JUNIPER NETWORKS

MALICIOUS MOBILE THREATS REPORT 2010/2011

An Objective Briefing on the Current Mobile Threat Landscape Based on Juniper Networks Global Threat Center Research

Table of Contents

Table of Figures

Executive Summary

Mobile malware attacks and other exploits are no longer just theoretical occurrences discussed by security researchers and vendors keen on cashing in on a projected market. The threats to mobile devices are real—and reach far beyond simple viruses to include malware, loss and theft, data communication interception, exploitation and misconduct, and direct attacks.

Already, mobile malware and exploitation techniques have reached the complexity and capabilities of their counterparts in wired networks. Malware developers are capable of researching, uncovering, and leveraging weaknesses in mobile platform security models, as well as inherent weaknesses in app stores and open ecosystems. A lack of oversight, coupled with an exploding number of new consumers who lack security awareness or are disinterested in the mundane aspects of mobile security with access to a plethora of new apps for their mobile devices, is creating a recipe ripe for a catastrophic malware disaster. As mobile device usage increases, the absence of installed mobile security products is playing an enabling role in the vulnerability of mobile devices and the exploitation of sensitive data and personal identifying information (PII).

This report, published by the Juniper Networks Global Threat Center (GTC), details specific attack vectors on mobile devices over the past year, defines new and emerging mobile threats expected in 2011, and gives mobile users practical advice to protect themselves from malicious attacks.

Introduction

From large enterprises and government agencies to small businesses and consumers, the use of smartphones and other mobile devices to manage professional and personal interactions is now ubiquitous. Mobile devices have become the new personal computer, storing as much data as a PC but providing greater flexibility and portability. Online banking, commerce, and other business applications put daily business and financial transactions at users' fingertips. And, at every turn, users are implored to download productivity and entertainment applications to further increase the value of their mobile devices.

While smartphones and tablet devices now perform the same functions as a PC, one critical feature is missing—security. Whereas most PCs come equipped with antivirus and other endpoint security software, the vast majority of mobile devices are devoid of any security protection, leaving both the data and applications on these mobile devices at risk of exploitation or misuse.

Smartphones and other mobile devices serve the same functions as laptop computers—with comparable computing power—but with little or no endpoint security.

The increasing number of mobile-related exploits, and the growing impact of these security breaches combined with the continuing exponential growth in mobile devices sold and in use, have put the mobile industry at a critical juncture: mobile security *must* be addressed in 2011 in order to ensure the privacy and safety of users' critical personal and business information and data.

This report delivers a comprehensive, objective briefing on the current mobile threat landscape, based on data gathered through research conducted by the GTC and data from Juniper Networks® Junos® Pulse Mobile Security Suite customers. It provides specific, in-depth information regarding the threat and exploitation vectors relating to mobile devices, including:

- **Malware**—Spyware, viruses, trojans, and worms
- **Loss and Theft**—Data lost due to misplaced or stolen mobile devices
- **Data Communication Interception**—Eavesdropping on communications, including emails, texts, voice calls, etc., originating from or being sent to a mobile device
- **Exploitation and Misconduct**—The inappropriate use of a mobile device for personal amusement or monetary gain
- **Direct Attacks**—Short message service (SMS) and browser exploits

Following the detailed description of the specific threat vectors listed above, this report outlines steps that mobile users can take to protect themselves and defend their—and their corporations'—mobile data from malicious attack, loss, or theft.

Malware

In the mobile security space, a relationship seems to exist between market share and mobile malware. Until recently, the Nokia Symbian operating system led the worldwide mobile OS market and, as such, Symbian malware dominated the samples that the Juniper Networks Global Threat Center discovered and analyzed on a daily basis. Malware affecting Symbian devices make up 77% of the virus definitions found in the Junos Pulse Mobile Security Suite's database.[1]

Together, the Symbian and Microsoft Windows Mobile platforms are the oldest and most researched mobile platforms, and devices running those mobile operating systems have been the targets of the most prolific and effective malware known to affect mobile devices. These platforms have been targeted by a range of malicious applications that run the full spectrum of known malware categories, including SMS trojans that send SMS messages to premium rate numbers unbeknownst to users, background calling applications that charge the victim for exorbitant long distance calls, keylogging applications, and self-propagating code that infects devices and spreads to additional devices listed in the address book. The Juniper Networks Global Threat Center also sees polymorphic malware, which changes its characteristics during propagation to avoid detection, on the Symbian and Microsoft Windows Mobile platforms.

Key Findings

- 400% increase in Android malware since summer 2010.
- One in 20 mobile devices was lost or stolen, requiring locate, lock, or wipe commands.
- 20% of all teens admit sending inappropriate or explicit pictures or videos of themselves from a mobile device.

Source: Juniper Networks; Cyberbulling Research Center

Although newer to the mobile market, the RIM BlackBerry, Google Android, and Apple iOS operating systems are not immune to malware. These mobile operating systems suffer predominantly from spyware applications designed to monitor device communications, often with the capability to control the spyware remotely. Some commercial spyware applications, such as FlexiSpy[2], Mobile Spy[3], and MobiStealth[4], are very effective at concealing both their presence and actions from the user. These applications can enable an attacker to monitor every SMS and Multimedia Messaging Service (MMS) message, email, and phone call initiated and received by the device, as well as the device's physical location. They can even allow an attacker to remotely listen to voice conversations.

Key Mobile Malware Findings

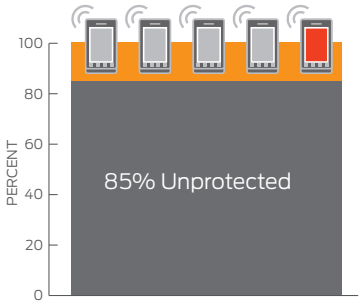
- Mobile device and OS marketshare and mobile malware infection rates are linked
- Mobile malware uses the same techniques as PC malware to infect mobile devices.
- The greatest mobile malware risk comes from rapid proliferation of applications from app stores.
- RIM BlackBerry, Google Android, and Apple iOS operating systems suffer predominantly from spyware applications

While commercial spyware applications are nothing new to mobile security experts, the greatest malware risk to all mobile operating systems moving forward involves the rapid development, distribution, and proliferation of applications through so-called "app stores." Created as a means to distribute applications to mobile device users, app stores provide an ideal transport mechanism for the delivery of malicious software to high volumes of mobile devices.

App stores may be chartered and managed by mobile operating system developers such as the Apple App Store, Android Market, Windows Marketplace for Mobile, BlackBerry App World, or Nokia's Ovi Store; by known third-party entities such as Amazon.com and its Amazon App Store for Android; or by unknown third-party companies. Downloading applications from an unknown, unaffiliated third-party app store is known as "sideloading," and at times has been known to be a catalyst for the launch of renegade applications infected by malware.

Much debate has taken place in the industry regarding app store security and, specifically, how applications—many times created by entry-level developers with visions of huge profits—should be examined, policed, and monitored. Ultimately, endpoint security software is the best prevention against mobile malware.

A 2010 SANS[5] Institute report showed that 85 percent of smartphone users were not employing an antivirus solution on their mobile device to scan for malware.[6] Of the 15 percent of the survey respondents who were using an antivirus product on their smartphone, one in five of those users reported having been infected with a malicious application. According to SANS, that number is higher than the overall infection rate for PCs in North America, which remains between seven and ten percent.



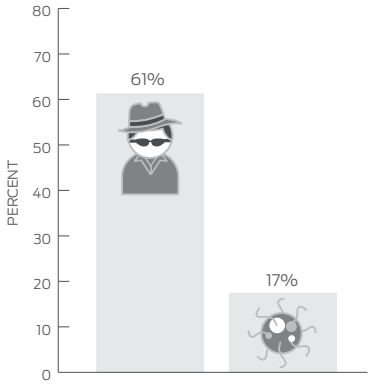
SANS.org noted that 80% of member smartphones do not employ antivirus protection.

Of the 15% of smartphone users that did employ antivirus protection, 1 in 5 had reported being infected by mobile malware.

Data compiled in 2010 by the GTC from actual Juniper Networks customers noted an average 2.2 percent infection rate across all mobile platforms.[7] Results from a specific Fortune 15 enterprise customer that deployed the Junos Pulse Mobile Security Suite to over 25,000 global mobile devices noted that the Junos Pulse Mobile Security Suite software uncovered a five percent infection rate.

Spyware capable of monitoring any and all forms of communication to and from a mobile device accounted for 61 percent of all reported Juniper Networks mobile customer infections. More tellingly, spyware accounted for 100% of all infections for Android devices as reported by Juniper Networks customers. Specifically designed to reside silently and invisibly on devices, and be undetectable by traditional means, spyware can only be detected by professional mobile anti-malware products.

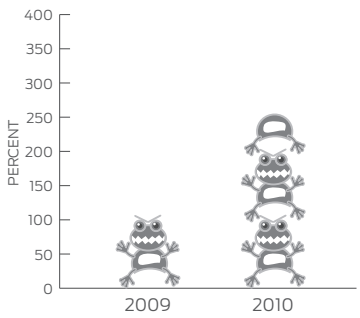
According to the GTC, 17 percent of all reported infections were due to SMS trojans that sent SMS messages to premium rate numbers, often at irretrievable cost to the user or enterprise.



61% of Juniper Networks-detected malware infections are from spyware

17% of Juniper Networks-detected mobile malware infections are from SMS trojans

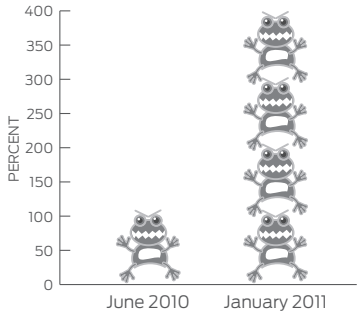
One-third of all signatures in Juniper Networks' malware definition database were added in a single year, 2010. This translates to one signature in 2010 for every two signatures written from 2002 to 2009, an increase of 250 percent from 2009 to 2010.[8]



Mobile malware **grew 250%** from 2009 to 2010

Google Android

The Google Android mobile operating system, as the dominant growing force in the mobile device market, was the biggest target of malware and exploit developers in 2010. Capable of researching, uncovering, and leveraging weaknesses in both Android's security model and the open ecosystem fostered by the Android Market, malicious individuals took advantage of a market with little oversight and a large and exponentially growing number of new users who were largely uneducated, unaware, or disinterested in mobile security, and being introduced to a plethora of applications for the very first time. It was, in effect, a perfect storm—and it continues to brew in 2011.



Google Android malware samples **grew 400%** from June 2010 to January 2011

January 2010: Phishing for Dollars

In early January 2010, the first bank phishing application appeared in the Android Market, the official Android app store, when a developer by the name of "Droid09" published an application that purported to be a banking client to access online financial accounts and asked the user for his login credentials, only to ship the credentials to an unknown location.[9]

March 2010: The First Android "Botnet"

In March 2010, another highly publicized Android attack took place. Mobile service provider Vodafone was unknowingly shipping devices from its mobile handset manufacturer with Secure Digital (SD) cards preloaded with the Mariposa botnet that affected Windows systems.[10] When a user unpacked the new device and connected it via USB cable to a Windows-based PC to transfer files or synchronize the device, the SD card's "autorun" function would initiate and infect the user's computer with the botnet.

Android Attacks: 2010

- January 2010: First bank phishing application for Android
- March 2010: First Android "botnet"
- July 2010: GPS monitoring embedded in Tap Snake game
- August 2010: First Android SMS trojan

2010 Juniper Networks Study of Malicious Applications Available in the Android Market

In the summer of 2010, the GTC identified applications capable of malicious activity in the Android Market.[11] The findings showed that one out of every 20 applications requested user permissions that could allow the application to place a call without a user knowing it or without any user interaction required. In all, the research indicated that 29 applications were found to request exactly the same permissions as known spyware applications.

Additionally, the GTC found that eight applications in the Android Market at the time requested an especially dangerous permission that could "brick" the mobile device, rendering it totally unusable. In all, 383 applications in the Android Market were found to have the ability to read or use authentication credentials from another service or application; and, of all the applications analyzed, three percent of them requested the permissions necessary to send an SMS message without the user's interaction or authorization.

The study also revealed numerous, malicious spyware applications—including the "Tap Snake" game that garnered headlines around the globe—and incorporated these into signatures in the Junos Pulse Mobile Security Suite to protect Juniper Networks customers.

July 2010: GPS Monitoring Spyware Cloaked in "Tap Snake" Game

In late July 2010, the "Tap Snake"[12] game—really an insidious spyware application—was released into the Android Market. To the casual user, it was nothing more than a simple game where the user guided the snake around obstacles by tapping the direction in which they would like the snake to move. In reality, "Tap Snake" was spyware that could monitor the mobile device's location through the device's GPS. It was accompanied by another application, "GPS Spy", which could be installed on an attacker's Android device and then used to access the Web portal to which the "Tap Snake" game uploaded the location of the victim's infected mobile device, for monitoring purposes.

August 2010: The First Android SMS Trojan

"Fake Player"[13] was the first known SMS trojan in Android devices, and it swept the world in August 2010, affecting many Russian users. The application pretends to be a media player application that sends SMS messages to Russian premium numbers at a rate of 6.00 USD (170 rubles) per message. While "Fake Player" was never released in the official Android Market, it has continued to be updated twice monthly since its original release. The most recent update came in the middle of October 2010.

November 2010: The "Angry Birds" Experiment

Shortly after the last known update to "Fake Player," security researchers Jon Oberheide and Zach Lanier unveiled a notable Android exploit with their revelation at an Intel security conference in Oregon.[14] Oberheide and Lanier showed that current iterations of the Android security model include a security flaw that allows an application to invisibly download additional applications, or APK files, without requiring the user to be alerted to the permissions of the downloaded applications—or even knowing that the applications were being installed!

In order to illustrate how the Android Market and similar app stores can be used against an unwitting mobile user, Oberheide and Lanier chose the tremendously popular game "Angry Birds" as their delivery mechanism. Their proof-of-concept malware did not contain any actual malicious code; it simply portrayed itself as bonus levels for "Angry Birds" that, once installed, would open up more levels for the player. In reality, nothing related to "Angry Birds" was ever included in the application. However, Oberheide and Lanier proved that users could be tricked into downloading this application, and that the application could download and install additional applications without prompting the user to approve the additional installs, or to verify and agree with the permissions required for the background applications to be installed.

More Android Attacks: 2010/2011

- November 2010: "Angry Birds" proof-of-concept malware demonstrated
- December 2010: First pirated Android application, Geinimi
- January 2011: ADRD and PJApps available in China

December 2010: Android Takes Crown as Primary Mobile Malware Target

Over the years, it has been common practice for malware writers to pirate Symbian and Windows Mobile applications and to then pack malicious code within these applications. However, in December 2010, researchers discovered that a series of Android applications, downloaded from the official Android Market, were being distributed through Chinese third-party application repositories and app stores. The legitimate applications were unpacked and the malicious code, known as "Geinimi," was added to as many as 24 different applications.[15] The modified applications were then repackaged, appearing as the original application to the casual user.

Geinimi infected applications were then posted to Chinese websites used to distribute software and mobile device applications. In many cases, several versions of the pirated applications were available, some malicious and others not. Unless the user paid attention to the permissions they were approving at the time of installation of the app, they would not realize that new malicious capabilities were being added to otherwise innocuous activities.

The first of its kind, Geinimi not only leveraged pirated Android applications for the distribution of malware, it also included rather extensive botnet-like command and control functionality, early attempts at encrypting communications, and the obfuscation of malicious code entered directly into the application. While Geinimi monitored communications, harvested mobile device identifying data, monitored location data, and enumerated lists of installed applications, it also used a relatively weak Data Encryption Standard (DES) cipher to encrypt particular strings in the code that would reveal the malicious intent when dissected. The same DES cipher was used to encrypt HTTP traffic for the command and control functions.

January/February 2011: The Storm Continues to Brew in China

In the weeks following the Geinimi discovery, researchers uncovered two additional families of malicious applications that followed the same basic approach and dissemination method. Both "ADRD"[16] and "PJApps"[17] are different families of legitimate applications that were pirated from the Android Market, deconstructed, packed with malicious code, and then repackaged for dissemination in third-party Chinese application stores. Together, ADRD and PJApps represented more than 75 different pirated and "trojanized" applications.

ADRD

While ADRD gathered extensive amounts of mobile device identifying information, it also attempted to identify the device's Wireless Application Protocol (WAP) gateway so that it could change the WAP settings to route traffic through a specific gateway. This artificially raised the search profile of sites containing additional ADRD infected applications, thereby promoting a greater number of downloads. ADRD also had the ability to reach out to the Internet and download updated versions of itself to the device.

PJApps

PJApps is similar in infection type and dissemination method as Geinimi and ADRD. When a device becomes infected with PJApps, it immediately attempts to register itself with an offline server by obtaining and sending mobile device identifying information to a URL. Once the device is registered, it is configured to download commands from a different URL that instructs the device to send SMS messages to premium rate numbers, check with an offline service to determine whether the device's number has been blacklisted anywhere, perform SMS spamming, download additional applications to the device, navigate to a given website after checking for the existence of a list of particular Android browsers, and set a series of browser bookmarks.

March 2011: Myournet/DroidDream Gives Android Users Nightmares

As researchers were still trying to uncover the extent of ADRD and PJApps, the Android Market was once again hit with a vengeance by "Myournet," also known as "DroidDream."[18] Myournet/DroidDream was also a series of legitimate applications that were pirated out of the Android Market, deconstructed, and then packed with malicious code. The difference between Myournet/DroidDream and Geinimi, ADRD, and PJApps, however, was the method of dissemination. In the case of Myournet/DroidDream, three different developer accounts were created and more than 55 infected applications were found inside the Android Market. The infected applications are known to have existed in the Android Market for at least four days, and were downloaded between 50,000 and 250,000 times onto unique Android devices.

Myournet was initially named after the first developer account identified to be pushing these malicious applications. Immediately after settling upon that name, the mobile security industry began calling the family of malicious applications DroidDream because it was considered to be the mother of all Android malware. In many cases, they were right.

Myournet/DroidDream began its reign of terror by attempting to leverage the "rageinthecage" exploit that allows root access to the mobile device. "Rooting" an Android device allows an application to gain access to systems and services that are not otherwise available to a normal app. Once Myournet/DroidDream had successfully rooted the device, it installed another APK file that was obfuscated inside the code of the original application. The installed application appeared to leverage the research conducted by Jon Oberheide, enabling the application to be installed in the background with absolutely no user intervention or knowledge.

The Attacks Against Android Continue: 2011

- March 2011: Myournet/DroidDream, the first Android malware available and distributed through Android Market on a large scale, affects 50,000 users.
- Google's solution, the Android Market Security Tool, was also pirated and turned into malware in China.
- April 2011: Walk-and-Text pirate puts egg on users' faces.
- April 2011: Research at IU Bloomington results in "Soundminer" proof-of-concept communications interception application.

The newly installed application provided Myournet/DroidDream with unfettered access to vast amounts of sensitive user and device identifying information, which was gathered and then sent off to a third-party server in California. Then, the infected application would facilitate the downloading and installation of additional applications onto the device, once again conducted without user interaction or knowledge.

Myournet/DroidDream marked the first time that Android malware had been made available and distributed through the Android Market on a large scale. The tactic showed that Google's open approach toward its Android Market could unfortunately allow malicious applications onto the ecosystem, with the potential to impact large numbers of users quickly.

Users suspecting they were infected with malware had only one recourse to reverse the effects of the infection—to perform a hard reset of their devices, possibly losing large amounts of data and settings if they had not been employing an effective backup and restore utility. The impact of over 50,000 users performing a hard reset of their mobile devices would also likely take a toll on mobile service providers, undoubtedly fielding thousands of support service calls.

Google released an application that would reverse the effects of the Myournet/DroidDream infections so that users would not be forced to perform a hard reset on their device. In doing so, Google released the Android Market Security Tool, which was automatically pushed to those mobile devices that had been infected with Myournet/DroidDream. Google determined which devices downloaded the applications by referring to the user's Checkout account. Even after installing this update, though, the underlying vulnerability responsible for the rooting does remain, thus accentuating the need for an endpoint anti-malware solution to prevent future infection related rooting from taking place.

The Android Market Security Tool was automatically pushed to the user's mobile device, installed, performed a series of activities to remove the effects of the Myournet/DroidDream infection, and then removed itself from the device. Therefore, it was not necessary for users to do anything other than wait for the update to be pushed to their device and to automatically begin cleaning up the infection. Google posted the Android Market Security Tool to the Android Market with *strict instructions* stating that it was not necessary to manually download the application. However, just a few days later, a version of the Android Market Security Tool that had been pirated off the Android Market, deconstructed, and packed with malicious code, was being disseminated in third-party app stores based in China.[19]

The corrupt version of the Android Market Security Tool in Chinese app stores had a few additional capabilities beyond those intended by Google. This newly pirated, trojanized version of the Android Market Security Tool gathered sensitive, device identifying information and shipped it to an offline server. Once the mobile device was checked in to the offline server, it began to receive commands to send SMS messages to premium rate numbers that were only effective inside of China and on Chinese service provider networks.

April 2011: The Joke's on You

Most recently, the Android world saw the fourteenth-rated application on the "101 Best Android Apps" list, "Walk and Text," pirated off of the Android Market.[20] However, this case was a little different—the developer who pirated and repackaged the application only meant to ridicule users who were installing pirated applications.

It appears that several hours after a new release of the popular "Walk and Text" application hit the Android Market, it was already being pirated and shared in third-party app stores. One enterprising developer grabbed this pirated version of the application off of a third-party app store and decided to follow the routine of his predecessors, deconstructing the application, and stuffing it with his own malicious code.

In the case of the malicious "Walk and Text" application, as soon as a user installed the application that had been "sideloaded," it began sending SMS messages to all of the user's contacts stored on the mobile device with a message stating, "Hey, just downlaoded [*sic*] a pirated App off the Internet, Walk and Text for Android. Im [*sic*] stupid and cheap, it costed [*sic*] only 1 buck [*sic*].Don\'t [*sic*] steal like I did!"

Using Research to Plug the Holes in Android

In 2010 and continuing into 2011, researchers at Indiana University, Bloomington collaborated with City University, Hong Kong to explore the possibility of "sensory malware" and communications interception. The research initiative[21] gave way to the proof-of-concept "Soundminer" application, which is capable of leveraging an Android device's microphone to monitor when a user calls a known credit card company. Once Soundminer identifies that a credit card company has been called, it listens for the user to input the actual credit card number, either by voice or by using the keypad, and transmits the captured information to an off-device location.

Not only does Soundminer revolutionize how sensitive data and personal information can be monitored and intercepted, it also breaks down the controls in the Android security model that prohibit an application from operating outside of its "sandbox," which is essentially a confined execution environment for running untrusted programs and to stop them from interacting with another application without going through a system API to do so. In order for Soundminer to function, it is coupled with a second application called "Deliverer," which actively transmits the captured data from the Android device to the receiving host.

The researchers showed that even though Soundminer and Deliverer operated within the constraints of their defined sandboxes, they were able to leverage characteristics of the Android operating system to pass information between themselves through covert channels. Specifically, Soundminer and Deliverer rely upon device settings such as volume or vibrate settings, which are available system-wide, to pass information back and forth between the two applications. In doing so, Soundminer is able to leverage its ability to translate voice and keypad patterns of credit card numbers into a specific series of settings changes that Deliverer recognizes as data it needs to translate and forward to the attacker's server.

While Soundminer has never been officially released to the public and remains proof-of-concept, it shows that research into and techniques for bypassing security controls in mobile platforms are ramping up. More of this type of research is needed to stay ahead of the increasingly complex types of malware that are emerging and that are able to avoid detection.

Apple iPhone and iPad

The Apple iPhone suffers from relatively little known malware, although applications exist to obtain user data and clandestinely transmit this information outside of the device.[22] In a study prepared for the NDSS 2011 conference, researchers from the Technical University of Vienna and the University of California, Santa Barbara worked with other universities to analyze 1,400 iPhone and iPad applications to determine the extent of personal data leakage by developers to third parties.

The results showed that nearly half of the analyzed applications leaked various forms of sensitive data to third parties. In most cases, application developers used prepackaged code purchased from advertising agencies, originally intended to collect device information that could be used to build advertising profiles of the device user. According to the researchers, the amount of data leakage was about the same in Apple App Store applications as in Cydia applications associated with *jailbroken* devices

To date, the major threat to iPhones is still associated with jailbroken devices and web-based jailbreak utilities that lure unsuspecting victims to malicious websites to attack the user's PC. Jailbreaking an Apple iOS device not only allows a user to sever ties with the vetting process of the Apple App Store; it allows users to install services such as SSH, which open the device to a plethora of risks.

RIM BlackBerry

In 2010, several instances of commercial spyware were released for the RIM BlackBerry device. FlexiSpy, Mobile Spy, MobiStealth, and SpyBubble[23] all expanded to include threats targeted specifically at BlackBerry devices. These spyware applications pose a great risk to ensuring the confidentiality, integrity, and availability of corporate data if they infiltrate BlackBerry devices connected to corporate assets.

Loss and Theft

The ultra portability of mobile devices enables users to have continuous access to business and personal information, regardless of location. However, this portability also leads to a significant risk of loss or theft of mobile devices.

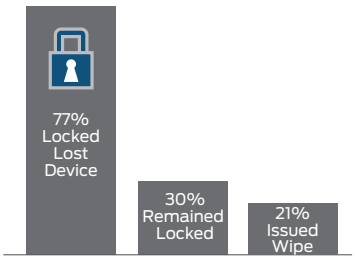
One in 20 mobile devices is lost or stolen, risking loss of confidential and sensitive data.

Data collected by the Juniper Networks GTC found that, in 2010, one out of every 20 enterprise, consumer, and government users registered with Junos Pulse Mobile Security Suite lost his or her mobile device, and had taken action to locate, lock, wipe, or back up their device. Not only was the data on the device at risk, but so were any bookmarked bank accounts with passwords set to auto-complete in the browser, contacts with pictures and addresses tied to the contact, calendar events, social media accounts, personal photos, pre-connected corporate email accounts, and other sensitive personal and corporate data.

1 out of 20 users registered with Junos Pulse Mobile Security Suite leveraged its capabilities to find and secure a lost or stolen mobile device.

A survey of registered Junos Pulse Mobile Security Suite users found that of the one out of 20 users who took action on a lost or stolen device, one-third used the "locate device" capabilities of Junos Pulse Mobile Security Suite to display the device's location within the product's online mapping functionality. Seventy-seven percent of the user subset then followed their locate requests by sending a command to lock the device in order to prohibit unauthorized access. Thirty percent of the user subset never issued an unlock command on the device, leading to the assumption that the device was never recovered. In such cases, best practice dictates that the user issue a wipe command in order to completely remove all of the data on the phone. Only 21% of users who locked their device issued a wipe command to protect their device, removing all personal or corporate data on the lost or stolen device.[24]

In line with forensic Apple iPhone encryption research[25] published by SMobile Systems in 2009, researchers at the Fraunhofer Institute Secure Information Technology (Fraunhofer SIT) revealed that it was trivial[26] for an attacker to use well-known exploits, scripts, and tools to jailbreak and decrypt passwords from the iPhone keychain. This includes passwords used for personal and corporate email, Wi-Fi, and VPN. Even if the device were protected by a screen locking mechanism or the user had enabled a passcode, it was still possible for attackers to fairly simply extract this sensitive information.



1/3 of Junos Pulse Mobile Security Suite users who took action on a lost or stolen device used GPS location data to track and locate the device.

77% of the 1/3 of Junos Pulse Mobile Security Suite users who took action on a lost or stolen mobile device locked the device to prohibit unauthorized access until the device could be recovered.

30% of those users never recovered their device and their device remained locked.

21% subsequently issued a wipe command

Data Communication Interception

The interception of communication is a threat to any device that sends and receives data and connects to a network. While mobile device communications over cellular networks are often encrypted, unauthorized individuals can use specialized equipment and tools to access the specific frequencies used by mobile devices, and listen to conversations between the devices and cell towers.

What's more, data encryption over cellular networks is easily broken, using a well documented and publicly available methodology. With approximately half of all smartphone devices today providing Wi-Fi capabilities, and 90 percent of all mobile devices projected to have this functionality by 2014[27], the risk of Wi-Fi sniffing (monitoring data in transit) accentuates the communication interception threat.

Numerous tools have been created to enable even novice computer users to easily intercept mobile data that is transmitted via WI-FI.

Specially crafted SMS/MMS message attacks can enable a person with malicious intent control over a mobile device or deem the device unusable.

Man-in-the-Middle (MITM) Attacks

Studies have shown that, once a mobile device connects to a Wi-Fi network, it is susceptible to Man-in-the-Middle (MITM) attacks, just like any other networked device on that segment.[28] In an MITM attack, the attacker introduces himself into a communication stream, becoming a "middle man" in a conversation, and logs all of the information relayed between the communicating parties. MITM attack tools are widely available, and the methodologies are well documented on websites such as Ethicalhacker.net.

Key Data Communications Intercept Findings

- 90% of all mobile devices will be Wi-Fi enabled by 2014.
- MITM attacks are increasingly possible against Wi-Fi enabled devices using widely available tools.

Depending on how a particular smartphone or tablet device application handles the data it transmits in the course of normal transactions, communications may be transmitted in clear text, making them visible to a middleman. Below is an example of an email sent by an Apple iPhone over Wi-Fi and intercepted using the common network monitoring tool, WireShark (see Figure 1).

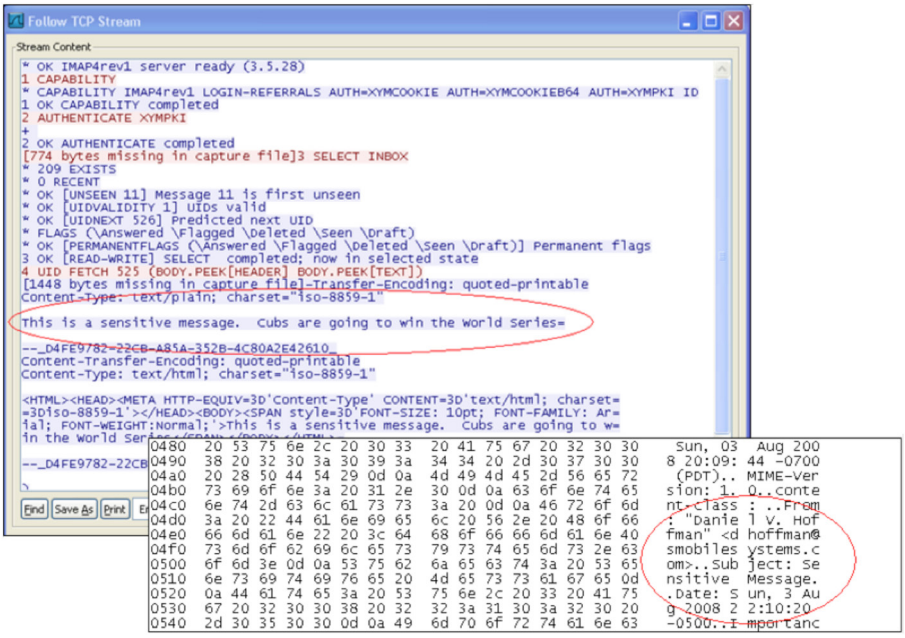


Figure 1: Example of email sent by an Apple iPhone over Wi-Fi and intercepted using the common network monitoring tool, WireShark.

Wi-Fi Hacking

In the past, Wi-Fi hacking required deep technical expertise. But today, these processes have been simplified to the extent that a user with basic computer knowledge can load a browser plug-in into Mozilla Firefox and easily hack into user email and social networking accounts by simply clicking a button in a browser extension. A specific example of this is the hacking tool, Firesheep, which was released in late 2010. With Firesheep, a person with malicious intent can run the Firefox plug-in and view specific user accounts that can access the Wi-Fi network simply by clicking the icon presented in the plug-in pane.

Rather than steal user credentials such as username and password, Firesheep intercepts the unencrypted cookie. Because access to the cookie enables the hacker to log in as the authenticated user simply by clicking an icon, this type of attack is very powerful. With Firesheep, hackers can easily exploit a user's email account on any Wi-Fi enabled device (see Figure 2).

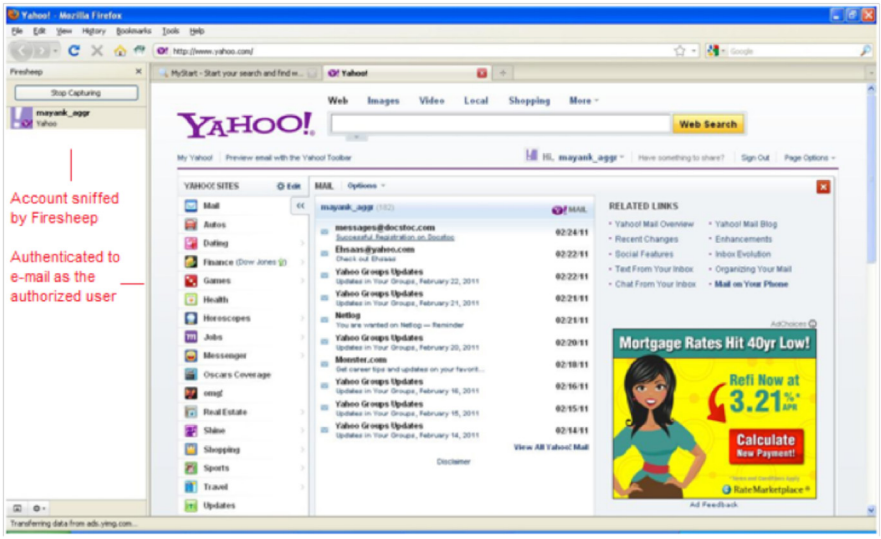


Figure 2: User's email account on an Apple iPad exploited by the Firesheep tool.

Using Firesheep to hijack a user's email account is merely one example of a Wi-Fi attack; there are many other attacks and tools capable of intercepting credentials and data itself. What is particularly noteworthy is the simplicity in executing this particular attack and the increased connectivity of smartphones and tablets to Wi-Fi hotspots.

Exploitation and Misconduct

As with many different aspects of security, the human element plays a central role in mobile security. The same threats of exploitation and misconduct that apply to personal and corporate computer users also apply to personal and corporate users of mobile devices. One notable difference, however, is that teenagers and employees now have 24x7 access to mobile devices, which significantly increases the threat.

In 2004, the Cyberbullying Research Center[29] was established to track and inform people of the dangers that children face from their peers while they are online. This center has gone to great lengths to study and document the phenomenon. One of the most important findings is that cell phones continue to be the most popular technological device used by teens. In fact, 83 percent of all teens report using a cell phone at least weekly.

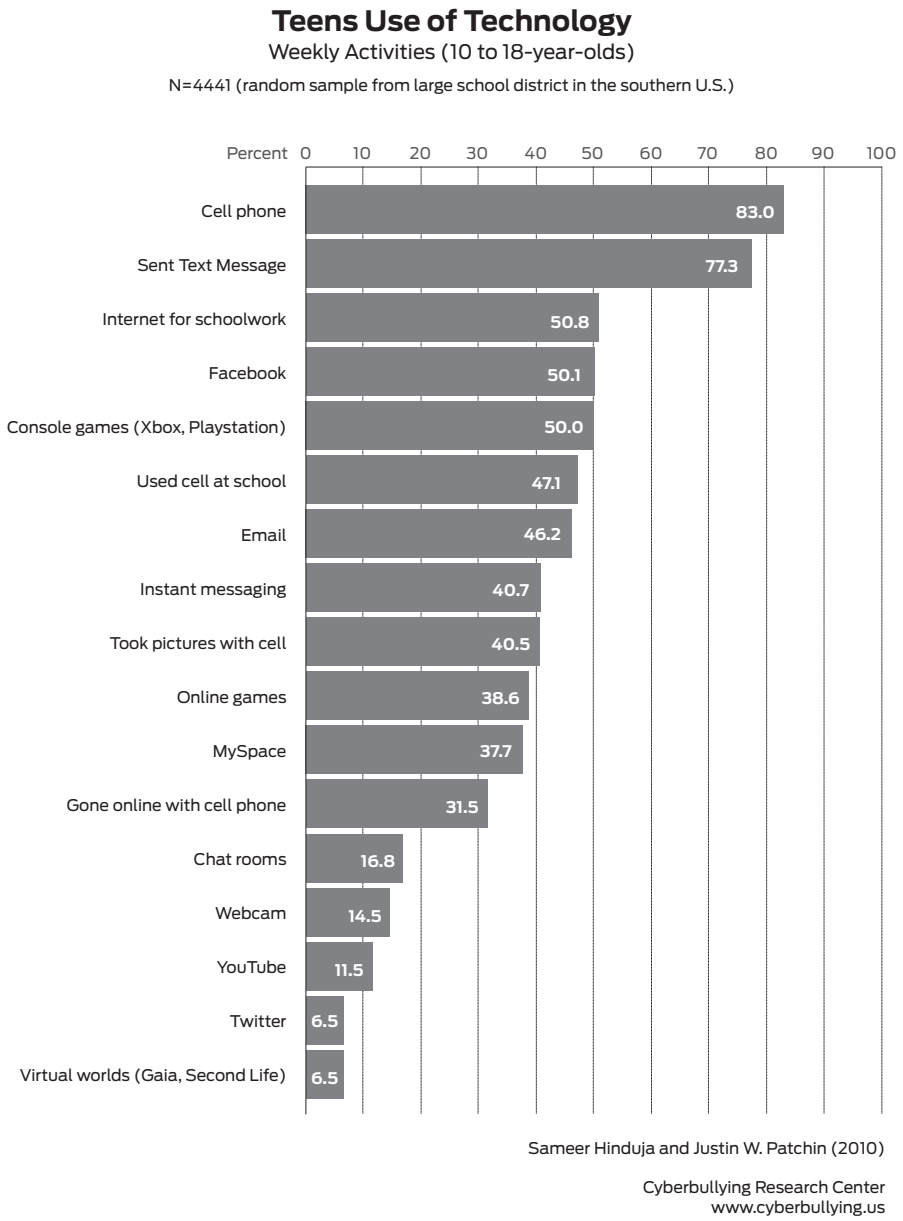


Figure 3: Most teens use their cell phones and send text messages at least weekly.

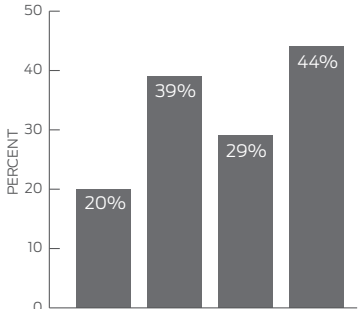
Social media tools are also areas where teens have reported being bullied and harassed by their peers. To exacerbate the problem, social media applications are easily accessible from the smartphones that most teens carry in their pockets. Shockingly, nearly 21 percent of all teens surveyed have been bullied in one form or another over social media.

In addition to cyberbullying, teens are also using their mobile devices for inappropriate or suggestive use. Just as parents are able to remain connected in the corporate world, smartphones make it easy for teens to stay in touch with their friends as well. Studies show that 20 percent of all teens have sent inappropriate or explicit pictures or videos of themselves from their phones. And 39 percent of teens have sent suggestive messages via SMS.

Exploitation and Misconduct Key Findings:

- 83% of teens use mobile technology to stay connected with friends and family.
- 20% of all teens have been cyberbullied through a mobile device.
- 20% of all teens admit to sending inappropriate or explicit pictures or videos of themselves from a mobile device.

Even more eye-opening is that 29 percent of teens who report sending suggestive content to someone from their mobile phone say that they only know the recipient through online means or have never met the other person at all! Further, 44 percent of teens also freely admit that it is common practice for sexually suggestive content to be shared with individuals other than the intended recipient.[30]



20% of teens admit to having sent inappropriate or explicit pictures or videos from their cell phones

39% of teens admit to sending sexually suggestive messages from their device

29% of teens admit that they are sending suggestive messages, or inappropriate and explicit pictures or videos to someone they have never met

44% of teens admit that it is common for suggestive messages that were received to be shared with someone else

With smartphones, there is the additional concern of corporate data leakage. Enterprise security administrators must ensure not only the safety of the information inside their network, but also that information is not being distributed beyond the company's security perimeter exposing it to misuse. Smartphones and tablet devices provide a convenient means for transferring massive amounts of data, just as a laptop or USB thumb drive. Today's smartphones can store more than 16 gigabytes of data. Additionally, the camera features of mobile devices enable employees with malicious intent to transmit sensitive information outside of an organization in a format commonly undetectable to traditional email monitoring technologies.

Direct Attacks

In the realm of personal computers, buffer overflows and similar direct attacks are commonly used to exploit systems. These attacks can target computer interfaces, subsystems, browsers, and programs running on the device as well as associated protocols. Additionally, devices can be scanned as a means to identify the type of device and operating system in use, so that the attacker can formulate and launch an appropriate exploit. Mobile devices share these same threat vectors, plus with the additional components of the SMS and MMS messaging interfaces. Direct attacks on smartphones and tablet devices have a two-fold goal:

1. Exploit the device to gain control over device functions and data
2. Render the device or components unusable via denial-of-service (DoS) attacks

- Direct attack landscape is 2-fold—exploits to control device and data, and denial-of-service (DoS) attacks.
- Browser-based attacks have been known to be effective against mobile browsers.

To date, reported mobile direct attacks predominantly focus on the SMS and MMS messaging components of smartphone devices. One well-known example is the Curse of Silence[31] attack against Symbian devices. By sending a specifically crafted SMS message, attackers can render a significant number of Symbian devices unusable when the devices simply receive the message.

For Apple iPhone devices, proofs of concept have been released whereby simply receiving a malformed SMS message allows an attacker complete control of the iPhone[32], including the ability to dial the phone, visit websites, activate the device's camera, and further propagate the attack by sending additional malformed SMS messages to contacts listed in the user's address book. Similar Windows Mobile and Android SMS attacks have been reported and discussed online.

By sending hundreds of SMS messages to a smartphone, a device can be spammed to the point where it is unable to distinguish wanted from unwanted text messages or to adequately use the messaging function of the device. This simple DoS attack can render a smartphone unusable and commonly targets first responders, who rely heavily on SMS messaging when responding to emergencies and other incidents.

In addition to SMS message attacks, 2010 also saw a proliferation of browser-based exploits. For example, the simple act of visiting a specific webpage from an Apple iPhone can jailbreak the device and, in noted cases, render various components of the operating system inoperable.[33]

A browser-based proof-of-concept exploit for Android was released in 2009. This exploit allowed an attacker access to sensitive user information on the device and was categorized as a severe/critical exploit.

As mobile browsers become as powerful as those associated with personal computers, browser-based attacks will continue to increase. Attackers will surely exploit the same known browser vulnerabilities on mobile devices as they do on personal computers.

Looking Ahead: The Year of Mobile Malware

While well established smartphone platforms such as Symbian and Windows Mobile have been a proving ground for malicious developers over the past five years, 2010 saw the crown handed over to the Google Android platform. As the dominant, growing force in the mobile operating system market, Google Android captured the lion's share of attention from malware and exploit developers in 2010.

This attention is continuing well into 2011. In the first four months of 2011, several exploits have emerged based on research and development conducted in 2010, combining techniques for bypassing controls in the Android security model. These include bypassing permission checks, leveraging covert communication channels to illegally communicate between applications to avoid detection, invisibly installing applications, and opening backdoor communication channels that will undoubtedly lead to complex mobile botnets.

The Juniper Networks Global Threat Center predicts that 2011 will be the year of mobile malware, and consumers and enterprises can expect to see more advanced malware attacks against the Android platform. Further, the Juniper Networks GTC expects to see command and control capabilities for zombies and botnet participators, devices that are remotely controlled to execute malicious attacks. While *rootkits*—applications that can root a device upon infection—have mostly been theoretical or difficult to implement in mobile devices until now, Juniper Networks anticipates that, in 2011, the door will open for these malicious programs due to the increasing sophistication of hackers.

As payment options such as Near-Field Communications (NFC) become widely adopted in 2011, the Juniper Networks GTC anticipates that an increasing number of malware attacks targeted at intercepting valuable financial information will emerge. This year will also bring more concerted effort on the part of malicious individuals to attack the mobile browser as an entry point into a device for infection. Today, browser exploits are the leading attack platform for PC malware, and Juniper Networks expects that this will become a major focus of mobile device exploit artists in 2011.

Juniper Networks also anticipates an increase in malware over 2011 that infiltrates mobile devices through application stores, whether run by mobile operating system developers or known and trusted Web vendors. Additionally, as unauthorized application stores continue to multiply, sideloading will continue to grow as a major source of malware dissemination throughout 2011.

Finally, Juniper Networks expects to see an increase in the frequency of malicious SMS and MMS messages specifically intended to exploit mobile devices. To date, nominal research into these messaging mediums has resulted in numerous exploits capable of taking control of mobile devices. While much of the legacy threat from mobile malware has centered on the financial aspect of sending SMS messages to premium rate numbers for profit, Juniper Networks anticipates that, in 2011, significant progress will be made by exploit artists in using SMS and MMS as an entry point into a mobile device.

Now What: Steps to Protecting Mobile Devices

In each of the malicious threats and attacks described in this report, proper mobile security and device management protections would have alleviated the risk of exploitation.

For Consumers

In order for consumers to protect themselves from the growing mobile malware threat, Juniper Networks recommends installing the following security solutions on their mobile devices:

- On-device anti-malware solution to protect against malicious applications, spyware, infected SD cards, and malware-based attacks on the device
- On-device personal firewall to protect device interfaces
- Password protection for device access
- Remote locate, track, lock, wipe, backup and restore software to retrieve and restore a lost or stolen device
- Antispam software to protect against unwanted voice and SMS/MMS communications
- (For parents) Device usage monitoring software to monitor and control pre-adult mobile device usage and protect against cyberbullying, cyberstalking, inappropriate use, and other online threats, including automated alerting for:
  - SMS message content
  - Email message content
  - Insight into pictures taken, sent, and received by the device, as well as those stored on the device
  - Installed applications
  - Address book and contact lists

For Enterprises

When implementing a mobile security solution, Juniper Networks recommends that enterprises, government agencies, and small and medium sized businesses (SMBs) implement the following components:

- On-device anti-malware to protect against malicious applications, spyware, infected SD cards and malware-based attacks to the device
- On-device firewall to protect device interfaces
- SSL VPN clients to effortlessly protect data in transit, and to ensure secure and appropriate network access and authorization
- Centralized remote locate, track, lock, wipe, backup and restore facilities for lost and stolen devices
- Centralized administration to enforce and report on security policies across the entire mobile device population
- Support for all major mobile platforms, including Google Android, RIM BlackBerry, Apple iOS, Microsoft Windows Mobile, and Nokia Symbian
- Device monitor and control, such as the monitoring of messaging and control of installed applications
- A solution that integrates with network-based technologies, such as network access control (NAC), to ensure the security posture of mobile devices and determine appropriate access rights prior to allowing access to corporate resources
- Management capabilities to enforce security policies, such as mandating the use of PINs/passcodes
- Ability for an administrator to monitor device activity for data leakage and inappropriate use

About the Juniper Networks Global Threat Center

The Juniper Networks Global Threat Center is the only "CERT-Style" organization in the world that conducts around-the-clock security, vulnerability, and malware research tailored specifically to mobile device platforms and technologies.

Consisting of highly skilled security professionals who have earned well-known industry certifications, including Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Certified Hacking Forensic Investigator (CHFI), the GTC research team members are experienced corporate, military, government, and academic professionals with decades of expertise in designing, building, managing, securing, attacking, and auditing networks and devices.

The GTC applies a proven, methodology-driven analysis of security concepts to mobile devices and operating systems, leveraging security concepts and advances to the three primary pillars of information security—confidentiality, integrity, and availability—to the dynamic mobile device market.

Based out of the Juniper Networks Mobile Center of Excellence located in Columbus, Ohio, the GTC consists of four teams:

- **Malware Research Team:** Identifies new mobile malware threats and device exploits.
- **Exploit Resolution and Integration Team:** Works with the Malware Research Team and other Juniper Networks development teams to mitigate discovered risks and incorporate those solutions into Juniper Networks products, including the Junos Pulse Mobile Security Suite.
- **Device Analysis Team:** Analyzes new devices as they are released to identify platform vulnerabilities. Where necessary, the team ethically discloses any findings or research to the appropriate vendor in order to address platform or application vulnerabilities that could lead to exploit or compromise.
- **Device Testing Team:** Conducts testing of threat resolutions, new virus signatures, and performance testing of Juniper Networks products across various device platforms.

Juniper Networks Global Threat Center research and output may be viewed at **www.globalthreatcenter.com**.

Glossary of Terms

Antivirus: Software that is used to prevent, detect, and remove malware, including but not limited to viruses, worms, trojans, spyware, and adware.

APK: Android Package (e.g., "filename.apk"), a packaging file format for the Android mobile operating system.

Botnet: A collection of software agents, robots, or "zombies" that run autonomously and automatically, typically overtaken by hackers to perform malicious operations.

Buffer Overflow (also known as buffer overrun): An anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. Buffer overflows can be triggered by inputs that are designed to execute code or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security.

CERT: Computer Emergency Response Team.

Cydia: Apple iOS application that allows users to locate and download apps for jailbroken iPhones and iPads.

Denial of Service (DoS): An attack which attempts to make a computer or mobile device resource unavailable to its intended users or for its intended use.

Data Encryption Standard (DES): A block cipher that uses shared secret encryption.

Hypertext Transfer Protocol (HTTP): A networking protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Jailbroken: An Apple iPhone or iPad that has had its Apple iOS operating system covertly "unlocked" to gain full root access, removing all Apple imposed limitations on applications, and essentially exposing all of an application's features.

Keylogging: Keystroke logging or the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that actions are being monitored. There are numerous keylogging methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis.

Malware: Short for malicious software, a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Multimedia Messaging Service (MMS): A standard way to send messages that include multimedia content to and from mobile devices. MMS extends the core SMS capability that allows exchange of text messages only up to 160 characters in length.

Phishing: A way of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social websites, auction sites, online payment processors, or IT administrators are commonly used to lure unsuspecting users.

Premium Rate Numbers: A billing mechanism that allows providers to bill consumers for services via SMS, MMS, WAP content, or video services. It is usually a 5-digit number that charges the consumer a specific amount that is then deposited in the account of the premium rate number owner.

Rootkit: Malware that lurks camouflaged from anti-malware software and administrators by circumventing or interrupting standard operating system or other application functionality, allowing unseen and unwanted privileged access to a device.

Sandbox: A security mechanism for separating running programs.

Secure Digital (SD): A non-volatile memory card format developed by the SD Card Association for use in portable devices.

Short Message Service (SMS): The text communication service component of phone, Web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line and mobile devices.

Secure Shell (SSH): A network protocol that allows data to be exchanged using a secure channel between two networked devices. The two major versions of the protocol are referred to as SSH1 (or SSH-1), and SSH2 (or SSH-2). Used primarily on Linux and Unix-based systems to access shell accounts, SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, rendering them susceptible to packet analysis.

Spyware: A type of malware that collects information and makes it available, usually secretly, to a third party. The presence of spyware is typically hidden from the user and can be difficult to detect.

Trojan: Shortened from the Trojan Horse story in history, software that appears to perform a desirable function while containing malicious and/or undesirable elements.

Virus Definition/Signature: A unique string of bits, or the binary pattern of the machine code of a virus. The term "virus definitions" typically refers to the database of all current virus signature files used by a particular antivirus software for virus detection. Virus definitions are the primary method of detection for most antivirus software programs.

Wireless Application Protocol (WAP): An open international standard; commonly used Web browser for small mobile devices such as cell phones or smartphones.

Zombie: An Internet connected mobile device that has been compromised by a virus or trojan that can be used to perform malicious tasks under remote direction, usually from a botnet.

References

1. Information obtained from analysis of Junos Pulse Mobile Security Suite virus definition database dated 2/15/2011
2. **www.FlexiSpy.com**
3. **www.mobile-spy.com**
4. **www.mobistealth.com**
5. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization, and is highly respected throughout the security community, with programs reaching more than 165,000 security professionals around the world. **www.sans.org**
6. **http://www.infoworld.com/t/malware/sans-study-one-in-five-mobile-devices-running-malware-997**
7. Information obtained from analysis of Junos Pulse Mobile Security Suite infection reporting/alerting
8. Information obtained from analysis of Junos Pulse Mobile Security Suite virus definition database dated 2/15/2011
9. **http://www.phonearena.com/htmls/Malicious-banking-app-found-in-the-Android-Marketplace-article-a_8744.html**
10. **http://isc.sans.edu/diary.html?storyid=8389**
11. **http://threatcenter.smobilesystems.com/?p=1887**
12. **http://threatcenter.smobilesystems.com/?p=1901**
13. **http://threatcenter.smobilesystems.com/?p=1907**
14. **http://blogs.forbes.com/andygreenberg/2010/11/10/when-angry-birds-attack-new-android-bug-lets-spoofed-apps-run-wild/**
15. **http://globalthreatcenter.com/?p=2056**
16. **http://globalthreatcenter.com/?p=2081**
17. **http://globalthreatcenter.com/?p=2226**
18. **http://globalthreatcenter.com/?p=2091**
19. **http://globalthreatcenter.com/?p=2108**
20. **http://globalthreatcenter.com/?p=2135**
22. **https://www.cs.indiana.edu/~kapadia/papers/soundminer-ndss11.pdf**
22. **http://www.iseclab.org/papers/egele-ndss11.pdf**
23. **www.spybubble.com**
24. Information obtained from Junos Pulse Mobile Security Suite internal transaction logs
25. **http://globalthreatcenter.com/?p=972**
26. **http://www.engadget.com/2011/02/10/researchers-steal-lost-iphone-passwords-in-6-minutes-video/**
27. **http://www.wi-fi.org/news_articles.php?f=media_news&news_id=969**
28. **http://threatcenter.smobilesystems.com/?p=1587**
29. **http://www.cyberbullying.us/research.php**
30. **http://www.pcsndreams.com/Pages/Sexting_Statistics.html**
31. **http://www.engadget.com/2008/12/31/curse-of-silence-exploit-squelches-inbound-sms-mms-to-nokia-s6/**
32. **http://www.pcworld.com/article/169436/black_hat_reveals_iphone_sms_vulnerability.html**
33. **http://www.iphoneincanada.ca/iphone-news/iphone-exploited-at-cansecwest-browser-jailbreak-revived/**

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

2000415-001-EN May 2011 Printed on recycled paper