Smartphone Cybercrime & Security – How to use your mobile powerhouse the *SMART* way

Part 1: Android 2.2 (Codename: Froyo) Security

By: Shadi Dibbini
Every day we hear something new about technology, whether it is the next generation televisions, the newest Apple “i” product, latest handheld device and etc... We are constantly surrounded by advanced technologies. Not only do these technologies make our lives a little bit easier…err I mean A LOT easier, they also allows us to become more efficient at the things we do best.

Smartphone’s have become increasingly popular and more affordable over the past few years since the mainstream availability of Android, Blackberry and the iPhone. The majority of the mobile devices that are purchased worldwide are a type of Smartphone. 200,000 Android devices are sold daily and millions of iPhones sold just at launch. According to Gartner’s May 2010 statistics of the Worldwide Smartphone Sales to End Users by Operating System in 1Q10*, the top mobile device operating systems are Smartphone platforms.

*Worldwide Smartphone Sales to End Users by Operating System in 1Q10 (Thousands of Units)

<table>
<thead>
<tr>
<th>Company</th>
<th>1Q2010 Units (In thousands)</th>
<th>Market Share (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symbian</td>
<td>24,069.8</td>
<td>44.3</td>
</tr>
<tr>
<td>Research In Motion</td>
<td>10,552.6</td>
<td>19.4</td>
</tr>
<tr>
<td>iPhone OS</td>
<td>8,359.7</td>
<td>15.4</td>
</tr>
<tr>
<td>Android</td>
<td>5,214.7</td>
<td>9.6</td>
</tr>
<tr>
<td>Microsoft Windows Mobile</td>
<td>3,706.0</td>
<td>6.8</td>
</tr>
<tr>
<td>Linux</td>
<td>1,993.9</td>
<td>3.7</td>
</tr>
<tr>
<td>Other OSs</td>
<td>404.8</td>
<td>0.7</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>54,301.4</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Source: Gartner (May 2010)

What people often don’t understand about these Smartphone’s is that they are in fact miniature computers. They run a variant of computer operating systems such as Linux (Android), Mac (iPhone), and Windows (Windows Mobile), and can do pretty much anything that a computer can do. Smartphones also pack powerful processors, a hefty amount of RAM and a lot of storage space—in some cases up to 48 Gigs! So, a Smartphone is a handheld computer, therefore you should treat it the same way as your computer at home. Smartphones are very susceptible to being hacked and catching viruses, in some ways even easier than a computer.

The Smartphone industry is exploding and hackers and cyber criminals from all over the world are using this to their advantage. For example, in January 2010, a mobile application developer that goes by the name of “Droid09” uploaded a malicious application to the Android App Store that posed as the “Official First Tech Credit Union” banking application. This application was nothing more than a way to steal personal information like banking logins and passwords. Eventually, the application was removed but not before a few customers felt the effect of this rogue application.

“It’s all about the Apps!” Most people purchase their mobile devices solely based on the number of “cool” applications that it can run. The more apps the better right? Wrong. Cyber criminals love this idea of an “Application Market”, “Store”, or whatever you want to call it, because now they can transmit malware easily throughout the world without having to put forth any effort at all. You download an infected app and BAM! Your phone is infected. So, how can you protect yourself from becoming a victim of mobile malware or data theft? Well, it’s a bit complicated right now, but with the right knowledge and security awareness, you can minimize your risks significantly. This page will show you how to protect yourself and your data when using your Android, iPhone, or BlackBerry.

Let us begin securing your device!
The first mobile operating system that we are going to cover is Android. Even though Android is one of the most secure Smartphone operating systems available today, it is inevitable that security bugs will be found in any complex operating system. Another prevalent issue among the Android community is, in fact, the Android Market. This central repository for Android applications is home to a lot of legitimate and not so legitimate applications. Did I mention that browsing the internet carelessly can affect your phone as well? So, how can you protect yourself you might ask? Easily! Just follow my simple guideline and you can lessen your chances of getting malware and having your identity and private/personal information stolen.

**Note:** The Android security documentation provided below covers the 2.2 (Froyo) OS. Some of steps in this guide may be similar or different than the previous 2.1 (Éclair) OS.

### Basic Android Security Configurations

So you have gotten yourself a new Android phone with the latest and greatest OS from Google (2.2 Froyo) and you have no idea how to use it yet; but you are a smart individual who is concerned with security and privacy of your personal/private data... Right? Well no fear, with a few minor adjustments and some security tips from yours truly; you will be on the right path to successfully securing your new device. Let us begin
This picture shows your home screen. Yes I know its basic, but in due time you will have this whole page, and the other 4 pages covered in cool apps and widgets. In the mean time, we are here to secure your device!

**Step 1:** You want to make sure no one can get into your device if someone is not authorized to use it right? Well the first thing that we want to do is create a lock code for your phone. To set up your lock code, **click on the menu button; click settings, then location and security.** This is where we will set up some basic Android security configurations.

**Step 2:** At this menu, click on **Set up screen lock**
Step 3: At this screen, you can choose any of the three types of screen lock security that your heart desires. Just follow the directions for whichever type of screen lock you choose and you will be one step closer to securing your device.

Note: Make sure you use a strong but easily remembered pattern, pin or password to securely lock your device. If you happen to forget your pattern, pin or password and your device locks, it will then ask you for your Gmail account and password to bypass the screen lock.

Step 4: After you have set up your screen lock, you are going to have to set up your SIM card lock if applicable. SIM cards are used with AT&T, Cincinnati Bell and T-Mobile. Sprint and Verizon do not use SIM cards. If you are unsure as to whether or not your phone uses a SIM card, please contact your service provider.

NOTE: Your SIM card holds a lot of valuable information and it should not be accessed by anyone other than you. In the event that your phone does get lost or stolen, the SIM card lock will only work when a device is powered up. This security feature is used as a verification to unlock the contents of the SIM card and allows you to have access to your cellular network. To secure your SIM card, click on the Set up SIM card lock and follow the prompts.

Step 5: Prevent unauthorized access to important data on your memory card by setting a strong password. Click Set password under the credential storage category, and follow the prompts.
Step 6: To protect the privacy of your location, uncheck **Use GPS Satellites**.

Look at you! You are growing up so fast! You have now taken the proactive measure of securing your device. I am proud of you. Well... these six easy steps conclude the Basic Android Security Configurations. Congrats! You have tackled the first obstacle in securing your device. Now off to tackle the next obstacle, the gateway into *teh interwebz.

*teh interwebz.... [http://lmgtfy.com/?q=teh+interwebz](http://lmgtfy.com/?q=teh+interwebz)
Browsing “teh Interwebz” Safely

Browsing the internet safely takes more than a bunch of security configurations. It also takes smarts, a good sense of judgment and a very sharp eye to determine a malicious site from a credible site. You also have to rely on yourself to not browse the dirty depths of the internet... it is not a good place for you to explore... I’ve seen a lot of bad things... errr... beside the point; this next section will give you the proper guidance on how to configure your Android browser, while also discussing some quick tips on browsing the internet safely. Let us begin...

Step 1: To stay safe while browsing the internet there a few configurations that needs to be made to the native Android browser. So open the Android browser, click menu, then click more and then finally click settings. This will take you to the configuration menu of the Browser.

Step 2: To prevent those pesky pop-ups during your exploration of the internet, make sure that you have a green checkmark next to Block pop-up windows.
Step 3: The privacy settings category is where we will perform most of the secure browser configurations. It is best practices to clear your cache, history, cookie data, and form data at least once a week.

Step 4: It is never a good idea to have an internet browser remember your form data. Form data holds very sensitive information such as usernames and passwords. Form data can include information such as bank account, email and social website login credentials. If your phone is compromised through theft or malicious applications, form data can be extracted and all of the online accounts that have been saved to your phone can be compromised.
Step 5: Websites like to gather information about you in many different ways. Some websites like to know where most of their viewing demographic is located. This information is used for marketing reasons and various researches. Some say this is an invasion of privacy... and I couldn't agree more. So if you do not want websites to know where you are located, I suggest that you uncheck Enable location and Clear location access.

Step 6: The final steps in creating a secure browsing environment is by unchecking Remember passwords and making sure Show security warnings is checked. As previously stated in step 4, passwords and form data go hand in hand. Storing sensitive information on a device, that can be easily lost or stolen, is not good privacy and security practice. The less private/sensitive data that is saved to any mobile device, the better...

Being able to see security warnings is a very good thing. The security warnings will tell you if you are about to enter a website that is not secure, have invalid security certificates or a malicious site that is possibly posing as a legitimate site.
Human Errors When Browsing the Net

Even though you have tweaked the browsers security and privacy settings to make it a little bit more secure, human ignorance, when browsing the web, can defeat the purpose of even having these security settings. People cannot always rely on security hardware and software to protect them fully from malicious content. With these security mechanisms in place, as well as the right security knowledge, even you can prevent bad things from happening to your personal information. So... here are a few guidelines when browsing the net on your Android device.

**Step 1:** Always browse with `https://`. When going to websites that requires you to login using some sort of credentials, make sure that the site is in fact using `https://`. For those of you who don’t know what this means, http stands for hypertext transport protocol, to simplify it even more it is the language that a browser and server speak to transfer data back and forth to one another. So what is https you might ask? Https, or hypertext transport protocol secure, goes a step further than http. Https encrypts the traffic between your browser and the server hosting the website that you are on. What is encryption and why is this important?

Well... let’s just say I am a hacker for example, and you are browsing the internet at a café using their free WIFI on your Android. I, the computer hacker, take my laptop and I do some “things” to the WIFI network so I can steal everyone’s information. You, a naïve college student that is unaware of what’s about to happen, is about to log into 5/3’s website to check on your bank account. You didn’t check to see if you were using `https://` did you? Of course not! So, you log into your account and everything is fine and dandy on your side. On my end, I am super excited so I pack up and leave; I have completed my task.

**So what just happened?**

You logged into a banking site using http and not `https://`.

**Why should you care that you didn’t use `https://`?**

You should care because since I am a great hacker, I manipulated the network using various hacking tools and was able to monitor your Android device and capture your login information.

**NOTE:** When using `https://` the transmission of data is encrypted. When traffic is scanned by yours truly when you use `https://`, I will see something like this:

A;lyu9f0874kajhvp9i7y6kjjhpsoiduyv98y45kljadhsf9y985 << this will not make any sense to me since it is encrypted

But... when you used http to log into 5/3’s site, this is what the transmitted data will look like to me.

Username: Johndoe   Password: 12345   << by the way.... This is a horrible password. Never use it.
Typically, I never recommend logging into your banks website, or any other important website, on a mobile phone, but you are going to do it anyway right? I hope not! But, the rebellious side of you is going to go to those sites anyway. So, in case you do, just look out for the https:// connection beforehand, otherwise, I would highly recommend that you leave that site!

Think Before You Download…Seriously This Time

Ahh… The Android MarketPlace. It is filled with thousands upon thousands of fun and exciting apps to download. What should I get today? Yelp looks nice… o wait how about a new wallpaper… or even four square! Whatever it is I can’t wait to indulge myself with all of these Apps! There are just so many to choose from!

Yes, even though the Android Market is probably the best thing to happen to Android, it is also the one of the worst (I cannot emphasize the word worst enough) things to happen to Android and to you! That’s right folks; the Android Market is hazardous to your important data and private information. According to a June 22nd post by the mobile security firm Smobile, “about 20 percent of the 48,000 apps in the Android marketplace allow a third-party application access to sensitive or private information”. Smobile also mentions that, “some of the apps were found to have the ability to do things like make calls and send text messages without requiring interaction from the mobile user.”

On July 28th 2010, Lookout mobile security had reported, at the BlackHat Conference, that a malicious application, now classified as non-malicious by Google, had been downloaded by millions of users. According to Lookout, this application developed by Jackeey Wallpaper, offers a variety of wallpapers. “Aside from providing backgrounds”, Lookout states that, “the utility quietly collects personal information such as SIM card numbers, text messages, subscriber identification, and voicemail passwords. The data is then sent to www.imnet.us, a site that hails from Shenzhen, China.” Google pulled the application from the app market place to further investigate. Upon its investigations, Google lifted the suspension it placed on the application and responded back to the app developer, “Our investigation has concluded that there is no obvious malicious code in your apps, though the implementation accesses data that it doesn’t need to.”

In recent news regarding Jackeey’s application, Lookout has corrected this misunderstanding and stated that there was no evidence of malicious behavior produced from his app. Lookout has posted on their blog, “There have been cases in the past where applications are simply a little overzealous in their data gathering practices, but not because of any ill intent.”

So, what can you take away from these recent studies? Well, before you install an application from the Android App Market, be cautious of what access the app may have. DO NOT… let me repeat myself once again… DO NOT just click install! Read what the app has control over. If a wallpaper application has access to your contact information, text messages and other private/sensitive information, steer clear away and do not download. This methodology applies to all Android apps. If you feel that an app has access to a lot of information that it shouldn’t have access to, then do not download it. Trust your gut feeling and download apps the smart and safe way.
In this section, we will be covering some free Android security applications that can help protect your phone. Even though, for the most part, Android’s security model is good, you can never be too cautious to implement additional security features to your device.

Recommendation: High

Overview:

The first application that I want to cover is Lookout Mobile Security (mylookout.com). Lookout is a mobile security company dedicated to making the mobile experience safe for everyone. Today, with users across 400 mobile networks in 170 countries, Lookout is a world leader in Smartphone protection.

Experience:

I have personally used lookout mobile on my Android powered Nexus One for a while now, and it honestly is one of the best mobile security software available today. It is available in the Android Market Place for the nominal price of FREE. Yes I said it... FREE! Lookout provides to you a comprehensive anti-virus/anti-malware security suit for your beloved Android phone. I recommend this software to all Android users because the features of this security suite are absolutely phenomenal.

What are the features you say?

Well, I'll let you decide by reading Lookout’s features page. You can check it out and be the judge by visiting the links provided below.

Security

https://www.mylookout.com/features/security

Backup

https://www.mylookout.com/features/backup

Missing Device

https://www.mylookout.com/features/missingdevice

Management
Recommendation: High

Overview:

The second application I want to cover is TextSecure. TextSecure is a drop-in replacement for the standard text messaging application, allowing you to send and receive text messages as normal. All text messages sent or received with TextSecure are stored in an encrypted database on your phone, and text messages are encrypted during transmission when communicating with someone else also using TextSecure.

Experience:

Like most people, text messaging is a very important way we communicate. It has somewhat become a social norm in communication amongst each other. Regardless of how we communicate, we are still entitled to our privacy. This is where Text Secure comes in handy. Text secure replaces the native Android SMS client, creates its own encrypted database for all SMS/MMS messages to be stored and it allows you to initiate private encrypted chats with other Text Secure users. But don’t be scared... you can still SMS and MMS message non-TextSecure users. I highly recommend using text secure as your default messaging client. In the event that you lose your phone and someone can gain access to it; Text Secure protects all of your text messages in an encrypted password protected container that only YOU have the key to unlock.

Text Secure is now available in the Android Market.

Need more info about Text Secure... Check out the link below for more details

http://www.whispersys.com