enabling **Secure** mobility

Android Market

Threat Analysis of the Android Market

Troy Vennon, GTC Research Engineer
David Stroop, GTC Research EngineerJune 21, 2010

TABLE OF CONTENTS

ANDROID MARKET

In keeping with the Open Handset Alliance goals of Android being the first open, complete, and free platform created specifically for mobile devices, Google offers the Android Market. The Android Market offers the ability for developers to create any application they choose with the community regulating whether the application is appropriate and safe, as opposed to relying on a formal screening process.

The pros and cons of this open approach to an application store have been discussed in great detail. Notwithstanding, Spyware and other malicious applications have made their way onto even controlled application stores and these controls have not negated the need for mobile device security software, such as Anti-Malware applications. The desire for open source applications by mobile device owners on even strictly controlled operating systems is evidenced by the vast amount of iPhone devices that are jailbroken to allow for the running of out-of-market applications which have not been approved by Apple.

The Android Market offers flexibility that markets such as the Apple App Store do not by allowing anyone to develop and publish an application to the Market's consumers. This presents the opportunity to easily defraud innocent consumers for financial gain. Financial gain drives the paradigm of information security and attackers now see consumer and enterprise smartphones as targets. Since today's Smartphone devices are the equivalent of mobile computers, it is logical that attackers have expanded their focus from PC-based malware to Smartphone malware and an open application repository lends itself to these types of attackers.

ANDROID MARKET SECURITY MODEL

The Android Market relies on the community to identify and flag applications that either malfunction or are malicious in nature. This would imply that there will always be a window where a number of consumers would need to use, test and determine if an application is malicious before it could be removed from the Market. This has already occurred in the instance of a bank phishing application that was published by an author by the name of Droid09.

The application created by Droid09 stated it would allow the user to conduct banking activities from the handset. All the user had to do was give the application the user's account information and it would facilitate the communication tunnel to the bank in order to process transactions. In reality, the application only facilitated a web browser connection to the bank's online banking website, just as if the user opened Android's browser and typed the bank's URL into the address bar. What it actually did with the account credentials that the user provided is still unknown.

This bank phishing application is an excellent example of both how the Market lends itself to attackers, as well as how those types of malicious applications are supposed to be dealt with by the community. In this case, it is unclear exactly how long this application was in the Market or how many consumers actually installed it before it was removed from the Market

It is these types of applications that security researchers have been discussing for some time now. It is known that the Android security model requires that applications declare the permissions they will be using prior to installation by the user. An informed user can use these declarations to determine if it is reasonable for a particular application to be able to access certain types of information and then decide whether they want that particular application to be installed.

An example that SMobile often uses is the case of an application that plays various animal sounds when the image of that animal is pressed. It effectively plays pre-defined .wav files that are stored alongside the application. One would logically assume that certain types of permissions would need to be granted to allow the application to call those .wav files and play the appropriate sounds. One would also be able to look at the permissions being requested and wonder why that same application would need access to things such as the GPS location of the device, or contacts, or incoming and outgoing calls or maybe even Internet access.

It is this type of access to sensitive information that SMobile sees the attacker community gearing their attacks toward. Attackers are always trying to find new and inventive ways of harvesting large quantities of personal information. An efficient means to this goal is by distributing a seemingly innocent application that a user installs without giving credence to the types of access they are providing the application. .

It is important to note that electronic criminals, as a rule, will pick the easiest opportunities available when attempting an attack. An attacker would not need to spend months fuzzing a particular handset or platform trying to find undiscovered vulnerabilities when all they would need to do is write a simple application that they are certain most consumers would willingly install on their own, in order to obtain the personal or enterprise data they are interested in obtaining to use for financial gain.

PERMISSION-BASED DETECTION

To date, nearly every attempt at detecting malicious applications on a mobile device has relied upon the same signature-based methods that PC anti-virus vendors have been using for years. In the PC world, anti-virus engines alone cannot handle the 10's of thousands of signatures for malware that they must now detect. The same should be said about mobile anti-virus engines. Signature-based detection alone cannot be relied upon as the only means of identifying malicious applications on mobile devices. Smartphone anti-virus must also look for other means of determining malicious applications for platforms whose application repositories are ripe for attackers.

Android requires application developers to declare the permissions their application will need in order to interact with the system and its data. As a result, SMobile has incorporated patent pending technology to use application permissions and other identifying attributes to determine what an application can do and subsequently, identify Spyware and other malicious applications.. This provides a prime opportunity to identify an application that is trying to access sensitive data or communications and then assist the user in determining if this access is truly necessary for an application.

SMobile has developed a methodology and technology to determine potentially malicious applications based upon the permissions granted the application. In doing so, it is imperative to determine what information or type of access an application is allowed to ask. Table 1 is a listing of the permissions that an application can request to be allowed access to sensitive information or services which could be used maliciously:

Permission Name	Permission Description
ACCESS_COARSE_LOCATION	Allows an application to access coarse (e.g., Cell-ID, WiFi) location
ACCESS_FINE_LOCATION	Allows an application to access fine (e.g., GPS) location
BRICK	Required to be able to disable the device
CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed.
CALL_PRIVILEGED	Allows an application to call any phone number, including emergency numbers, without going through the Dialer user interface for the user to confirm the call being placed.
GET_ACCOUNTS	Allows access to the list of accounts in the Accounts Service
INTERNET	Allows applications to open network sockets.
PROCESS_OUTGOING_CALLS	Allows an application to monitor, modify, or abort outgoing calls.
READ_CALENDAR	Allows an application to read the user's calendar data.
READ_CONTACTS	Allows an application to read the user's contacts data.
READ_OWNER_DATA	Allows an application to read the owner's data.
READ_SMS	Allows an application to read SMS messages.
RECEIVE_MMS	Allows an application to monitor incoming MMS messages, to record or perform processing on them.
RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them.
RECORD_AUDIO	Allows an application to record audio
SEND_SMS	Allows an application to send SMS messages.
USE_CREDENTIALS	Allows an application to request authtokens from the AccountManager
WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage
WRITE_HISTORY_BOOKMARKS	Allows an application to write the user's browsing history and bookmarks.
WRITE_OWNER_DATA	Allows an application to write the owner's data.

Table 1

Singularly, each of these permissions has a viable purpose. When used correctly, each allows the developer to create robust and useful applications. However, attackers can use these same permissions against an unsuspecting user. Let’s take an example from an application SMobile identified as spyware, but has remained in the Android Market for months:

SMS Message Spy Pro and **SMS Message Spy Lite** are similar spyware applications from the same developer. **SMS Message Spy Pro/Lite** were both developed by Carrot App. The Pro version of this spyware application is the full, paid version. The Lite version is currently listed in the Market as free, but it expires in seven days. **SMS Message Spy Lite** can be considered a trial version of the Pro variant.

SMS Message Spy Pro runs on the device under the package name **com.carrotapp.smsspypro** and contains the following description in the Market:

> “A real spy tool! Automatically sending all SMS messages to an email in the background hourly. It pretends to be a Tip Calculator. No one can see the difference.
>
> To use: Go Menu->About, LONG PRESS on the logo, password is spy.
>
> Please try our free version first. Search SMS Spy.
>
> Its illegal to spy on phones you don't own!“

SMS Message Spy Lite runs on the device under the package name **com.carrotapp.smsspyfree** and contains the following description in the Market:

> “Need a real spy tool? Automatically forwarding all SMS messages to an email in the background hourly.It pretends to be a Tip Calculator. No one can see the difference.
>
> To use:Go Menu->About, LONG PRESS on the logo, password is spy.
>
> Please buy the full version if you like it.
>
> Its illegal to spy on phones you don't own“

Both applications request the following permissions upon installation:

- **RECEIVE_BOOT_COMPLETED**
- **INTERNET**
- **DEVICE_POWER**
- **READ_SMS**
- **RECEIVE_SMS**
- **READ_CONTACTS**
- **WAKE_LOCK**

SMS Spy was labeled and is detected by SMobile’s Security Shield as spyware. This application could allow an attacker to monitor the SMS communications of an unsuspecting user. Notice the **READ_SMS,** and **RECEIVE_SMS** permissions. A mobile device user with SMobile’s Security Shield installed would be alerted to the fact that the SMS Spy application was installed on their device because the permission signature and other attributes would be detected.

It is possible for a legitimate application to have permissions that could be identified as those used for malicious purposes. As a result, SMobile has created categorization to communicate to the device user the state of their installed applications. These are categorized as the following:

- **Spyware –** An application that possesses a particular set of permissions and attributes that have been identified in previously known Spyware applications.

- **Suspicious –** An application that possesses a combination of 2 or more notable permissions that grants access to personal identifying information or services that could be used maliciously

- **Notable –** A permission that grants access to personal identifying information, location or service that could be used maliciously.

Based upon this information, the users can make an educated and guided decision regarding the applications installed on their device.

MARKET ANALYSIS AND METHODOLOGY

SMobile has published two previous whitepapers on the Android Market that have documented specific types of malicious applications and threats. Those whitepapers can be found here and here. In this whitepaper, SMobile has taken a more inclusive look into the Android Market for applications that, based upon the aforementioned criteria, could be considered malicious or suspicious.

To perform this task, SMobile needed to conduct an automated analysis to analyze thousands of applications. Since it is possible to identify whether an application may be malicious by the permissions it requests, a large scale analysis of the Android Market was conducted to gain further insight into its applications.

In order to perform large scale analysis of the Market, one would need to be able to interface with the Market to get application permission data. As of now, there is no downloadable repository of the Android Market that can be interfaced from a PC to directly download applications for analysis. A few websites, such as Androlib.com and Appbrain.com, have done a good job of keeping up to date with descriptions of apps that are being added to the Market. Androlib even provides a statistical analysis of how and when the Android Market is growing. Prior to this whitepaper, no other research has taken the step to analyze the Market for malicious content on a large scale.

On Android devices, the Market application is the method by which a user is able to browse or search for applications. It also facilitates the download and installation of the application to the handset. The Market application is one of the few portions of the Android operating system that is considered to be closed source to Google, which explains Google's implementation of its protocol buffers into the communication stream to obfuscate portions of the exchange between the vending.apk (Market application package) and the Android Market ecosystem.

While Google has attempted to obfuscate portions of the communications stream between an Android device and the Android Market, there are still certain portions of the connection that can be sniffed when connecting to the Market from a device emulator that comes as the standard toolkit in the Android SDK (Software Developers Kit). However, the standard device emulator that comes in the Android SDK does not include the Market application; it's considered closed source. As a result, The Android community has created emulator ROMs that have the Market application included. This grants the ability to sniff the network traffic between the emulator and the Market to analyze the communication.

With the Market client recreated in the form of a PC desktop application, it is possible to browse the Android Market servers by querying for various strings. When performing these string queries on the Market servers, the response yields the application name, the application asset ID, the developer's name, the application price, application category and the permissions that the application will request. The permission information is the important part for this whitepaper's analysis.

MARKET STATISTICS

With application metadata being collected from the Android Market, SMobile began to query the application metadata and determined that there are some concerning statistics in play.

To date, metadata collection has netted information from 48,694 applications in the Android market, roughly 68% of all applications that are available for download. It is noted that one in every five applications request permissions to access private or sensitive information that an attacker could use for malicious purposes. One out of every twenty applications has the ability to place a call to any number without interaction or authority from the user.

More frighteningly, 29 applications were found to request the exact same permissions as applications that are known to be spyware and have been categorized and detected as such by SMobile's solution. A full eight applications explicitly request a specific permission that would allow the device to brick itself, or render it absolutely unusable. 383 applications were found to have the ability to read or use the authentication credentials from another service or application. Finally, 3% of all of the Market submissions that have been analyzed could allow an application to send unknown premium SMS messages without the user's interaction or authorization.

Permission Name	# of Apps Requesting the Permission
ACCESS_COARSE_LOCATION	12,062
ACCESS_FINE_LOCATION	7,533
BRICK	9
CALL_PHONE	2,670
CALL_PRIVILEGED	103
GET_ACCOUNTS	312
INTERNET	34,636
PROCESS_OUTGOING_CALLS	274
READ_CALENDAR	500
READ_CONTACTS	4,203
READ_OWNER_DATA	200
READ_SMS	849
RECEIVE_MMS	107
RECEIVE_SMS	1,172
RECORD_AUDIO	876

SEND_SMS	1,356
USE_CREDENTIALS	71
WRITE_EXTERNAL_STORAGE	7,846
WRITE_HISTORY_BOOKMARKS	138
WRITE_OWNER_DATA	211

Table 2

Further analysis indicates that of the 68% of the Market applications that have been queried, 20,786 of those applications would be considered to be suspicious because they request two or more of the permissions that would grant access to personal information or services that could be used incorrectly. Below is a breakdown of how those permission representations escalate:

- 5,783 applications in the Market request 3 or more notable permissions
- 2,708 request 4 or more notable permissions
- 826 request 5 or more notable permissions
- 435 request 6 or more notable permissions
- 147 request 7 or more notable permissions
- 97 request 8 or more notable permissions
- 27 request 9 or more notable permissions
- 39 applications request 10 notable permissions
- 10 applications request 11 notable permissions

SUMMARY

Security researchers have been debating the risk that application repositories pose to consumers and enterprises for several years now. At this point, it is no longer just a theory that attackers could use these repositories as a means to distribute malicious applications that are built specifically to defraud a user of their personal information, facilitate spying, or steal money and trade secrets- All of these things are happening today.

Threat analysis of the Android Market indicates that there are thousands of applications that exist in the Market that grant access to personal information, location data, or access to services that could be misused for nefarious purposes. Users are downloading and installing these apps daily. Without question, a majority of these applications were developed with the best of intentions and the user data will likely not be compromised. However, the fact remains that there is no means available for a user to know for sure that the app they just downloaded is doing only what the user sees it doing. One must look at the permissions it has requested to determine what the application's true capabilities might be.

SMobile's new behavior-based detection methodology leverages heuristic-style technology to determine if an application could be malicious, then gives the user the ability to use this information to determine if an otherwise innocent application is requesting permission to do things that just doesn't make sense for the application. From there, the user would then determine if the application should remain on the phone or if it is safer to remove it from their device.

Security researchers know that users are often tricked into the traps that cause information to be compromised. Permission-based detection of malicious Android applications provides a unique and patent pending method to outpace and compliment signature-based anti-virus technology in speed, reliability and functionality.