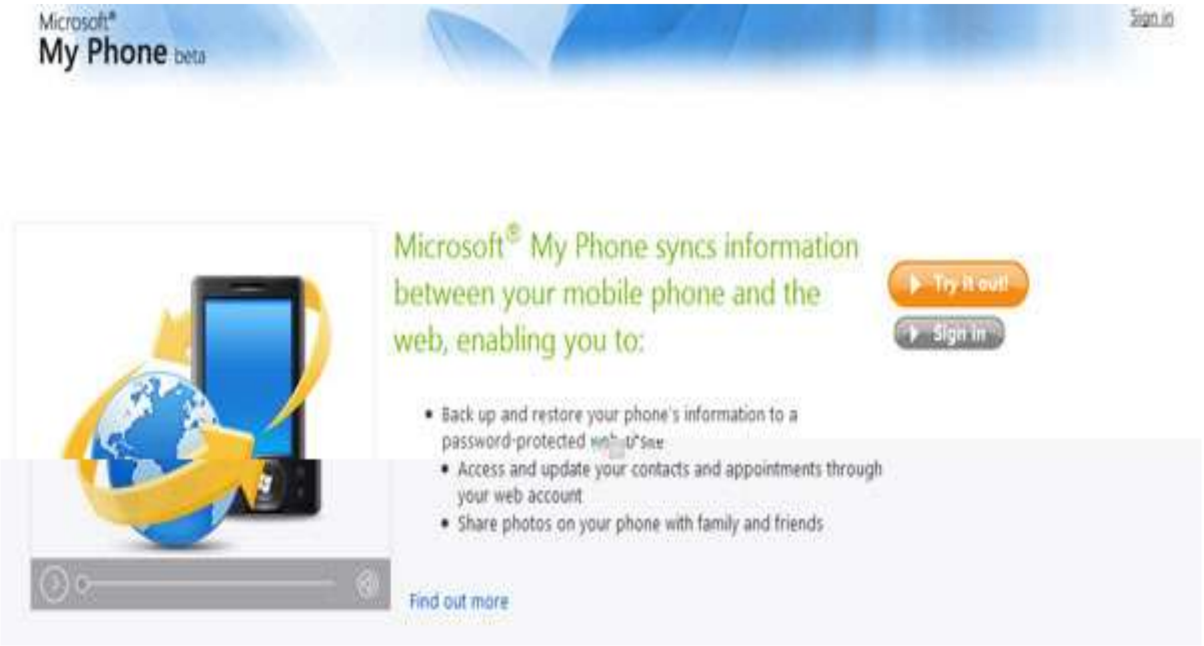
Figure 7: BlackBerry Backup Frequency

6.3 iPhone Smartphone Backup

iPhones come with backup software that is included with iTunes. iTunes attempts to perform a backup every time you connect and/or sync an iPhone. The backup for an iPhone connected to a Windows Vista or Windows 7 computer is located in the following path, \Users\Username(loginuser name) \AppData\Roaming\Apple Computer\MobileSync\Backup\. The iTunes application allows one or several backups per iPhone connected to the computer. The data that can be backed up from an iPhone is very extensive and includes just about everything on the iPhone. In addition, iPhone backups can be encrypted. When iPhone backups are encrypted, a password needs to be set for the encrypted backup and to restore an encrypted backup. If you forget the password you can continue to do backups and use the device; however you will not be able to restore the encrypted backup to any device without the password. [23]

6.4 Windows Smartphone Backup

Microsoft provides smartphone backup software that is usually installed on the Windows smartphone. The software that is available for the most recent Windows smartphones is My Phone. If My Phone is not installed on the smartphone it can be downloaded. My Phone is a great option for smaller backups because the data that is backed up to the cloud. However, My Phone provides the user 200MB of data to store on the cloud. This is usually enough to back up a smartphone unless the smartphone has a lot of media. The backup is not encrypted however, a password is required to backup and access the backup. My Phone synchronizes contacts, calendar appointments, tasks, photos, videos, text messages, music, and documents that are stored on the device. The data is backed up directly from the smartphone to the cloud if the user has internet access on the smartphone. The intervals for backing data are automatically, daily and manually. Figure 8 is a display of the Windows smartphone My Phone login screen for completing backups.



Microsoft® My Phone syncs information between your mobile phone and the web, enabling you to:

- Back up and restore your phone's information to a password-protected web site
- Access and update your contacts and appointments through your web account
- Share photos on your phone with family and friends

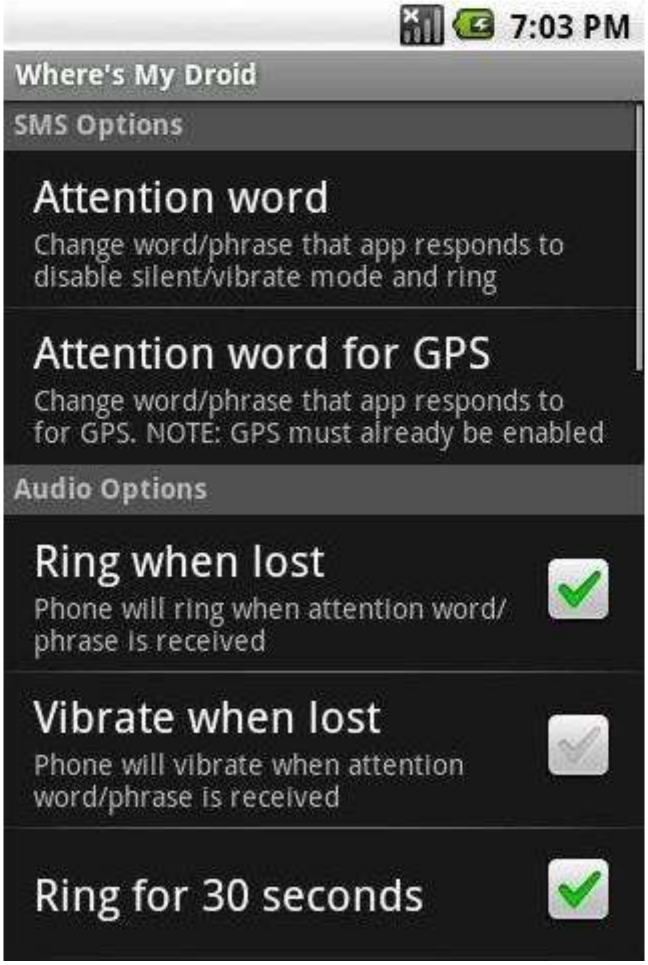
Figure 8: Microsoft My Phone Login Screen

Chapter 7: Smartphone Locating/Tracking

There are times when you want to retrieve a lost or stolen smartphone and wiping the phone can prevent this option. When you want to reclaim a lost or stolen smartphone you need smartphone locating/ tracking software. Smartphone tracking software uses the GPS location of your phone. A smartphone signal is transmitted to three satellites and trilateration is used to determine the longitude and latitude of where your smartphone is located. A simple explanation for trilateration is that you can calculate the coordinates of a given position if you know the distance from it to another three known positions in two dimensional spaces. This software can even turn your smartphone into a siren so you can narrow the location of a smartphone via sound. This is great software to have if your smartphone is lost or stolen.

7.1 Android Smartphone Locating/Tracking

Android smartphones have an application that can locate your Android smartphone of it is lost or stolen. The application that performs this function is Where's My Droid. Where's My Droid was installed on the HTC EVO however, if it is not installed on an Android smartphone running Android 1.6 or higher (minimum requirement) it can be downloaded from Android Market and the application is free. The installation process is very simple and just requires you to install the application. The setting can be changed once the installation is complete. Where's My Droid as four features that include: finding your Android smartphone by making it ring/vibrate; finding your Android smartphone using GPS location; passcode protection to prevent unauthorized app changes and using a computer to email either attention word. GPS must be enabled before these features can be utilized. The first feature is making the phone ring to help locate the phone. The options are Ring when lost, Ring for 30 seconds, Ring for 60 seconds and Ring for 5 minutes. Figure 10 shows the options that are available to make the phone ring.



7:03 PM

Where's My Droid

SMS Options

Attention word

Change word/phrase that app responds to disable silent/vibrate mode and ring

Attention word for GPS

Change word/phrase that app responds to for GPS. NOTE: GPS must already be enabled

Audio Options

Ring when lost ☑

Phone will ring when attention word/ phrase is received

Vibrate when lost □

Phone will vibrate when attention word/phrase is received

Ring for 30 seconds ☑

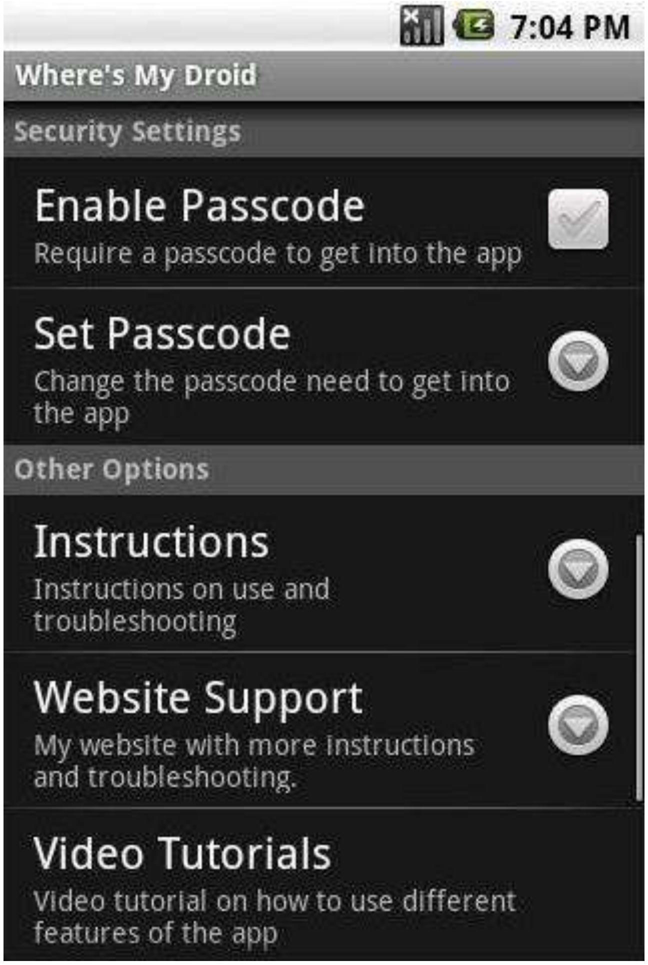
Figure 10: Ring enable Options

To make the phone ring you need to text your Attention word (password) for this function to your Android smartphone. The text can be sent from any phone. The Android smartphone will receive the text and display “PHONE FOUND!!” and ring for the amount of time that was checked in the settings. To locate your Android smartphone you need to text your Attention word (password) for this function to your Android smartphone. This can be done from any phone however, a smartphone is recommended because the reply text will contain the latitude and longitude of the Android smartphone and a link to Google Maps which will show where the Android smartphone is approximately located. The third feature is lock passcode feature which locks individuals out of the Where's My Droid main menu feature so they cannot change your setting in Where's My Droid. Figure 11 is a display of the passcode enabling and setting screen. This feature does not remotely lock the Android smartphone nor does it prevent individuals from uninstalling applications on an Android smartphone. If you want to set a passcode for the Where's My Droid application you would have to press Enable Passcode and it will require you to set a four number passcode, then you have to verify that four number passcode. The Set Passcode button allows you to change the passcode. After that the passcode will keep Where's My Droid unlocked for ten minutes. After ten minutes Where's My Droid will lock and require a passcode to unlock the features of Where's My Droid. The email Attention words to make the phone ring or to use the GPS locator perform the same way as the text message enabling of these features except the features are done via email instead of text. The application developer states that this feature has been tested on the following networks Sprint, T-Mobile and Verizon and he recommends using a Gmail account to send the emails. Other email accounts were not test and may or may not work. To email a mobile telephone number you need to use an extension after the telephone number and those extensions are listed below.

Sprint: phonenumber@messaging.sprintpcs.com

T-Mobile: phonenumber@tmomail.net

Verizon: phonenumber@vtext.com



7:04 PM

Where's My Droid

Security Settings

Enable Passcode ☑
Require a passcode to get into the app

Set Passcode
Change the passcode need to get into the app

Other Options

Instructions
Instructions on use and troubleshooting

Website Support
My website with more instructions and troubleshooting.

Video Tutorials
Video tutorial on how to use different features of the app

Figure 11: Passcode Screen

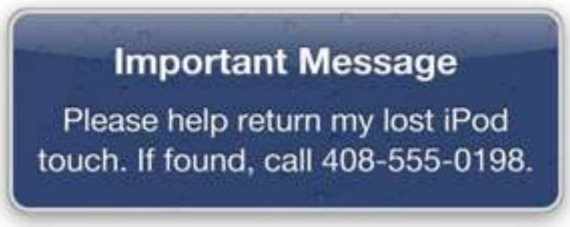
To enable the features send an email to your phone using the appropriate carriers and extensions listed above for your phone. The passcode can be put in the body or subject line of the email to either make the phone ring or to use the GPS location. The developer recommends that you remove any signature or text from the email body with the exception of the passcode. If using the ring option the Android smartphone will ring and if using the GPS option the email address used will receive and email with the latitude and longitude of the Android smartphone and a link to Google Maps which will show where the Android smartphone is approximately located. For locating/tracking software to work you need to have EDGE, 3G, 4G or Wi-Fi enabled and have a data plan, preferably an unlimited data.

7.2 BlackBerry Smartphone Locating/Tracking

The BlackBerry smartphones do not have an included application for tracking smartphone. BlackBerry App World has a BlackBerry tracking device that is free to install and use. The first step to use GPS Tracker would be to go to http://www.instamapper.com/fe?page=register and register online for an account. An email will be sent to the email account you used to register. This email will require you to click on the attached link and login to your account. Once you login to your account you will be provided a device key for your BlackBerry and you can label your device i.e. Dwayne's Blackberry, so you can determine which device you will be tracking. This is important because you might have more than one BlackBerry you want to track/locate. The second step is to visit BlackBerry App World and download GPS Tracker. Or you can download the GPS Tracker software over the air with your BlackBerry at http://www.instamapper.com/download/GPSTrackerBB.jad . Once the software is installed the third step is to enable the software your BlackBerry. This is done by clicking on the GPS Tracker icon, then clicking on the BlackBerry button and click settings. Then input the device key that was be provided when you registered your account. The last step is to visit http://www.instamapper.com/fe?page=track login into your account and click live tracking. This will display the approximate location of your BlackBerry. GPS Tracker should be set to active on startup to ensure the software is tracking. If the software is run on startup it is recommend that an unlimited data plan be include on the cellular account. The reason is because by default, your phone tries to transmit location data to InstaMapper every 5 seconds if you are moving 20 mph or faster and if someone is currently tracking you online. If you are not moving, the minimum update rate is 60 seconds. If are not being tracked online, the minimum update interval is 30 seconds.[30] For locating/tracking software to work you need to have EDGE, 3G, 4G or Wi-Fi enabled.

7.3 iPhone Smartphone Locating/Tracking

The iPhone has a program that enables the owners of iPhones to locate their phones if the phones are ever lost or stolen. The application is Find My iPhone and it can be downloaded free from the iTunes App Store. This application is free with the newest iPhone which is the iPhone4 however, it is $99 a year for older iPhones. There are other commercial applications that are available for free that work with the iPhone like GPS Tracker from InstaMapper, however, if you have the iPhone 4 MobileMe is free. The MobileMe application can be accessed by going to Setting, Mail/Contacts/Calendars, and MobileMe. Once there you can access or setup your MobileMe account and add your iPhone to your MobileMe account. This is required for you to be able to track your iPhone. MobileMe will provide an approximate location of your iPhone within a circle. The smaller the circle is the more accurate the location of the iPhone. It is important to know that the iPhone has to have Wi-Fi, EDGE or 3G enabled in order for tracking to take place. MobileMe also provides some other features that are important. The MobileMe application allows the user to remotely add a password or display a message on the iPhone. If your iPhone was not previously password protected and you determined that is was lost or stolen you can login to MobileMe from any iPhone, iPad or iPod Touch and add a password to your iPhone. You can also login into www.me.com and remotely control your iPhone. The remote message feature is also important because with this feature you can display a message like the message shown in Figure 9, iPhone Displayed Message. This message can be displayed even if the iPhone is locked. In addition, the iPhone volume can be activated to help locate the iPhone and this is activated from the MobileMe application as well. MobileMe is the application to use if your iPhone is lost or stolen and can aid in the recovery of your device.



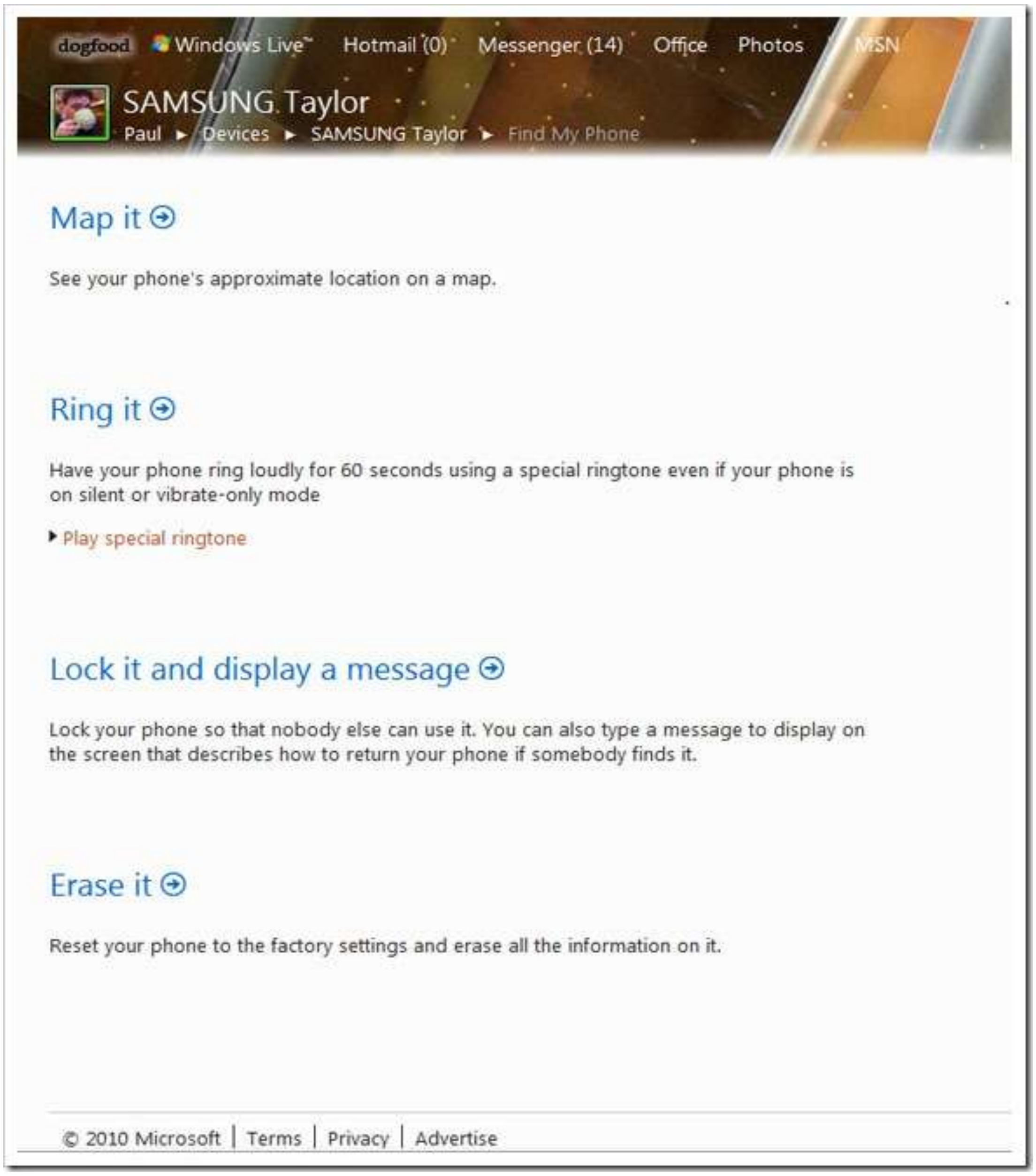
Important Message

Please help return my lost iPod touch. If found, call 408-555-0198.

Figure 9 iPhone Displayed Message

7.4 Windows Smartphone Locating/Tracking

Windows Phone with the Windows Phone 7 operating system uses the Find My Phone Software which comes with Windows Phone 7. This software can locate your Windows Phone 7 device, made your smartphone ring, lock your device, display a message and wipe your device. The wiping of a Windows Phone 7 was discussed in another section of this paper and therefore will not be discussed in this section. These features require you to have and setup a Windows Live account. From the Windows Live account you can locate your phone. A picture of the Windows Phone 7 Find My Phone Home Screen is shown below in Figure 13. This is the screen that allows you to access the feature of Find My Phone. Figure 14 below shows what the screen looks like when you want to locate your phone. The Ring it feature allows the user to turn on the ringer of the phone for 60 seconds to help locate the smartphone. Figure 15 is a display of what you will see when this feature is activated from Windows Live. The remote message and locking features is also an important because with these features you can display a message like the message shown in Figure 16: Windows Phone 7 Locking Screen. And you can also lock your device to prevent access from Find My Phone.



Map it

See your phone's approximate location on a map.

Ring it

Have your phone ring loudly for 60 seconds using a special ringtone even if your phone is on silent or vibrate-only mode

► Play special ringtone

Lock it and display a message

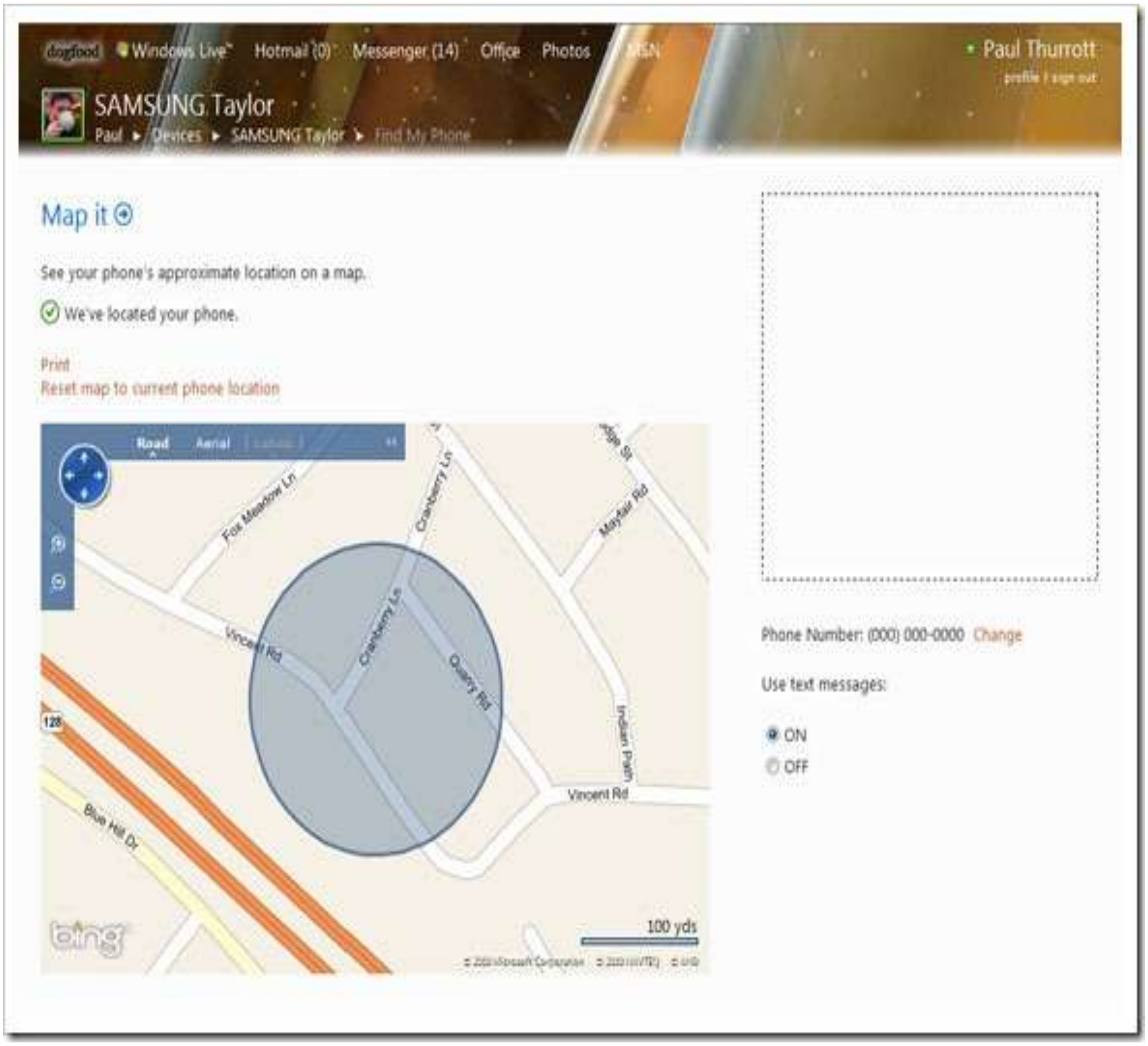
Lock your phone so that nobody else can use it. You can also type a message to display on the screen that describes how to return your phone if somebody finds it.

Erase it

Reset your phone to the factory settings and erase all the information on it.

© 2010 Microsoft | Terms | Privacy | Advertise

Figure 13: Windows Phone 7 Find My Phone Home Screen



Map it

See your phone's approximate location on a map.

✓ We've located your phone.

Print

Reset map to current phone location

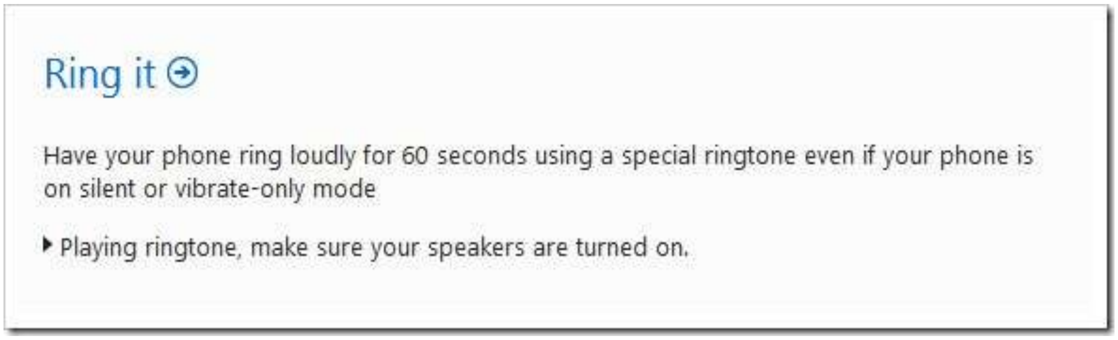
Phone Number: (000) 000-0000 Change

Use text messages:

● ON

○ OFF

Figure 14: Windows Phone 7 Locator Screen

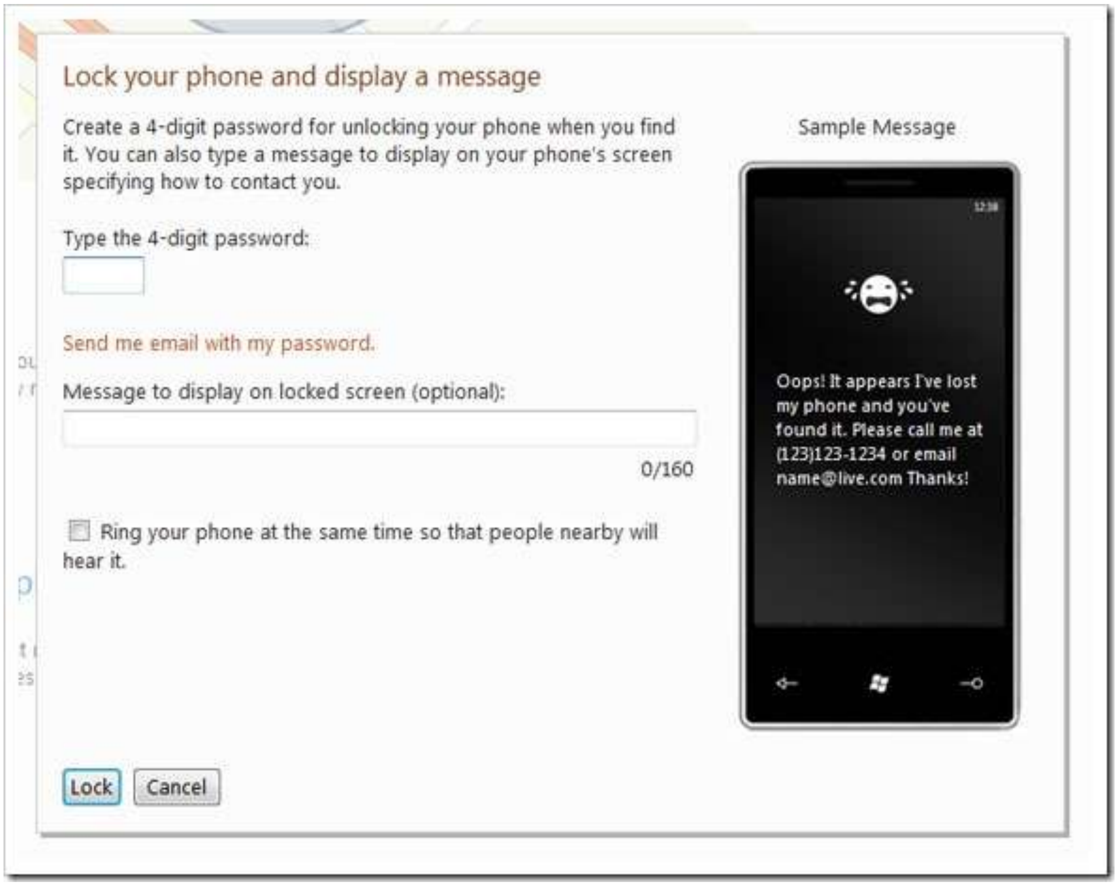


Ring it ➔

Have your phone ring loudly for 60 seconds using a special ringtone even if your phone is on silent or vibrate-only mode

▸ Playing ringtone, make sure your speakers are turned on.

Figure 15: Windows Phone Ring it Screen



Lock your phone and display a message

Create a 4-digit password for unlocking your phone when you find it. You can also type a message to display on your phone's screen specifying how to contact you.

Type the 4-digit password:

Send me email with my password.

Message to display on locked screen (optional):

0/160

□ Ring your phone at the same time so that people nearby will hear it.

Sample Message

Oops! It appears I've lost my phone and you've found it. Please call me at (123)123-1234 or email name@live.com Thanks!

Figure 16: Windows Phone 7 Locking Screen

Chapter 8: Smartphone Anti-Virus Protection

Most people are aware that computers need anti-virus protection to protect them from the malicious code in the wild that can do harm to their computer. However, smartphones require anti-virus protection as well. Smartphones can do many of things that computers do, even catch viruses and other malware. [27] Smartphone viruses can come in a variety of way and do a variety of malicious things. Viruses can record telephone calls, intercept text messages, sends text messages to for pay service providers. One virus that recently attacked the Android mobile operating systems was Trojan-SMS.AndroidOS.FakePlayer. The virus was in a program that individual thought was a media player but was far from a media player. Once on your smartphone, it fires off SMSes to premium-rate phone numbers, sending your phone bill through the roof, as well as a share of the profits from the line owners to the nasty bugmakers. [28] Another example of a smartphone virus also affected Android phones. DroidDream was recently discovered in more than 50 Android applications. DroidDream has been known to steal information from the smartphone and the program also has the ability to download malicious programs to the phone which can cause more havoc. Smartphone owners need to be proactive and reactive in preventing viruses from maliciously affecting their smartphones. Proactively smartphone users can install antivirus programs. Symantec's Mobile Security and Management is an anti-virus program that proactively protects the following smartphone operating systems including Android, Blackberry, iOS, and Windows Phone. Smartphones are similar to computer and thus they require anti-virus protection from multiple vectors. These multiple vectors include short message service, multimedia, infrared, email and Bluetooth protection. Another proactive approach to protecting your smartphone from viruses is to only download application from trusted websites like iTunes App Store, BlackBerry App World, Android Market and Windows Phone Marketplace. You also need to be reactive to antivirus programs that have infected your smartphone. Once a virus is suspected or know to be on a smartphone it needs to be removed as soon as possible. Antivirus programs like Symantec's Mobile Security and Management can be used to remove a virus on a smartphone. Another option would be to wipe the smartphone and restore it to the factory settings. Before this is done you need to ensure you have a known good and recent backup or you will have to reinstall all the applications and data that were previously on the smartphone. The operating system creators also have reactive methods of removing malicious software. As a result of the DreamDroid virus Google remotely removed the malicious malware from Android phones and Google send a forced update called Android Market Security Tool March 2011. Android Market Security Tool March 2011 addresses the vulnerabilities exposed by Dreamdroid. There was also a hack exposed for iPhone and it only required the hacker to know the telephone number of the iPhone. The hack addresses memory corruption in the way the iPhone handles SMS messages. For the attack to work, an attacker must send hundreds of SMS control messages (different from regular SMS messages) and only the initial SMS will be seen.[34] Blackberry smartphones have been infected with a Trojan named Zeus Trojan. This virus allows the initiator of the virus to observe information that the Blackberry user has related to mobile banking. The virus can view, delete and forward text messages, block calls, change the administrator on the device and block phone numbers. It allows the hacker to change the telephone number the device sends all the data to in the event that it gets shut down," he said.[35] Windows smartphones have been infected with the game 3D Anti-Terrorist and PDA Poker Art. This game allows the Windows smartphones to dial numbers in Somalia and Italy which rack up huge bills for the smartphone owner. Hackers are actively at work to infect these for mobile operating systems

Chapter 9: Firmware and Software Updates

Firmware and software updates are critical to ensuring that your smartphone is safe. Firmware and software updates are an essential part in proactively ensuring the safety of your smartphone. Some even believe it is the first line of defense in keeping your smartphone safe. The first line of defense, says Nocera, is making sure that all your software is up-to-date. "Almost every release of software patches a number of security vulnerabilities that are out there," he says. [29] Android, BlackBerry, iOS and Windows Phone smartphone operating systems all have settings to automatically update the operating systems. However, the smartphone owner must check the box to automatically update the operating system. These setting are located on the computer that is used to sync your smartphone and can be accessed by the particular operating system program that is installed on the computer. For individuals without a computer a manual check for updates can be done wirelessly via the smartphone if the smartphone has a data plan or Wi-Fi. Since updates can be completed manually it is a good idea for smartphone users to know how often to check for updates. Before every trip, or at least every few weeks, it's a good idea to check the manufacturer's

Web site (or search Google) to see if a software or firmware update is available. [29] Regardless of how you complete your updates they should be completed unless there is a huge outcry from a number of individuals who have previously applied the update.

Chapter 10: Smartphone Voice Encryption

In addition to encrypting data users may want to be able to encrypt the calls that they make on a smartphone. The average person may not need to encrypt their calls but there is a need for certain smartphone users. However, there are companies and organizations that like to have their voice calls encrypted to ensure these communications are not overheard. Cellcrypt is a company that provides voice encryption software to the following organizations, Department of Defense, Homeland Security, Intelligence Community, Law Enforcement, Administrative, and Procurement/Policy. There are free and commercial products that encrypt calls and these applications vary based on the smartphone operating system. The operating systems that will be discussed include Android, BlackBerry, iOS and Windows.

It has been known that the Military and other government agencies have wiretapping capabilities. However, Chris Paget has shown that GSM networks are vulnerable to having calls intercepted and the cost to intercept these calls is relatively small. GSM makes up a large percentage of the mobile networks around the world. Chris was able to intercept and decrypt several calls with equipment that cost about $1500. This was done by creating a fake GSM base station, turning on an interceptor and jamming the 3G signal, which forces a 3G handset to drop down to 2G which is vulnerable. The calls that were intercepted were with the range of one GSM cell site. If the handsets were equipped with voice call encryption then the calls that were intercepted by Chris Paget would not have been able to be heard in plain voice.

10.1 Android Voice Encryption

Android smartphone do not come equipped with smartphone voice encryption software. However, there is a free commercial product that is available to Android smartphone users. The application that encrypts calls for Android smartphones is RedPhone. Android users can download this application from the Android Market. Both the sender and receiver of the call must have RedPhone for the encryption to work on both ends. RedPhone uses ZRTP which is a cryptographic protocol used over Voice over Internet Protocol (VoIP).   This is a nice benefit because RedPhone users are do not use any of their minutes because VoIP works over the internet via 3G, 4G or Wi-Fi. One disadvantage of RedPhone is it does not support international calling.

10.2 BlackBerry Voice Encryption

BlackBerry smartphones lack voice encryption software when they are purchased. There does not appear to be a free voice encryption software application for the BlackBerry smartphone. There is a commercial option available for BlackBerry user and that option is Cellcrypt. With Cellcrypt the BlackBerry smartphone users can encrypt their call with Federal Information Processing Standards (FIPS) 140-2 over VoIP therefore it has the benefit of call without the use of cellular plan minutes. However, Cellcrypt has two other benefits that include use in over 200 countries and it can be remotely disabled. The major disadvantage is the cost which is $3,732 per year. Figure 13 shows diagram shows how Cellcrypt works.

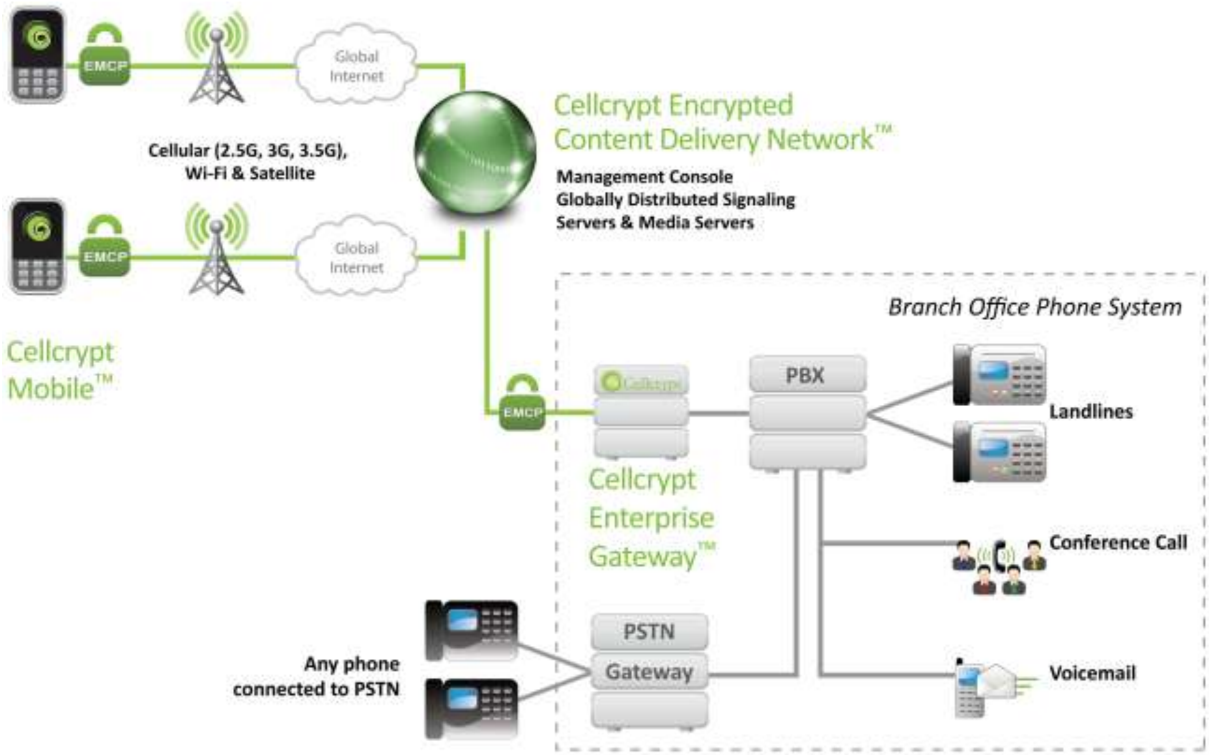

EMCP
Global Internet
Cellular (2.5G, 3G, 3.5G), Wi-Fi & Satellite
EMCP
Global Internet
Cellcrypt Mobile™
Cellcrypt Encrypted Content Delivery Network™
Management Console
Globally Distributed Signaling Servers & Media Servers
Branch Office Phone System
EMCP
Cellcrypt
PBX
Landlines
Cellcrypt Enterprise Gateway™
Conference Call
Any phone connected to PSTN
PSTN Gateway
Voicemail

Figure 13: Cellcrypt Diagram

10.3 iPhone Voice Encryption

iPhones do not come with an installed application to encrypt voice calls. There is a commercial option available to iPhone users and that option is Kryptos. The Kryptos application can be downloaded from the iTunes App Store for free. The application is free but to use the application there is a fee of $4.99 a month. Kryptos uses military grade 256 bit AES encryption to encrypt calls via VoIP. The benefits are the use of VoIP so the user does not have to use any cellular plan minutes and AES which is the current standard adopted by the United States government. The disadvantages is it cannot be exported or re-exported to the following countries Cuba, Iran, Sudan, North Korea, Syria, or any country is under U.S. economic and the cost of $4.99 a month.

10.4 Windows Voice Encryption

Windows smartphones lack voice encryption software when they are purchased. There does not appear to be a free voice encryption software application for the Windows smartphone. There is a commercial option available for BlackBerry user and that option is Cellcrypt. With Cellcrypt the Windows smartphone users can encrypt their call with Federal Information Processing Standards (FIPS) 140-2 over VoIP therefore it has the benefit of call without the use of cellular plan minutes. However, Cellcrypt has two other benefits that include use in over 200 countries and it can be remotely disabled. The major disadvantage is the cost which is $3,732 per year.

Chapter 11: Conclusion

Smartphones are becoming very popular, have computer type functions and smartphone users are storing more important data on these device. Users of Android, Blackberry, iOS and Windows smartphones as well as the manufacturers of these smartphones, operating system developers and the network providers like AT&T, Sprint, T-Mobile, Verizon and US Cellular all play a significant part in protecting the data on these devices. Since the data on the device belong to the user of these smartphone they need to be aware of proactive and reactive methods of protecting the data on these devices from being captured from individuals trying to procure the data from these devices. the methods of proactive and reactive protection of data on smartphone that were discussed in this paper include Smartphone Wiping, Smartphone Password Protection and Encryption, Smartphone Data Backup, Smartphone Locating/Tracking, Smartphone Anti-Virus Protection, Smartphone Software and Firmware Updates and Smartphone Voice Encryption. The methods and applications may vary based on the operating system however, the principles of these protection methods are the same. If the data on your smartphone is valuable to you or someone else, utilize the methods described in this paper to protect your smartphone.

Chapter 12: References

[1] Opam, K. (2010, March 30). GSM vs. CDMA: Or, How Dueling Mobile Standards May Get You a New iPhone. Retrieved from http://www.geekosystem.com/gsm-cdma-new-iphone-difference-info-faq-history/

[2] Eaton, N. (2010, March 10). Windows Mobile market share drops like a rock. Retrieved from http://blog.seattlepi.com/microsoft/archives/197338.asp

[3] Safford, M (2010, February 01). Hackers Crack Cell Phone Encryption. Retrieved from http://www.technewsdaily.com/hackers-crack-cell-phone-encryption-0143/

[4] Radia, R. (2011, January 16). Why you should always encrypt your smartphone. Retrieved from http://arstechnica.com/gadgets/guides/2011/01/why-you-should-always-encrypt-your-smartphone.ars

[5] Kaspersky (2008). Kaspersky Mobile Security. Retrieved from http://www.kaspersky.com/downloads/pdf/leaflet_kms_70_en.pdf

[6] Rubino, D. (2010, July 02). Looking at encryption in Windows Phone 7. Retrieved from http://www.wpcentral.com/looking-encryption-windows-phone-7

[7] UNC-Chapel Hill (2011 January 14). Encrypting Cell Phones. Retrieved from http://help.unc.edu/CCM3_024914

[8] BlackBerry (2011, January 20). Wireless Data Security. Retrieved from http://us.BlackBerry.com/ataglance/security/features.jsp

[9] Madger, J. (2010, December 30). How hackers cracked into GSM phones. Retrieved from http://communities.canada.com/montrealgazette/blogs/tech/archive/2010/12/30/how-hackers-cracked-into-gsm-phones.aspx

[10] Pinola, M. (2011). Install or Enable Remote Wipe on Your Smartphone Now. Retrieved from http://mobileoffice.about.com/od/mobilesecurity/qt/smartphone-remote-wipe.htm

[11] Stanislav, J. (2011, January 20). 5 tips for keeping your smartphone secure. Retrieved from http://www.greystonetech.com/2011/01/20/5-tips-for-keeping-your-smartphone-secure/

[12] Herrman, J. (2009, November 22). How To: Back Up Any Smartphone. Retrieved from http://gizmodo.com/5410369/how-to-back-up-any-smartphone

[13] GPS for Today (2008). Free GPS Cell Phone Tracking.
Retrieved from http://www.gpsfortoday.com/free-gps-cell-phone-tracking/

[14] Komando, K. (2011, January 21). It's quite easy to protect private data on your smartphone. Retrieved from
http://www.pittsburghlive.com/x/pittsburghtrib/business/s_719127.html

[15] Apple (2011). iPhone in Business.
Retrieved from http://www.apple.com/iphone/business/integration/#security

[16] Frakes, D. (2009, July 15) Inside IPhone 3.0's Remote Wipe Feature
Retrieved from http://pcworld.about.com/od/phones/Inside-IPhone-3-0-s-Remote-Wip.htm

[17] Reckner, M. (2008 February) Installing Mobile Defense as a System Application.
Retrieved from https://support.mobiledefense.com/entries/435668-installing-mobile-defense-as-a-system-application

[18] BlackBerry (2011) Remote Wipe Reset to Factory Defaults IT policy rule.
Retrieved from
http://docs.BlackBerry.com/en/admin/deliverables/4222/Remote_Wipe_Reset_to_Factory_Defaults_250402_11.jsp

[19] Bradley, T. (2010 June 24) Protect the Data on Your iPhone 4. Retrieved from
http://www.pcworld.com/businesscenter/article/199790/protect_the_data_on_your_iphone_4.html

[20] Android Central (2011) Password protect your phone. Retrieved from

http://www.androidcentral.com/password-protect-your-phone

[21] The Tech Journal (2011 February 19) Here’s How Easily a Hacker Can Crack Your Weak Passwords. Retrieved from http://thetechjournal.com/electronics/computer/security-computer-electronics/heres-how-easily-a-hacker-can-crack-your-weak-passwords.xhtml#ixzz1ES3GOZzQ

[22] Microsoft (2011) Screen Lock FAQ Retrieved from http://www.microsoft.com/windowsphone/en-GB/howto/wp7/basics/lock-screens-faq.aspx

[23] Apple (2011) iPhone and iPod touch: About backups. Retrieved from http://support.apple.com/kb/ht1766

[24] Smrtguard (2011) Smrtguard Knowledge Base Articles For Android. Retrieved from http://www.smrtguard.com/support_kb/support_droid_kb_5.jsp

[25] Partlow, J. (2009 February 16) Microsoft My Phone. Retrieved from http://windowsteamblog.com/windows_phone/b/windowsphone/archive/2009/07/13/microsoft-my-phone.aspx

[26] Goldstein, L. (2011) Five Tips for Securing Your Smartphone. Retrieved from http://ezinearticles.com/?5-Tips-For-Securing-Your-Smartphone&id=5901457

[27] Rankin, B. (2010 April 21) Does My Smartphone Need Antivirus Software? Retrieved from http://askbobrankin.com/antivirus_for_smartphones.html

[28] Dugdale, A. (2010 August 10) Android Gets Its First Ever Virus--You're a Mandroid, My Son (Updated) Retrieved from

http://www.fastcompany.com/1680011/android-gets-its-first-ever-virus-youre-a-mandroid-my-son

[29] Kugler, L. (2011 March 2) 9 Ways to Keep Your Mobile Device Secure While Traveling. Retrieved from http://www.pcworld.com/printable/article/id,218671/printable.html

[30] InstaMapper FAQ (2011 April 1) InstaMapper FAQ. Retrieved from http://www.instamapper.com/faq_li.html

[31]Verizon Wireless (2007) CDMA Network Security Verizon Wireless White Paper. Retrieved from http://b2b.vzw.com/assets/files/SecurityWP.pdf

[32] Singaram, J. (2011) A Brief History of CDMA (2011) Retrieved from http://rcarora.nuvvo.com/lesson/11803-a-brief-history-of-cdma

[33] Cellular Online (2011) The History of GSM: 1982 to 2001 Retrieved from http://www.cellular.co.za/gsmhistory.htm (The History Of GSM: 1982 to 2001)

[34] iPhone SMS Virus (2009 July 30) iPhone SMS Virus. Retrieved from http://www.quickpwn.com/2009/07/iphone-virus.html

[35] Web Digest (2011 April 07) Blackberry smartphones under Trojan virus. Retrieved from http://iwabs.com/content/blackberry-smartphones-under-trojan-virus