



SMARTPHONES

Creating a Mobile Workforce and a New Hacker Landscape

A White Paper

January 2011

This page intentionally left blank.

Table of Contents

1	<u>INTRODUCTION.....</u>	<u>1</u>
2	<u>PROBLEMS</u>	<u>1</u>
3	<u>SOLUTIONS</u>	<u>3</u>

1 INTRODUCTION

“Smartphones” are generating two-thirds of total mobile cellular traffic worldwide despite the fact only one out of every seven mobile subscribers is using one. Smartphone users are spending more and more time on the Internet and their average traffic per user is projected to increase by 700% over the next five years. The number of mobile devices that are interacting with corporate environments is also skyrocketing. It is predicted that by 2015, mobile devices (smartphones, iPads, and non-PC tablets) will outnumber computers in corporate networks. After all, the latest mobile devices combine portability, function rich applications, access to corporate networks and data, are web enabled, and allow for online collaboration. Furthermore, they live outside your firewall and often make simultaneous use of various wireless networks (Bluetooth, Wi-Fi, and cellular).



As the popularity of smartphones like the iPhone and Android skyrockets, so does the attention received from individuals looking to exploit such technology. Smartphone viruses and malicious applications are beginning to appear at a rapid pace and chances are they have already introduced an adverse affect on the security posture of your corporate or government network. Although major malware outbreaks on smartphones on the scale of PC infections of past years are not as common, the amount of attacks is on the rise. More than twice the number of malware and spyware attacks are hitting BlackBerry, Windows Mobile, and Android phones than six months ago. Most of the known viruses and Trojans will propagate through Bluetooth or Multimedia Messaging (MMS), but new attack vectors are materializing that follow smartphone user behavior trends and exploit the booming popularity of downloadable applications.

2 PROBLEMS

Smartphone use on your networks can introduce a variety of risks including poorly engineered and maliciously designed applications, loss of corporate data, and other vulnerabilities associated with the latest mobile device and associated technology (web, web browsers, mobile code). A large effort lately has been focused on grabbing personal information in attempts to monetize it by reselling the information.



The Coverity Scan 2010 Open Source Integrity Report reveals test findings of more than 61 million lines of open-source code from 291 open-source projects, including Android, Linux, Apache, Samba, and PHP. Android devices, which are currently shipping out at a rate of 65,000 devices a day, have been linked to 88 high-risk defects that included memory corruption, memory illegal access, and resource leak-type flaws that could crash the system or result of loss of data.

The App Genome Project, created to map and study mobile applications, has identified about a third of mobile phone applications have the ability to collect some form of your phone's personal information (device phone number, subscriber identifier number, voicemail password, physical location). A majority of these applications do so for legitimate reasons based on the advertised functionality of the application, but some applications do not need such access. What malicious applications do with your information is still largely unknown, but there have been cases where certain applications have been found to send your information to other websites and servers housed in foreign countries.

Another smartphone weakness is they are easily lost or stolen. Without the proper protection measures in place, your data could be at risk. Most devices have the ability to be locked by the user through a unique passcode, usually a pin or a custom swipe pattern, but even those techniques will not ensure your information remains protected. Recent studies have found oily smudges your fingers leave behind on the touch screens could betray you. A team of researchers have described a method for uncovering the smartphone password based on the fingerprints on the touchscreen. The three main reasons smudge attacks are a threat to smartphone security are the smudges are surprisingly persistent in time, they are difficult to obscure or delete the smudges, and analyzing the smudges can be done with a camera and a computer. The security risk is present on all touchscreen smartphones to some extent, but it is a much bigger risk on Android devices that rely on a swipe pattern rather than the more traditional numeric or alphanumeric PIN.

Spyware seems to be the primary threat being created for BlackBerrys likely due to the heavy corporate use of BlackBerrys, which would make any data lifted from them more easily monetized. Windows Mobile phones suffer more from traditional malware. For example, a recent attack leveraged an existing, legitimate smartphone application and injected it with an auto-dialer that was automatically started up when the user ran the application and with the user incurring the unauthorized charges. Androids are suffering from both types of threats. Two flaws were recently discovered in the Android OS that could allow attackers to install malicious applications on Android-based devices without the owner's knowledge by exploiting vulnerabilities in fake add-ons for real Android applications and by incorrect settings in device web browsers. Web browsing enables a range of malware for smartphones in general, identified exploits can dive down into the phone's browser and the phone itself. iPhones are also targeted, but most exploits are associated with "jail-broken" phones. Jailbroken devices, between 6 to 8 percent of all iPhones, can run code or applications on the devices that aren't "signed" by Apple. iPhone malware (iPhone/Privacy.A, iPhoneOS.lkee) can copy the user's email, contacts, SMS text messages, calendar, photos, music, video, and other data gathered by an iPhone app and the victim would have no idea his iPhone was hacked.

3 SOLUTIONS

With the added focus of improving available security features, such devices are now becoming accepted for use in enterprise environments, but there are still significant gaps. For example, even though new Android operating system versions offer enhancements like ActiveSync policies that include password complexity requirements and remote wiping capabilities, they still lack other desirable features such as certificate authentication and built-in hardware encryption. With these things in mind, now is the time for enterprises to start thinking systematically about these sorts of issues, because there is no simple, formulaic solution to the problem of smartphone security. A comprehensive security scheme needs to be designed that can be implemented, monitored, and enforced through a collection of enforceable policies and procedures, software products, and user awareness and training.

Policies that should be considered should include restricting mobile user's access to sensitive data from their devices unless the data is fully encrypted and the phone is centrally managed. This should include a policy for remote device management, so compromised or lost devices can be locked or erased and establishing an approved list of applications users can use or download on these devices. This helps protect against the data and monetary losses that could be incurred from a compromised or lost phone. Information security departments need to adjust to the new threat landscape, where managing the vulnerabilities inside the company is less about plugging software holes and more about protecting data.

Also a policy regarding the monitoring of your wireless networks to detect rogue devices and attacks is typically a good idea. While compromised devices are a danger, the small form factor of most mobile devices means attackers could load in a variety of attack programs in a smartphone and find a way to have it delivered to the corporate office. Once inside the network, the phone could be used to exfiltrate data.

Given the fact most mobile devices are not owned by the company but by the employee, it is recommended companies develop mobile device security policies and discuss those policies with their employees. These policies are bound to introduce a variety of privacy concerns based on the type of information the company chooses to track (i.e. end user's locations, archive SMS messages, phone calls). The level of privacy loss versus security compliance is a tough decision companies will have to consider as they develop mobile security policies.

There are also commercial security applications that can help businesses enforce their Acceptable Use and Privacy Policies on company-provided phones. Such applications can silently track GPS locations, SMS messages, photos, and calls of employees inside a secure online control panel. This application runs in total stealth mode and no mentions of the program are shown on the phone. The software runs in the background behind all other applications and silently uploads captured information a secure online account, which can be checked from the web without requiring further access to the phone. Other options include

hiring a managed service for mobile security. Fee-based services exist that will push out regular patches and security fixes and manage other aspects of your mobile security program.