Mobile Devices: The Case for Cyber Security
Hardened Systems

Maurice Dawson
Jorja Wright, University of Charleston
Marwan Omar

Available at: https://works.bepress.com/maurice_dawson/29/
Chapter 2
Mobile Devices:
The Case for Cyber Security
Hardened Systems

Maurice Dawson
University of Missouri – St. Louis, USA

Jorja Wright
Florida Institute of Technology, USA

Marwan Omar
Nawroz University, Iraq

ABSTRACT

Mobile devices are becoming a method to provide an efficient and convenient way to access, find and
share information; however, the availability of this information has caused an increase in cyber attacks.
Currently, cyber threats range from Trojans and viruses to botnets and toolkits. Presently, 96% of mobile
devices do not have pre-installed security software while approximately 65% of the vulnerabilities are
found within the application layer. This lack in security and policy driven systems is an opportunity for
malicious cyber attackers to hack into the various popular devices. Traditional security software found in
desktop computing platforms, such as firewalls, antivirus, and encryption, is widely used by the general
public in mobile devices. Moreover, mobile devices are even more vulnerable than personal desktop
computers because more people are using mobile devices to do personal tasks. This review attempts to
display the importance of developing a national security policy created for mobile devices in order to
protect sensitive and confidential data.

INTRODUCTION

Currently, mobile devices are the preferred device for web browsing, emailing, using social media and
making purchases. Due to their size, mobile devices are easily carried in people’s pockets, purses or
briefcases. Unfortunately, the popularity of mobile devices is a breeding ground for cyber attackers.
Operating systems on mobile devices do not contain security software to protect data. For example,
DOI: 10.4018/978-1-4666-8345-7.ch002
traditional security software found in personal computers (PCs), such as firewalls, antivirus, and encryption, is not currently available in mobile devices (Ruggiero, 2011). In addition to this, mobile phone operating systems are not frequently updated like their PC counterparts. Cyber attackers can use this gap in security to their advantage. An example of this gap in security is seen in the 2011 Valentine’s Day attack. Cyber-attackers dispersed a mobile picture-sharing application that covertly sent premium-rate text messages from a user’s mobile phone (Ruggiero, 2011). Thus, this example illustrates the importance of having a security policy for mobile phones.

Social Networking and Electronic Commerce (E-Commerce) Applications

Many people rely on their mobile devices to do numerous activities, like sending emails, storing contact information, passwords and other sensitive data. In addition to this, mobile devices are the device of choice when it comes to social networking; thus, mobile applications for social networking sites (Facebook, Twitter, Google+) are another loophole for cyber attackers to gain personal data from unsuspecting users (Ruggiero, 2011). Social networking sites are host to a surplus of personal data. That is why malicious applications that use social networking sites to steal data yield severe consequences. Recently, M-Commerce or “mobile e-commerce” has gained popularity in our society. Many smartphone users can now conduct monetary transactions, such as buying goods and applications (apps), redeeming coupons and tickets, banking and processing point-of-sale payments (Ruggiero, 2011). Again, all of these smartphone functions are convenient for the user but advantageous for malicious cyber attackers. Ultimately, there is a niche in technology for cyber security software that is specifically designed for the mobile operating system.

Hypothetical Consequences of Cyber Attacks on Smartphones

The consequences of a cyber attack on a smartphone can be just as detrimental, or even more detrimental than an attack on a PC. According to Patrick Traynor, a researcher and assistant professor at the Georgia Tech School of Computer Science, mobile apps rely on the browser to operate (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). As a result of this, more Web-based attacks on mobile devices will increase throughout the year. Traynor also states that IT professionals, computer scientists and engineers still need to explore the variations between mobile and traditional desktop browsers to fully understand how to prevent cyber attacks (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012).

Challenges with a Mobile Browser

One cyber security challenge for mobile devices is the screen size. For example, web address bars (which appear once the user clicks on the browser app) disappear after a few seconds on a smartphone because of the small screen size (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is usually the first-line of defense for cyber security. Checking the Uniform Resource Locator (URL) of a website is the first way users can insure that they are at a legitimate website. Moreover, SSL certificates for a website are usually more difficult to find on a mobile phone browser (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This adds another gap in security for mobile devices. Furthermore, the touch-screen
attribute of mobile phones can be cause for concern when dealing with cyber attackers. Traynor states that the way elements are placed on a page and users’ actions are all opportunities to implant an attack. An illustration of this is seen when an attacker creates an attractive display content (i.e. an advertisement for an app or a link to a social media app) in which the malicious link is carefully hidden underneath a legitimate image. Unfortunately, once the user clicks the image they can be redirected to the malicious content via the link (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012).

**Common Mobile Device OS: iOS and Linux**

Apple debuted iOS, or iPhone OS, in 2007, with the inception of the iPhone to the cell phone market (Barrera & Van Oorschot, 2011). Presently, the iOS platform not only runs on iPhone but also iPod Touch and iPad (Barrera & Van Oorschot, 2011). Apple developers specifically write apps to run on all iOS devices. Apple’s iOS popularity stems from an easy user interface, including “onscreen interactive menus, 2D and 3D graphics, location services, and core OS functionality such as threads and network sockets” (Barrera & Van Oorschot, 2011).

Apple utilizes various techniques to ensure that the security and quality of their applications are not compromised by malicious cyber attackers. Unlike Android’s OS, iOS prevents third-party apps from accessing external data by utilizing a “sandbox mechanism” (Barrera & Van Oorschot, 2011). This mechanism employs policy files that restrict access to certain device features and data (Barrera & Van Oorschot, 2011). App developers use registered Application Programming Interface (APIs) to restrict apps from accessing protected resources (Barrera & Van Oorschot, 2011). Finally, Apple approves every iOS app developers create. The approval process has not been published by Apple, however it is believed that “the company employs both automated and manual verification of submitted apps” (Barrera & Van Oorschot, 2011). Once Apple approves a potential app, Apple “digitally signs it and releases it” to the App Store (Barrera & Van Oorschot, 2011). Ultimately, Apple has the final say pertaining to which apps are available for download in the App Store – “apps that Apple hasn’t digitally signed can’t run on the device” (Barrera & Van Oorschot, 2011).

Linux is a Unix like Operating System (OS) that is built on the Linux kernel developed by Linus Torvalds with thousands of software engineers. As of 2012 there are over two hundred active Linux distributions. The majority of the kernel and associated packages are free and OSS. This type of software provides a license which allows users the right to use, copy, study, change, and improve the software as the source code is made available. Providing source code allows developers or engineers to understand the inner workings of development. Imagine being able to study Mac or Windows by viewing all the source code to replicate similar developments. This exercise is great for a developer to learn low level coding techniques, design, integration, and implementation. This is also a great method for penetration testing with the ability to test all available back doors within the software.

In terms of associated cost the majority of Linux distributions are free. However some distributions require a cost for updates or assistance that related to specific needs such as OS modifications for server hosting. In software, there is a packet management system that automates the process of installing, configuring, upgrading, and removing software packages from an OS. In the Linux OS builds the most common packet management systems are Debian, Red Hat Package Manager (RPM), Knoppix, and netpkg. The most popular Linux distributions for mobile use are Android IOS and Ubuntu.
Malware Attacks on Smartphone OS

Along with this, malware that targets smartphone operating systems is constantly evolving. An example of this is seen with “Zeus-in-the-Mobile” (ZitMo), a specific form of malware common to the Android operating system. ZitMo targeted Android users’ bank apps; it attempted to bypass the banking two-factor authentication, steal credentials and gain access to users’ bank accounts, and ultimately money (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is just one form of cyber attacks that IT professionals are trying to prevent from occurring.

Lastly, it is believed that mobile devices will be the new vector for targeting network and critical systems (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). According to the report, mobile devices are an excellent way to spread malware because phones are great storage devices. A hypothetical example of a wormcyber attack against a company’s network is seen when malware is implanted in a smartphone. For example, a clever cyber attacker can write code to remotely control wireless connectivity technology and plant malware on the mobile phone. If that same phone is connected to a corporate network, i.e. the user is charging the phone on the company’s computer; the malware can now attack the company’s network. IT professionals want to prevent attacks like that from occurring because the economic consequences of such an event would be catastrophic. Ultimately, it is imperative that a national security standard is created for mobile devices in order to protect personal data.

The Android Platform

According to Shabtai et al. (2010), Android is an open-source application execution environment that includes an operating system, application framework, and core applications. Android was designed and released originally by Android Inc. to provide a user-friendly, open, and easy-to-use mobile-based development environment. This open-source mobile development framework is user-centric because it provides a variety of developments, tools, and features. However, this open-development feature also poses challenges to securing sensitive user data and protecting users from malicious attacks, such as phishing applications that are usually sent to users to trick them into providing their financial information and credentials while accessing malicious websites that look the same as the legitimate banking sites.

The Android operating system was first released in October, 2008 by T-Mobile 1G, and soon major telecommunications companies (such as T-Mobile) in both the U.S. and Europe adopted it because of its rich capabilities exemplified by core applications (i.e., email, web browsing, and MMS), entertainment features, and services, such as camera and Bluetooth. This has also led to Android’s popularity amongst developers due to the open-source nature of Android, which offers the capability of developing and programming rich applications at the lowest level of Android’s operating system. Since its initial release in 2008, Android has undergone many releases, the last being Android 2.2; this latest version of the Android platform brings many new and existing features and technologies to make both users and developers productive. Some of the new services and applications included in the new version aim at increasing speed (CPU is about 2-5 times faster), performance, and browsing (using version 8 engine that provides 2-3 times faster java script heavy page load). This new version also offers improved security features by allowing users to unlock their device using a password policy and the ability to wipe data from devices in case of theft or loss.
The Android Security Model

Android is a multi-process system where each application (and parts of the system) runs its own process. The standard Linux facilities enforce security between applications and the system at the process level; those applications are assigned by users and group IDs. Applications are restricted in what they can perform by a permission mechanism, called permission labels, that uses an access control to control what applications can be performed. This permission mechanism is fine-grained in that it even controls what operations a particular process can perform (Shabtai et al., 2010). The permission labels are part of a security policy that is used to restrict access to each component within an application. Android uses security policies to determine whether to grant or deny permissions to applications installed on Android OS.

Those security policies suffer from shortcomings in that they cannot specify to which application rights or permissions are given because they rely on users and the operating system to make that guess. They are therefore taking the risk of permitting applications with malicious intentions to access confidential data on the phone. Ongtang, McLaughlin, Enck, and McDaniel (2009) best described this security shortcoming by their hypothetical example of “PayPal service built on Android. Applications such as browsers, email clients, software marketplaces, music players, etc. use the PayPal service to purchase goods. The PayPal service in this case is an application that asserts permissions that must be granted to the other applications that use its interfaces” (Ontang, McLaughlin, Enck, & McDaniel, 2009). In this hypothetical scenario, it is unknown whether the PayPal application is legitimate or not because there is no way to determine whether this is the actual PayPal service application or another malicious program. Again, Android lacks security measures to determine and enforce how, when, where, and to whom permissions are granted.

Android’s Permissions

Android uses permission mechanisms to determine what users are allowed to do in applications; this is achieved via the manifest permission that grants permissions to applications independently, which in turn, allows applications to run independently from each other as well as from the operating system. This could be a good security feature since the operations run by one application cannot interfere or otherwise impact operations within other applications. For example, users sending email messages will not be allowed (by default) to perform any operation within an application (such as reading a file from another application) that could adversely impact the email application (Developers, n.d). Applications achieve that using the “sandbox” concept, where each application is given the basic functions needed to run its own process; however, if the sandbox does not provide the needed functions to run a process, then the application can interfere with the operations of another process and request the needed functions to run a process. This capability of allowing applications to request permissions outside of their sandbox capabilities could be harmful to Android mobile devices because it opens a window of opportunity for malware to exploit the privilege of accessing sensitive data on Android handsets and thus install malicious software (Vennon, 2010).
METHODOLOGY

This is a conceptual paper; thus the main scope of this paper is to illustrate the importance of security software for smartphone operating systems. Case studies in scholarly journals and reports were used in the construction of this paper. Most sources contain qualitative information, describing predictions of various cyber attacks on mobile devices that may occur by the end of 2012. Quantitative methods were also used to assess the statistical increase in cyber attacks.

RESEARCH RESULTS

The current smartphone statistics are quite daunting due to the widespread lack of security software for mobile devices. The result of this void in security software is vulnerable mobile devices and tablets that are easily susceptible to cyber attacks. According to Andy Favell, editor of the website “MobiThinking,” in 2010, 96% of mobile devices and tablets do not contain security software (Favell, 2011). Moreover, the article states that over 2000 various types of mobile malware have been identified in the past two years (Favell, 2011). For example, Hydraq and Stuxnet, specific cyber attacks, “leveraged zero-day vulnerabilities to break into computer systems... Stuxnet alone exploited four different zero-day vulnerabilities to attack its targets” (Symantec, Inc., 2011). Moreover, many enterprises experienced a multitude of targeted attacks against their collection of corporate data in 2010 (Symantec, Inc., 2011).

Figure 1 depicts the current status of security for the majority of today’s mobile devices. This is an alarming statistic because, as mentioned earlier, mobile devices are the most popular way to communicate in our society. Malware is increasing at an exponential rate, and consumers’ nonchalant attitudes towards mobile security provide the perfect opportunity for cyber attackers to create and spread malware quickly. This breach in cyber security puts businesses at risk also. According to Favell, when consumers use smart devices for work purposes, the devices can access and/or store company emails and sensitive information (2011). This scenario is detrimental to the success and welfare of any company; hopefully, the fact that in 2010 only 4% of all mobile devices contained security software will alert consumers and businesses of the importance of having a secured smart device (Favell, 2011).

Figure 1. The current status of security for the majority of today’s mobile devices
Mobile Devices: The Case for Cyber Security Hardened Systems

Table 1 illustrates the various malware programs that now infect mobile devices. Originally, trojans, viruses, botnets and toolkits were common infections of personal computers; now, mobile devices are plagued with these various malware programs. In 2010, Favell stated that 2,500 different mobile malware programs exist (Favell, 2011). The majority of existing malware programs target Android apps because Android is the most popular OS, and it is easier for app developers to distribute apps through GooglePlay (Android’s App Market) due to Android’s lenient verification process (Favell, 2011). In 2009, iPhoneOS.Ikee.B and iPhoneOS.Ikee infected “jailbroken” Apple devices. “Jailbreaking” means to remove Apple’s restrictions; this grants the user freedom to use the phone as he/she pleases (Favell, 2011). Now, consumers must be aware of the various malware programs that are prevalent; consumers must also be vigilant to protect their data while using their device.

<table>
<thead>
<tr>
<th>Type</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan</td>
<td>Programs that pose as legitimate applications (Symantec, Inc., 2011).</td>
<td>Android.Pjapps Trojan, Rogue apps, Hydraq</td>
</tr>
<tr>
<td>Virus</td>
<td>Software program that can replicate itself and damage files and other programs on host computer.</td>
<td>Stuxnet</td>
</tr>
<tr>
<td>Botnet</td>
<td>A network of infected private computers controlled by cyber attackers who sell sensitive data to the highest bidder. Social media applications on mobile devices are now a new avenue for botnets to control devices (Trend Micro, 2009).</td>
<td>Opt-in botnets, Aurora botnet, Rustock</td>
</tr>
<tr>
<td>Toolkit</td>
<td>Software programs that can be used to assist with the launch of widespread attacks on networked computers or mobile devices; exploits Java vulnerabilities (Symantec, Inc., 2011).</td>
<td>Phoenix toolkit</td>
</tr>
<tr>
<td>Malvertising</td>
<td>Authentic looking advertisements that are linked to false sites (Rao, 2011).</td>
<td>Malicious Ad on social network apps, such as TweetMeme</td>
</tr>
<tr>
<td>Worms</td>
<td>Malware programs that self-replicate and is spread over the air (via mobile networks) (Favell, 2011).</td>
<td>iPhoneOS.Ikee.B; iPhoneOS.Ikee</td>
</tr>
</tbody>
</table>

Table 1 illustrates the various malware programs that now infect mobile devices. Originally, trojans, viruses, botnets and toolkits were common infections of personal computers; now, mobile devices are plagued with these various malware programs. In 2010, Favell stated that 2,500 different mobile malware programs exist (Favell, 2011). The majority of existing malware programs target Android apps because Android is the most popular OS, and it is easier for app developers to distribute apps through GooglePlay (Android’s App Market) due to Android’s lenient verification process (Favell, 2011). In 2009, iPhoneOS.Ikee.B and iPhoneOS.Ikee infected “jailbroken” Apple devices. “Jailbreaking” means to remove Apple’s restrictions; this grants the user freedom to use the phone as he/she pleases (Favell, 2011). Now, consumers must be aware of the various malware programs that are prevalent; consumers must also be vigilant to protect their data while using their device.

Figure 2. Illustrates various cyber threats in 2010
(Symantec, 2011).
Cyber threats are increasing at an alarming rate. According to Symantec, polymorphisms and toolkits have contributed to the increase in malware programs in 2010. Also, over 200 million malicious programs were created during 2010 (Symantec, Inc., 2011). Moreover, cyber criminals are exploiting the gaps in security with the Android OS. In fact, many zero-day exploits have increased since the inception of the Android Market. Unfortunately, with zero-day vulnerabilities, the attack happens the same day; hence, IT specialists cannot distribute software updates in a timely manner to block such attacks (Symantec, Inc., 2011). Other harmful malware programs, botnets, have wreak havoc on many smartphone OS. The botnet, Rustock, controlled over a million bots at one point in 2010; Grum and Cutwail, other botnet attacks, controlled hundreds of thousands bots (Symantec, Inc., 2011). Lastly, cyber threats that steal bank and credit card information has greatly increased in the past four years. Symantec’s Internet Security Threat Report states that black market forums pay top dollars for personal credit card data. The majority of this information is stolen through extensive botnet attacks (2011). Above is a numerical depiction of the increase in mobile cyber attacks in one year. From 2009 to 2010 there was a 42% increase in the number of mobile vulnerabilities (Symantec, Inc., 2011). Cyber criminals are capitalizing on the popularity of mobile devices; thus, this trend is an indication that will not falter without an intervention. Furthermore, most reported mobile vulnerabilities occurred in the form of Trojan Horse programs that acted as legitimate applications (Symantec, Inc., 2011). While many cyber attackers created some of the most pertinent malware from scratch, “in many cases, they [cyber attackers] infected users by inserting malicious logic into existing legitimate applications” (Symantec, Inc., 2011). Next, the hacker will distribute these malicious apps through public app stores, such as Google Play or Apple’s App Store. Pjapps Trojan is a recent example of a malicious app distributed through public app stores (Symantec, Inc., 2011).

Trend Micro, an international leader in data security, surveyed 1,000 smartphone and iPhone owners that were over the age of 18. The data revealed that nearly half (56 percent) of the respondents believe it is safe, if not safer, to browse the Internet from their mobile device as opposed to a PC (Trend Micro, 2009). Contrasting with this, 44 percent of respondents do not feel it is safe to surf the web using a mobile device.
Mobile Devices: The Case for Cyber Security Hardened Systems

Figure 4. Percentage of smartphone users that perceive it is safer to surf the Internet via mobile browser (Smartphone Users, 2009).

Smartphone Users
Opinion on
Cybersecurity in 2009

smartphone (Trend Micro, 2009). Moreover, according to the survey, only 23% of the respondents use security software that is installed on their smartphone (Trend Micro, 2009). In addition to this, another 20% of respondents “don’t think installing security software program[s] on their phones would be very effective (Trend Micro, 2009).” The same respondents feel that there is limited risk when using a mobile web browser. As stated earlier, this false mentality of a safe mobile browser environment has created many opportunities for cyber criminals to steal personal data. Contrasting with this, the majority of the survey respondents are aware of mobile Web threats, and nearly half of them have been infected by some form of malware (Trend Micro, 2009).

Spam emails are another prevalent form of cyber threats. As illustrated in Figure 5, out of the 1,000 respondents, 450 (45%) of them received spam emails in the past 3 months (Trend Micro, 2009). 170 (17%) respondents believe there is an increase in the amount of spam emails they have received (Trend Micro, 2009). 500 (50%) of respondents open email attachments on their smartphone; and 390 (39%) respondents click on URL links in emails they received on their phone (Trend Micro, 2009). These statistics can be projected onto the general smartphone user community. In fact, it can be assumed that nearly half of all smartphone users receive spam emails quite often throughout the year, and half of all smartphone users carelessly open email attachments on their phone. Since spam has become a common nuisance in the email environment; it is obvious it would be a nuisance for mobile devices.

Thus, the lack of installed security software coupled with the laissez-faire attitude of today’s smartphone users, leads to advantageous loopholes for malicious cyber attackers. 20% of smartphone users do not think installing security software to their phone will reduce their chances of malware attacks (Trend Micro, 2009). Another 20% of users have encountered phishing scams when surfing the internet on their mobile browser (Trend Micro, 2009). Phishing scams lure users into supplying ID information, bank account numbers, usernames and passwords by replying to false email messages (Trend Micro, 2009). Lastly, Apple aficionados must take necessary precautions when using the Safari web browser on their iPhone. Apple’s claim to fame is their stylish hardware, iOS Operating System (OS) and sleek

Figure 4. Percentage of smartphone users that perceive it is safer to surf the Internet via mobile browser (Smartphone Users, 2009).
functionality. Unfortunately, the traits that make Apple popular are also the same traits that make the iPhone susceptible to cyber attacks (Trend Micro, 2009). A recent example of this is seen in a reported SMS vulnerability for the iPhone, in which hackers have the ability to control the device if the user is on a malicious site or connecting to the internet through unsecured 3G or Wifi connections (Trend Micro, 2009).

ANALYSIS AND DISCUSSION

Various security services project that cyber attacks on mobile devices will increase exponentially by 2015. This is obvious based on the fact that the majority of mobile devices have no security software at all. Lookout Mobile Security company analyzed the current data on smartphone cyber attacks and released their malware predictions for 2011 (Rao, 2011). Lookout offers various security services for many smartphone operating systems, such as Android, Windows Mobile, Blackberry and iOS (Rao, 2011). Unfortunately, Android users, internationally, had a 36% chance of clicking an unsafe link in 2011 (Rao, 2011).

Lookout also identified the first U.S. mobile malware that steals money from Android smartphone users – GGTracker; and RuFraud, which steals money from Eastern European Android smartphone users (Rao, 2011). Lookout believes that malware creators will furtively combine thousands of mobile devices into extensive botnet-like networks, such as DroidDream, to spread spam, steal personal data and install more malware (Rao, 2011). Moreover, Lookout has predicted the likelihood that smartphone users will click on unsafe links (Rao, 2011). They predict the increase in “malvertising” – malware advertising, advertisements that link back to counterfeit websites – will continue to increase by the end of this year.
Predictions of the Mobile Security Market

Consistent with this, Canalys, an IT research company that specializes in “mobility services, data centers, networking, security, unified communications, client PC markets and go-to strategies,” did more research on mobile security. From a business perspective, they predict that mobile security investment will increase by 44% each year to 2015 (Canalys, 2011). They expect the mobile security market to become a $3 billion investment opportunity in 2015. Fortunately, by 2015, Canalys believes that 20% of smart phones and tablets will have mobile security software installed (Canalys, 2011). Canalys also states that device management will drive the incorporation of security-related products (secured-approved mobile devices) in the business sector (Canalys, 2011). For example, it is projected that corporate device management will increase implementation of security-related products. Businesses will use solutions “to track, monitor and authorize corporate data access, as consumers bring their devices into the workplace” (Canalys, 2011). Canalys recommends that it is advantageous for businesses to link the solutions to “enterprise app stores” so that only “approved apps” can be downloaded and mobile devices with corporate-approved apps installed will have the ability to access corporate data (Canalys, 2011). Lastly, Canalys experts predict mobile client security to increase by 54.6% every year until 2015 (Canalys, 2011). Mobile client security includes: anti-virus, firewall, messaging security (due to SMS texting capabilities), web threat security, VPN functionality and encryption (Canalys, 2011).

Presently, the U.S. and Canada are the leaders of mobile security implementation due to their need to adhere with data compliance policies (Canalys, 2011). Nevertheless, the Western European market is expected to grow as globalization, “enterprise mobility and consumerization trends” increase (Canalys, 2011). From 2013 to 2015, mobile security investment will sharply increase in developing countries such as Latin America, Asia, Africa and the Middle East, due to the instant popularity of the price-sensitive operating system, Android (Canalys, 2011). Unfortunately, as the steady growth of Android OS increases so does the volume of mobile malware threats because more consumers can download compromised applications (Canalys, 2011).

Corporations, Cyber Security, and Mobile Devices

Currently, corporations around the world are trying to manage a growing mobile workforce, in which employees are using multiple devices and operating systems (Canalys, 2011). This increase in data consumption exponentially increases the amount of vectors open to cyber attacks and leaves corporate data more vulnerable due to tangible loss of devices (Canalys, 2011). Ultimately, to counteract the era of cyber crimes, enterprises must have a holistic approach to mobile security – every layer of security must be analyzed in order to protect sensitive data. Lastly, Canalys urges service providers to provide security from a “network perspective, regardless of device or operating system type” (Canalys, 2011). Protecting the network of service providers is a key element in providing top notch security for the plethora of mobile devices that are currently on the market.

LIMITATIONS

It is a daunting task to establish a national cyber security standard to counteract the multitude of cyber attacks that exist today. There are quite a few limitations that must be addressed in order to move forward.
Legitimate Applications that Can Be Used to Retrieve Information

Presently, there is valid spy software available for various mobile devices. An example of this is FlexiSpy, a legitimate commercial spyware program that cost over $300 (United States Computer Emergency Readiness Team, 2010). FlexiSpy can:

- Listen to actual phone calls as they happen;
- Secretly read Short Message Service (SMS) texts, call logs, and emails;
- Listen to the phone surroundings (use as remote bugging device);
- View phone GPS location;
- Forward all email events to another inbox;
- Remotely control all phone functions via SMS;
- Accept or reject communication based on predetermined lists; and
- Evade detection during operation (United States Computer Emergency Readiness Team, 2010).

The creators of FlexiSpy claim that this application can help protect young children (that have a cell phone) or catch unfaithful spouses. However, the dangers of this software outweigh the positives once it is in the hands of a malicious cyber attacker. This example demonstrates the need for a federal implemented cyber security act to dictate the types of applications that can be available to the general public. For parents, FlexiSpy has wonderful attributes in terms of monitoring the whereabouts of underage children, but these same attributes can be abused by a cyber attacker to gain extremely personal data of a smartphone user.

Another example of a legitimate application that can be exploited by malicious cyber hackers is mobile e-commerce apps (M-commerce). M-commerce involves using a mobile device “to research product information, compare prices, make purchases, and communicate with customer support” (United States Computer Emergency Readiness Team, 2010). In addition to this, merchants can use mobile devices for checking prices, inquiring inventory and processing payments (United States Computer Emergency Readiness Team, 2010). Currently, vendors now have the ability to process credit card payments with a new device called “Square” (United States Computer Emergency Readiness Team, 2010). Square is a third-party smartphone attachment that is plugged into a smartphone’s headphone jack and is used for swiping credit cards (United States Computer Emergency Readiness Team, 2010). Square subscribers register their device online through the company’s website. This way, subscribers can manage their payment processes through their accounts. Unfortunately, Square can be used for malicious cyber activities, such as “skimming” and “carding” (United States Computer Emergency Readiness Team, 2010). According to the article entitled, “Cyber Threats to Mobile Devices,” “Skimming is the theft of credit card information using card readers, or skimmers, to record and store victims’ data” (2010). Also, carding is a process used to assess “the validity of stolen credit card numbers” (United States Computer Emergency Readiness Team, 2010). Both processes can be done in conjunction with other legitimate transactions, and can be exploited by cyber attackers to gain sensitive financial data.

A third example of a legitimate application that can be used for malicious activity are advertisement libraries, or ad libraries (Grace, Zhou, Jiang, & Sadeghi, 2012). Many app developers incorporate ad libraries into their legitimate applications for monetary compensation. For example, on the Android Market (now known as Google Play), over 60% of the apps are free to download (Grace, Zhou, Jiang, & Sadeghi, 2012). In order for app developers to be compensated for their product, they use ad libraries,
which “communicate[s] with the ad network’s servers to request ads for display and might additionally send analytics information about the users of the app” (Grace, Zhou, Jiang, & Sadeghi, 2012). Next, the ad network pays the app developer continuously, based on data that measure “how much exposure each individual app gives to the network and its advertisers” (Grace, Zhou, Jiang, & Sadeghi, 2012). Unfortunately, the Computer Science Department of North Carolina State University revealed that there are many privacy and security issues in some of the most prevalent ad libraries. Granted some of these ad libraries collect information for legitimate purposes, such as a user’s location for targeted advertising, a few ad libraries collect personal, sensitive data, such as a user’s call logs, account information or cell number (Grace, Zhou, Jiang, & Sadeghi, 2012). Consequently, malicious cyber attackers can use this information to infer the actual identity of the user, and enable greater comprehensive tracking of the user’s habits (Grace, Zhou, Jiang, & Sadeghi, 2012). A specific example of an ad library embedded into a popular smartphone app is the game Angry Birds, created by Rovio. The company Rovio employed the services from a third-party advertising network to capitalize Angry Birds on the Android Market (Grace, Zhou, Jiang, & Sadeghi, 2012). AdMob is the most popular ad library used by Angry Birds; it sends user’s information such as game scores to Google (Grace, Zhou, Jiang, & Sadeghi, 2012). This business arrangement is not uncommon for smartphone app developers. Unfortunately, ad libraries in legitimate applications can be loopholes for cyber attackers to exploit and abuse personal user information. One study discovered that some ad libraries “download additional code at runtime from remote servers and execute it in the context of running the app” (Grace, Zhou, Jiang, & Sadeghi, 2012). It is evident that these results garner the need for additional methods for regulating the behavior of ad libraries on Android apps.

When discussing legitimate applications we should also not forget how easy it is to create malware applications. With the aid of rootkit tools, and freely available malicious code it is easy to create a malware program. Figure 6 displays a simple script that can email as an executable file that will delete targeted files that are necessary for the OS to function. This script took less than four minutes to create.

Figure 6. Example of an executable file
Malware Social Network Exploitation

As stated earlier, the popularity of social networking applications can be a limitation in the fight against cyber threats. The wealth of personal data that social media applications inspire cybercriminals to create malware targeted for these applications. Twitter and Facebook are the main sources of communication and information for today’s generation of smartphone users. Unfortunately, accepting shared information on these websites can compromise the security of a user’s device. This issue is heightened on Twitter because users are limited to 140 characters when sharing updates or links. So on Twitter, Uniform Resource Locators, or URLs, are shortened severely in order to adhere to the 140 character rule. This is unfortunate because shortened URLs make it more difficult for a user to know if the link is legitimate or malicious. In brief, sharing links via Twitter is an opportunistic way for cyber attackers to lure innocent users into clicking fraudulent links.

Android Malware

Hackers first started to design malware for mobile devices in early 2004 when the Cabir worm came to the scene. Despite the fact that Cabir was only a “proof of concept” attack form and did not cause any serious damage to affected mobile devices, it brought hackers’ attention to mobile devices. Android, as a smartphone, is no exception when it comes to mobile malware attacks. Some of the first Android malware was devised by a group of security researchers as an attempt to bring attention to possible malware attacks on the Android platform because Android offers an integrated set of services and functionalities, such as internet access. The researchers were able to create the first Android running malware by exploiting undocumented Android Java functions and using them to create native Linux applications. Specifically, this malware was embodied in a valid, benign, Android application that a user would install. Once the benign application is installed, the malware would propagate the Linux system and execute its malicious payload, thereby wreaking havoc on Android devices. This was an indication of the possible vulnerabilities and risks associated with Android devices (Schmidt, Bye, Clausen et al., 2009).

The most dangerous Android malware is the one that exploits security flaws within the operating system (Linux) to gain root-level access with root privilege. One of the first security flaws was discovered in Android in November of 2008 when security experts found a bug that would allow users and potential attackers to run command-line instructions with root privilege; moreover, the bug, if exploited, would make the Android platform read and interpret actions based on the input text. For example, if an Android user input a simple text message, such as “Hello,” it could be interpreted by the operating system as “reboot,” which surprisingly reboots the Android device (ZDNet, 2010). This security shortcoming and many other vulnerabilities were discovered in Android over the last two years and have thus continuously raised pressing concerns about the credibility and effectiveness of security controls deployed in Android. Most of those vulnerabilities stem from Android’s open-source nature, which allows development of third-party applications without any kind of centralized control or any security oversight.

As a case in point, we can highlight malware risks targeting Android smartphone users. Android smartphone users tend to download and install apps frequently, as all kinds of apps dominate the marketplace; apps usually require access to certain areas of the phone to function, and they ask users to grant permissions at installation time. Many apps tend to request permissions more than they really need to be fully functional. Also, many apps are seemingly benign to users and do not seem to pose any threats to confidential information. Therefore, Android users normally get distracted by enjoying all the features and added functionality offered by apps and do not give adequate attention to the security aspects of those
Incorporating Pre-Existing Government Guidance

The Department of Defense (DoD) has addressed software security through governance issued under the Office of Management and Budget (OMB) Circular A-130. The focus of Information Technology security was further derived by DoD Directive 8500.2. It specifically states that all Information Assurance (IA) and IA-enabled IT products incorporated into DoD Information Systems (IS) shall be configured in accordance with DoD-approved security configuration guidelines. On April 26, 2010, the DoD released the third version of the Application Security and Development Security Technical Implementation Guide (STIG) provided by the Defense Information Systems Agency (DISA). This document provides DoD guidelines and requirements for integrating security throughout the software development lifecycle. The STIGs are accompanied by the NSA Guides which provide the configuration guidance for locking down a system. There are guides for multiple Oss to include those for mobile platforms.

In terms of development for mobile devices the commercial sector should employ those who have professional certifications such as International Information Systems Security Certification Consortium (ISC)2 Certified Secure Software Lifecycle Professional (CSSLP). The guidance that drives this requirement and those similar is the DOD 5870.01M Information Assurance Workforce Improvement Program. Organizations employing IA technically competent software developers should help mitigate the overall risk. This could be a requirement that could be levied not just upon the mobile phone developer but also the application developer.

The Common Criteria (CC), an internationally approved set of security standards, provides a clear and reliable evaluation of the security capabilities of Information Technology (IT) products (CCEVS, 2008). By providing an independent assessment of a product’s ability to meet security standards, the CC gives customers more confidence in the security of products and leads to more informed decisions (CCEVS, 2008). Security-conscious customers, such as the U.S. Federal Government, are increasingly requiring CC certification as a determining factor in purchasing decisions (CCEVS, 2008). Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings. The international scope of the CC, currently adopted by fourteen nations, allows users from other countries to purchase IT products with the same level of confidence, since certification is recognized across all complying nations. Evaluating a product with respect to security requires identification of the customer’s security needs and an assessment of the capabilities of the product. The CC aids customers in both of these processes through two key components: protection profiles and evaluation assurance levels (CCEVS, 2008). Utilizing guidance such as the CC could allow organizations to appropriately measure the security of their product. The problem is the cost that surrounds commercial companies meeting rigorous standards but this product certification process could replicated at a more cost efficient manner.
Lastly, another limitation for creating a cyber security environment for mobile devices is due in part to a lack of national cyber security policies. The internet is a brand new frontier with no physical or political boundaries (Brechbuhl, Bruce, Dynes, & Johnson, 2010). Furthermore, cyber security is a concern of everybody – common smartphone users, business and government officials; also, security issues have normally been the government’s responsibility. Contrasting with this, the sectors that are best equipped at dealing with cyber security issues is private or semiprivate enterprises that operate the information and communication technology (ICT) infrastructure, in other words the internet (Brechbuhl, Bruce, Dynes, & Johnson, 2010). Finally, the creation of a national policy is difficult because we currently “lack a feasible policy framework that systematically arrays the issues and specifies parameters that constrain this development” (Harknett & Stever, 2011). Ultimately, cyber security threats are versatile and constantly changing, we must develop programs to match and counteract the transient attributes of cyber security attacks.

**Issues with Android Phones and Other Mobile Devices**

Smartphones are becoming a more integrated and prevalent part of people’s daily lives due to their highly powerful computational capabilities, such as email applications, online banking, online shopping, and bill paying. With this fast adoption of smartphones, imminent security threats arise while communicating sensitive personally identifiable information (PII), such as bank account numbers and credit card numbers used when handling and performing those advanced tasks (Wong, 2005; Brown, 2009). Traditional attacks (worms, viruses, and Trojan horses) caused privacy violations and disruptions of critical software applications (e.g., deleting lists of contact numbers and personal data). Malware attacks on smartphones were generally “proof of concept” attempts to break through the phone’s system and cause damage (Omar & Dawson, 2013). However, the new generation of smartphone malware attacks has increased in sophistication and is designed to cause severe financial losses (caused by identity theft) and disruption of critical software applications (Bose, 2008). Because smartphones are becoming more diverse in providing general purpose services (i.e., instant messaging and music), the effect of malware could be extended to include draining batteries, incurring additional charges, and bringing down network capabilities and services (Xie, Zhang, Chaugule, Jaeger, & Zhu, 2009).

Smartphones are rapidly becoming enriched with confidential and sensitive personal information, such as bank account information and credit card numbers, because of the functionality and powerful computational capabilities built into those mobile devices. Cyber criminals, in turn, launch attacks especially designed to target smartphones, exploiting vulnerabilities and deficiencies in current defense strategies built into smartphones’ operating systems. Bhattacharya (2008) indicated that because of skill and resource constraints, businesses are ill-prepared to combat emerging cyber threats; this claim is true for smartphones as well, given the fact that those mobile devices are even less equipped with necessary protections, such as antivirus and malware protection software. Some services and features, such as Bluetooth and SMS, create attack vectors unique to smartphones and thus expand the attack surface. For example, in December, 2004, A Trojan horse was disguised in a video game and was intended to be a “proof of concept,” which signaled the risks associated with smartphones that could potentially compromise the integrity and confidentiality of personal information contained in smartphones (Rash, 2004). Attackers can easily take advantage of those services provided by smartphones and subvert their primary purpose because they can use Bluetooth and SMS services to launch attacks by installing software that can disable virus protection and spread via Bluetooth unbeknownst to smartphone users.
With the development of innovative features and services for smartphones, security measures deployed are currently not commensurate because those services and features, such as MMS and Bluetooth, are driven by market and user demands, meaning that companies are more inclined to provide more entertainment features than security solutions. In turn, this further increases vulnerabilities and opens doors for hackers to deploy attacks on smartphones. Furthermore, Mulliner & Miller (2009) argue that the operating systems of smartphones allow the installation of third-party software applications, coupled with the increase in processing power as well as the storage capacity. Scenarios like this pose worse security challenges because hackers could exploit those vulnerabilities, which are further compounded by users’ lack of security awareness. Smartphone attackers are becoming more adept in designing and launching attacks by applying attack techniques already implemented on desktop and laptop computers; smartphones’ enhanced features, such as music players and video games, produce easy-to-exploit targets by sending seemingly benign files via music or video game applications to users and luring them into downloading such files. Becher, Freiling, and Leider (2007) indicated that attackers could exploit such vulnerabilities to spread worms autonomously into smartphones. Therefore, hackers usually use a combination of technical expertise along with some social engineering techniques to trap users into accepting and downloading benign applications, which are used later to execute malicious code and affect critical applications running on smartphones.

**Attack Vectors and Infection Mechanisms**

- **Bluetooth:** This is a wireless communication protocol used for short-range (about 10 meters) transmissions at 2.4 G.H. Bluetooth is one of the most widely used and preferred attack techniques for infecting smartphones because by pairing Bluetooth-enabled devices, hackers are able to access infected phones’ critical applications and files, such as email, contact lists, pictures, and any other private data stored in the smartphone. Bluetooth-enabled smartphones are prone to various kinds of attacks due to security implementation flaws that exist in current security specifications. For example, Wong (2005) reveals that when two Bluetooth-enabled devices communicate after establishing a trusted relationship, all the credential information is left on both devices, even after the session is ended. This implementation hole allows potential hackers to have full access to the device, without the owner’s knowledge or consent, based on the previously established trust relationship; attackers then can access confidential data stored on smartphones and manipulate it. The only way smartphone users would be able to detect such security flaws is to observe the Bluetooth icon indicating an established Bluetooth connection; otherwise, attackers will have unauthorized access to the victim’s smartphone. This security shortcoming, along with other security flaws found in Bluetooth security architecture, such as device-based authentication rather than user-based authentication, make smartphones vulnerable to direct attacks and threaten privacy and critical personal information.

- **MMS/SMS:** Multimedia message service and short message service are both communication protocols that have become widely used and adopted by smartphone users as the standard for fast and convenient communications. Although it might seem unrealistic to think that hackers would ever be interested in targeting MMS/SMS, recent studies have shown that MMS/SMS can contain confidential information that is exposed to attacks due to lack of security services not provided by the cellular network. SMS suffers from exploitable vulnerabilities, such as lack of mutual authentication methods and non-repudiation. An SMS that is sent from a sender to a receiver cannot be
Mobile Devices: The Case for Cyber Security Hardened Systems

mutually authenticated by both parties, which opens doors for hackers to exploit. Also, senders who send SMS cannot be held accountable for their sent SMS because there is no mechanism that could be implemented to ensure the sender’s true identity. The weak security implementation of SMS can also be used as attack mechanisms by hackers, where an arbitrary computer can be used to inject SMSs into the network, thus exposing smartphones to risks. In addition, SMSs are susceptible to man-in-the-middle attacks while they are being transmitted over the air. Therefore, attackers are increasingly relying on MMS/SMS as an effective attack vector (Lockefer, 2010).

File Injection and Downloadable Applications: Malware authors constantly develop new and innovative ways for attacking smartphones; sending benign files that contain malicious code and downloadable applications have proven to be a successful attack mechanism adopted by hackers. What makes such attack vectors effective is the fact that they come in the form of legitimate applications, luring smartphone users to disclose their private and financial information. For instance, in January, 2010, a group of malicious writers calling themselves “09Droid” developed an application that specifically targeted Google Android phones and mobile banking institutions. The application contained the phrase “happy banking” on the summary statement that each application uses to advertise itself to potential users. The attack tempted users to purchase the mobile banking application from the Android Market in order to log on to their mobile banking accounts. While doing so, users would have to reveal their account numbers and passwords, which would then be sent to the authors of the malicious program (Morrison, 2010). This kind of well-crafted attack underscores the powerful capabilities of emerging attacks and the attackers; they target banking institutions and credit unions and use their logos to lure naive smartphone owners into giving their confidential information to applications that look exactly the same as the legitimate ones.

CONCLUSION AND SUGGESTIONS

Fortunately, there are possible solutions to the rampant cyber security problem with mobile devices. Once our society acknowledges that cyber security threats are detrimental not only to one smartphone user, but to the society as a whole; then the inception of a solution can begin. The value of data is steadily increasing, possibly even more so than actual money. It is imperative to establish a culture of cyber security because this issue is multifaceted and technology is constantly evolving.

Cyber Security Is Multidimensional: Collaboration Is Imperative for Its Success

Security concerns are not exclusive to “economists, political scientist, lawyers, business policy or management experts, or computer specialist” (Brechbuhl, Bruce, Dynes, & Johnson, 2010). In order to establish a policy of cyber security, it will take a collaborative effort from a variety of officials in various disciplines in society. Each official brings a specific set of knowledge to the issue of cyber security, and has a potential role in establishing the different set of functions that are needed to create a general intra-and international cyber security standard (Brechbuhl, Bruce, Dynes, & Johnson, 2010). Ultimately, a decentralized approach is the best way to make cyber security an interconnected, coordinating mechanism that benefits the society as a whole (Brechbuhl, Bruce, Dynes, & Johnson, 2010).
Cell Phone Attributes as Security Features

CTO Dan Schutzer of BITS, the technology policy division of the Financial Services Roundtable, states that mobile devices and other mobile devices are equipped with biometric security measures (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). Biometric is the statistical analysis of biological data using technology. Schutzer suggests that the cameras that are installed in mobile phones can be used for facial recognition or iris detection (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is actually a great idea because, thanks to DNA, biologically everyone is different. Thus, the authenticated user of a smartphone will be the only person that can unlock his/her phone. Moreover, Shutzer proposes that the microphones installed in mobile devices can be used for voice recognition (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is another way to secure and lock a cell phone; and only the authorized user of the phone will be able to unlock the device. In brief, using biometric measures to secure mobile devices is one way to prevent theft.

CONCLUSION

Lastly, IT companies are seeing the niche in the market for security software specifically designed for mobile operating systems. Recently, a few companies have presented different mobile security software that consumers can purchase. Bullguard Mobile Security, Kaspersky Mobile Security, ESET Mobile Security, and Lookout Premium are mobile security software currently available for purchase (2012 Best Mobile Security Software Comparisons and Reviews, 2012). The programs range in prices from $19.99 to $39.99. These programs are a start; however, it is up to consumers to purchase them to secure their data. As mentioned earlier, cyber security is a multifaceted issue that must be dealt with accordingly. Ultimately, creating a national standard of cyber security is the best way to counteract the increase in cyber attacks.

REFERENCES


KEY TERMS AND DEFINITIONS

**Authentication**: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information (Harris, 2002).

**Availability**: Timely, reliable access to data and information services for authorized users (Harris, 2002).

**Confidentiality**: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (Harris, 2002).

**Cyber Terrorism**: Attacks with the use of the Internet for terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, worms, Trojans, and zombies (Janczewski & Colarik, 2008).

**Integrity**: Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Harris, 2002).

**MMS/SMS**: Multimedia message service and short message service are both communication protocols that have become widely used and adopted by smartphone users as the standard for fast and convenient communications.

**Non-Repudiation**: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data (Harris, 2002).

**Rootkit**: Malicious software designed to hide the existence of programs or processes from the normal methods of detection and enable privileged access to a computer.

**Trojan**: Malicious non-self-replicating malware program when executed carries out actions determined by the developer of the program. Trojans act as an backdoor providing unauthorized access to the infected computer.