Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.13, No.1, 2023

A Policy Analysis of Cybersecurity and Mobile Applications: Implications on the Media Space

Olumide Akinsanmi
Department of Computer Science, College of Sciences and Engineering
Southern University and A&M College, Baton Rouge, Louisiana

Abstract
This study presents discussion for several examples that illustrates the importance of having a security policy for mobile phones. The study further examines the importance of developing a national security policy created for mobile devices in order to protect sensitive, and personal data to safeguard the media space. By inspection, it was observed from the literature that smartphones are becoming a vehicle 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 smartphones do not have pre-installed security software. This lack in security is an opportunity for malicious cyber attackers to hack into the various devices that are popular (i.e. Android, iPhone and Blackberry). Traditional security software found in personal computers (PCs), such as firewalls, antivirus, and encryption, is not currently available in smartphones. Moreover, smartphones are even more vulnerable than personal computers because more people are using smartphones to do personal tasks. Nowadays, smartphone users can email, use social networking applications (Facebook and Twitter), buy and download various applications and shop. Furthermore, users can now conduct monetary transactions, such as buying goods, redeeming coupons and tickets, banking and processing point-of-sale payments. Monetary transactions are especially attractive to cyber attackers because they can gain access to bank account information after hacking a user's smartphone. Lastly, smartphones are small and are easy to carry anywhere. Unfortunately, the convenience of using smartphones to do personal task is the loophole cyber attackers need to gain access to personal data.
Keywords: Smartphones, Social Media, Cybersecurity, Computers, E-commerce, Operating Systems, Internets, Browsers
DOI: 10.7176/ISDE/13-1-04
Publication date: March 31st 2023

INTRODUCTION

Currently, smartphones are the preferred device for web browsing, emailing, using social media and making purchases. Due to their size, smartphones are easily carried in people's pockets, purses or briefcases (Ruggiero, 2011). Some specific examples of smartphones, according to Poushter, Caldwell, and Chwe (2018) include the following: iPhone, Android, Blackberry, Windows phone, Samsung Galaxy, etc. iPhone, Android, Blackberry, Windows phone, Samsung Galaxy, Nokia E5, Venus and Huawei (see Figure 1 for more details)**.** Unfortunately, the popularity of smartphones is a breeding ground for cyber attackers. Operating systems on smartphones do not contain security software to protect data. For example, traditional security software found in personal computers (PCs), such as firewalls, antivirus, and encryption, is not currently available in smartphones (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, 201 1).

Figure 1: A Picture of Smartphones
Source: Author's modification

DISCUSSION OF SOME SPECIFIC EXAMPLES THAT ILLUSTRATES THE IMPORTANCE OF HAVING A SECURITY POLICY FOR MOBILE PHONES AND OTHER ELECTRONIC GADGETS

This section of the article is used to discuss some specific examples that illustrates the importance of having a security policy for mobile phones and other electronic gadgets Thus, this example illustrates the importance of having a security policy for mobile phones (see Figure 2 for more details).

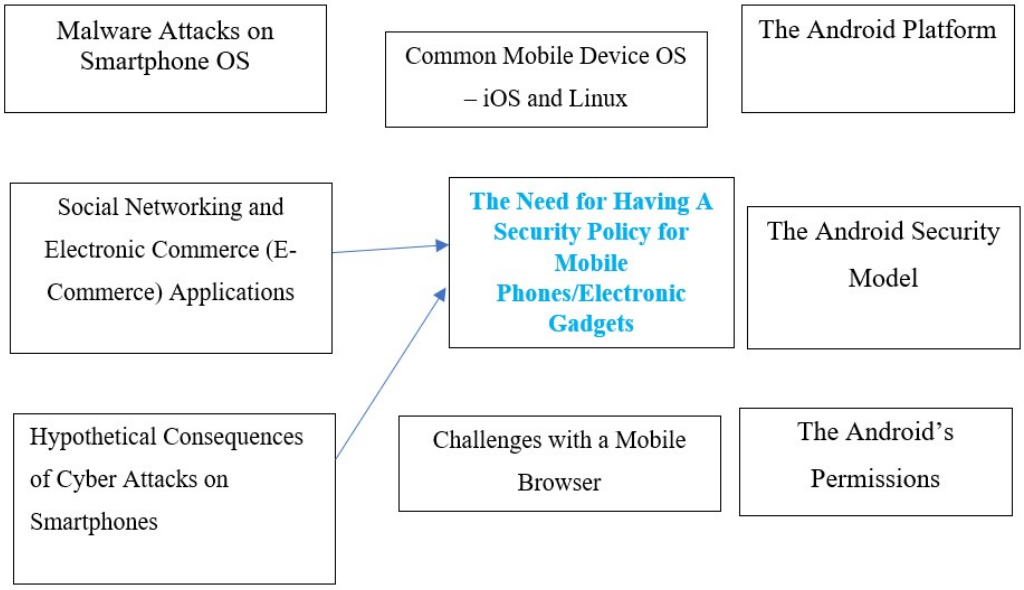

Figure 2: The Need for Having A Security Policy for Mobile Phones/ Electronic Gadgets
Source: Author's modification

Social Networking and Electronic Commerce (E-Commerce) Applications

Figure 2 reveals that social networking and electronic commerce (E-commerce) applications is one of the reasons why there is the need for having a security policy for mobile phones, and other electronic gadgets. In perusing the literature, it was observed that many people rely on their smartphones to do numerous activities, like sending

emails, storing contact information, passwords and other sensitive data. In addition to this, smartphones are the device of choice when it comes to social networking; thus, mobile applications for social networking sites (such as Facebook, Twitter, Google+) are another loophole for cyber attackers to gain personal data from unsuspecting users (Ruggiero, 2011). Meanwhile, 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

Again, Figure 2 revealed that hypothetical consequences of cyber attacks on Smartphones is one of the reasons why there is the need for having a security policy for mobile phones, and other electronic gadgets. 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 smartphones 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

Furthermore, Figure 2 discovered that the challenges with a mobile browser is also one of the reasons why there is the need for having a security policy for mobile phones, and other electronic gadgets. Very importantly, it is underscored in the literature that 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 smartphones. 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

From the literature, it was observed that common mobile device OS (i.e. iOS and Linux) is one of the reasons why there is the need for having a security policy for mobile phones, and other electronic gadgets (see Figure 2 for more details). Apple debuted iOS, or iPhone OS, in 2007, with the inception of the iPhone to the cell phone market (Barrera & Van Oorschot, 201 1). 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, 201 1). 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, 201 1). 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

Malware attacks on Smartphone OS is also seen as one of the reasons why there is the need for having a security policy for mobile phones, and other electronic gadgets (see Figure 2). 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, smartphones are an excellent way to spread malware because phones are great storage devices. A hypothetical example of a cyber 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

Interestingly, the use of the Android platform has also seen as one of the reasons why there is the need for having a security policy for mobile phones, and other electronic gadgets (see Figure 2). According to Shabtai, Fledel, Kanonov, Elovici, Dolev & Glezer (2010), Android is an opensource 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

Also, the existing Android security model is also seen as one of the reasons why there is the need for having a

security policy for mobile phones, and other electronic gadgets (see Figure 2). 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

Above all, the Android permission mechanism is also seen as one of the reasons why there is the need for having a security policy for mobile phones, and other electronic gadgets (see Figure 2). 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. 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 smartphones 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).

Legitimate Applications that Can Be Used to Retrieve Information

Presently, there is valid spy software available for various smartphones. An example of this is FlexiSpy, a legitimate commercial spyware program that cost over $300 (United States Computer Emergency Readiness Team, 2010). FlexiSpy can: (a)Listen to actual phone calls as they happen; (b) Secretly read Short Message Service (SMS) texts, call logs, and emails; (c) Listen to the phone surroundings (use as remote bugging device); (d) View phone GPS location; (e) Forward all email events to another inbox; (f) Remotely control all phone functions via SMS; (g) Accept or reject communication based on predetermined lists; and (h) 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 root kit tools, and freely availably malicious code it is easy to create a malware program.

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 smartphones 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 smartphones, it brought hackers' attention to smartphones. 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, Schmidt, Clausen & Kiraz, 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 apps. To make matters worse, hackers target popular apps, modify their source code, and then upload them again to the Android Market after injecting their malicious piece. Unfortunately, Google is not proactive in this area in that it does not remove potentially malicious apps until they receive complaints or until apps have already caused disruption and compromised sensitive data. Therefore, the researcher strongly believes that the greatest security risk lies at the heart of Android apps, where attackers are most capable of passing their malicious apps to end users through the Market and gain unauthorized access to confidential data to achieve financial gains. Furthermore, hackers are known to use attack strategies that tend to send expensive SMS messages and dial prime rate numbers as a quick and efficient way to gain money illegally.

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 5870.01 M 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 be replicated at a more cost-efficient manner.

Lastly, another limitation for creating a cyber security environment for smartphones 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.

CONCLUSION & SUGGESTIONS

Fortunately, there are possible solutions to the rampant cyber security problem with smartphones. 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. Some of the policy recommendations and implications are discussed based on the study findings as given below.

- **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 smartphones 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 smartphones 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.
- 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 (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

Barrera, D. & Van Oorschot, P. (2011). Secure Software Installation on Smartphones, *IEEE Security and Privacy*, *9*(3), pp. 42-48, Retrieved February 22, 2023.

Brechbuhl, H., Bruce, R., Dynes, S., & Johnson, E. (2010). Protecting Critical Information Infrastructure: Devloping Cybersecurity Policy. *Information Technology for Development*, *16*(1), pp. 83-91.

Best Mobile Security Software Comparisons and Reviews (2012) Retrieved February 17, 2023, from Top Ten Reviews: http://mobile-security-software-review.toptenreviews.com/

Canalys. (2011 , October 04). Mobile Security Investment to Climb 44% Each Year Through 2015, Retrieved February 22, 2023, from Canalys: http://www.canalys.com/newsroom/mobilesecurity-investment-climb-44-each-year-through-2015

CCEVS. (2008). National Security Agency, Common Criteria Evaluation and Validation Scheme, Common criteria evaluation and validation scheme -- organization, management, and concept of operations (Version 2.0), Retrieved from National Information Assurance Partnership: http://www.niap-ccevs.org/policy/ccevs/scheme-pub-1 .pdf

Eeten, M. V., & Bauer, J. (2009). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. *Journal of Contingencies and Crisis Management*, 17(4), 221-232.

Favell, A. (Ed.) (2011, November 2). 96 Percent of Smartphones and Tablets Lack Necessary Security Software. Why It Matters to Your Business - A Lot, Retrieved February 22, 2023, from MobiThinking: http://mobithinking.com/blog/mobile-security-business-implications

Goth, G. (2009). U.S. Unveils Cybersecurity Plan. *Government Policy*, *52*(8), 23.

Grace, M., Zhou, W., Jiang, X. & Sadeghi, A.R. (2012). Unsafe Exposure Analysis of Mobile In-App Advertisements, Association for Computing Machinery - *Security and Privacy in Wireless and Mobile Networks, 5*, pp. 101-1 12, doi:10.1 145/2185448.2185464.

Poushter, J., Caldwell, B., & Chwe, H. (2018). Appendix B: Country-specific examples of smartphones. *Pew Research Center*. Social Media Use Continues to Rise in Developing Countries | Pew Research Center

Harknett, R., & Stever, J. (2011). The New Policy World of Cybersecurity, (N. Roberts, Ed.). *Public Administration Review*, pp. 455-460.

Kaplan, J., Sharma, S., & Weinberg, A. (2011). Cybersecurity: *A Senior Executive's Guide. McKinsey Quarterly*(4).

MacWillson, A. (2011, May 9). Rethinking Cybersecurityin a Mobile World. Retrieved February 22, 2023, from Security Week: Internet and Enterprise Security News, Insights & Analysis: http://www.securityweek.com/rethinking-cybersecurity-mobile-world

Ontang, M., McLaughlin, S., Enck, W. & McDaniel, P. (2009) Semantically rich applicationcentric security in Android, Retrieved from Proceedings of teh 25th Annual Computer Security Applciations Conference (ACSAC '09): http://dl.acm.org

Rao, L. (2011, December 13). Lookout's 2012 Mobile Security Threat Predictions: SMS Fraud, Botnets And Malvertising, Retrieved February 22, 2023, from Tech Crunch: http://techcrunch .com/2011/12/13/lookouts-2012-mobile-security-threat-predictions-sms-fraud-botnets-andmalvertising/

Ruggiero, P. (2011). Cyber Threats to Mobile Phones, United States Computer Emergency Readiness Team, Pittsburgh, PA.

Schmidt, A.D., Bye, R., Schmidt, H.G., Clausen, J., & Kiraz, O. (2009). Static analysis of executables for collaborative malware detecion on Android, Retrieved from www.dailabor.de

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010, March/April). Android: A comprehensive security assessment. *IEEE Security & Privacy*, 8(2), pp. 35-44.

Symantec, Inc. (2011, April 5). Retrieved February 17, 2023, from Symantec Report Finds Cyber Threats Skyrocket in Volume and Sophistication: http://www.symantec.com/about/news /release/article.jsp?prid=201 10404_03

Traynor, P., Ahamad, M., Alperovitch, D., Conti, G. & Davis, J. (2012). Emerging Cyber Threats Report 2012, Georgia Tech Information Security Center, Atlanta, GA.

Trend Micro. (2009, August 17). Smartphone Users: Not Smart Enough About Security, Retrieved February 17, 2023, from Trend Micro: http://newsroom.trendmicro.com/index.php?s=43&news_item=738&type=archived&year=2009 United States Computer Emergency Readiness Team (2010, April 15) Cyber Threats to Mobile Devices, (TIP - 10-105-01), 1-16.

Vennon, T. (2010). Android malware, retrieved from http://threatcenter.smobilesystems.com/ ZDNet. (2010) Google fixes android root-access flaw, Retrieved from ZDNet: www.zdnetasia.com