IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURITY FOR MOBILE THREATS: THE NEED FOR SECURITY OF MOBILE PHONES

Aashutosh Umare
Student, Amity University Chhattisgarh, Raipur

Mohammed Bakhtawar Ahmed
Assistant Professor, Amity University Chhattisgarh, Raipur

ABSTRACT

Now days as we know smart phones have become a great part of our lives. A person does most of his work from calling, messaging, mailing, paying bills to booking tickets and hotels etc through their mobiles. So it's also necessary to take care that the transfer of data through one person to other are in a secure manner or not, since day to day we came across a lot of news that mobile scam are rising a lot due to which people are facing a serious problem . So to overcome these problem here is a great need to combine cyber security with smartphones .So that people can be tension free in e-transactions and using smart phones. At present, digital dangers run from Trojans and infections to botnets and toolboxes. Now days cell phones don't have pre-introduced security programming. This need security is an open door for noxious digital assailants to hack into the different smartphones that are well known (for example Android, iPhone and Blackberry). These days, smartphone clients can email, utilize informal communication applications (Facebook and Twitter), purchase and download different applications and shop. Specialized safety efforts, for example, firewalls, antivirus, and encryption, are unprecedented on smartphones, and smartphones working frameworks are not refreshed as often as possible as those on PCs. Versatile long range informal communication applications at times come up short on the point by point protection controls of their PC partners. Shockingly, numerous smartphone clients don't perceive these security deficiencies. Numerous clients neglect to empower the security programming that accompanies their telephones, and they accept that surfing the web on their smartphones is as protected as or more secure than surfing on their PCs. In the mean time, smartphones are turning out to be increasingly more significant as focuses for assault. Subsequently, this paper looks at the significance of building up a cybersecurity arrangement made for smartphones so as to ensure touchy, individual information.

INTRODUCTION

Smartphones, or mobile phones with advanced capabilities like those of personal computers (PCs), are appearing in more people's pockets, purses, and briefcases. Smartphones' popularity and relatively lax security have made them attractive targets for attackers. According to a report published earlier this year, smartphones recently outsold PCs for the first time, and attackers have been exploiting this expanding market by using old techniques along with new ones.1 One example is this year's Valentine's Day attack, in which attackers distributed a mobile picture sharing application that secretly sent premium-rate text messages from the user's mobile phone. One study found that, from 2009 to 2010, the number of new vulnerabilities in mobile operating systems jumped 42 percent.2 The number and sophistication of attacks on mobile phones is increasing, and countermeasures are slow to catch up. Smartphones and personal digital assistants (PDAs) give users mobile access to email, the internet, GPS navigation, and many other applications. However, smartphone security has not kept pace with traditional computer security. Technical security measures, such as firewalls, antivirus, and encryption, are uncommon on mobile phones, and

mobile phone operating systems are not updated as frequently as those on personal computers.3 Mobile social networking applications sometimes lack the detailed privacy controls of their PC counterparts. 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, 2011). Thus, this example illustrates the importance of having a security policy for mobile phones.

Typical Attacks Leverage Portability and Similarity to PCs

Mobile phones share many of the vulnerabilities of PCs. However, the attributes that make mobile phones easy to carry, use, and modify open them to a range of attacks. • Perhaps most simply, the very portability of mobile phones and PDAs makes them easy to steal. The owner of a stolen phone could lose all the data stored on it, from personal identifiers to financial and corporate data. Worse, a sophisticated attacker with enough time can defeat most security features of mobile phones and gain access to any information they store.5 • Many seemingly legitimate software applications, or apps, are malicious.6 Anyone can develop apps for some of the most popular mobile operating systems, and mobile service providers may offer third-party apps with little or no evaluation of their safety. Sources that are not affiliated with mobile service providers may also offer unregulated apps that access locked phone capabilities. Some users "root" or "jailbreak" their devices, bypassing operating system lockout features to install these apps. • Even legitimate smartphone software can be exploited. Mobile phone software and network services have vulnerabilities, just like their PC counterparts do. For years, attackers have exploited mobile phone software to eavesdrop, crash phone software, or conduct other attacks.7 A user may trigger such an attack through some explicit action, such as clicking a maliciously designed link that exploits a vulnerability in a web browser. A user may also be exposed to attack passively, however, simply by using a device that has a vulnerable application or network service running in the background.8 • Phishing attacks use electronic communications to trick users into installing malicious software or giving away sensitive information. Email phishing is a common attack on PCs, and it is just as dangerous on email-enabled mobile phones. Mobile phone users are also vulnerable to phishing voice calls ("vishing") and SMS/MMS messages ("smishing").9 These attacks target feature phones (mobile phones without advanced data and wireless capabilities) as well as smartphones, and they sometimes try to trick users into receiving fraudulent charges on their mobile phone bill. Phishers often increase their attacks after major current events, crafting their communications to look like news stories or solicitations for charitable donations. Spammers used this strategy after the March 2011 earthquake and tsunami in Japan.10

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 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).

Consequences of a Mobile Attack Can Be Severe

Many users may consider mobile phone security to be less important than the security of their PCs, but the consequences of attacks on mobile phones can be just as severe. Malicious software can make a mobile phone a member of a network of devices that can be controlled by an attacker (a "botnet"). Malicious software can also send device information to attackers and perform other harmful commands. Mobile phones can also spread viruses to PCs that they are connected to. Losing a mobile phone used to mean only the loss of contact information, call histories, text messages, and perhaps photos. However, in more recent years, losing a smartphone can also jeopardize financial information stored on the device in banking and payment apps, as well as usernames and passwords used to access apps and online services. If the phone is stolen, attackers could use this information to access the user's bank account or credit card account. An attacker could also steal, publicly reveal, or sell any personal information extracted from the device, including the user's information, information about contacts, and GPS locations. Even if the victim recovers the device, he or she may receive many spam emails and SMS/MMS messages and may become the target for future phishing attacks. Some personal and business services add a layer of authentication by calling a user's mobile phone or sending an additional password via SMS before allowing

the user to log onto the service's website. A stolen mobile phone gets an attacker one step closer to accessing the services as the user. If the device contains the owner's username and password for the service, the attacker would have everything necessary to access the service.

Take Steps to Protect Your Mobile Phone

Although mobile phones are taking on more capabilities formerly available only on PCs, technical security solutions for mobile phones are not as sophisticated or widespread as those for PCs. This means that the bulk of mobile phone security relies on the user making intelligent, cautious choices. Even the most careful users can still fall victim to attacks on their mobile phones. However, following best practices regarding mobile phone security can reduce the likelihood or consequences of an attack. • When choosing a mobile phone, consider its security features. Ask the service provider if the device offers file encryption, the ability for the provider to find and wipe the device remotely, the ability to delete known malicious apps remotely, and authentication features such as device access passwords. If you back up your phone data to a PC, look for an option to encrypt the backup. If you plan to use the device for VPN access, as some users do to access work networks, ask the provider if the device supports certificate-based authentication. • Configure the device to be more secure. Many smartphones have a password feature that locks the device until the correct PIN or password is entered. Enable this feature, and choose a reasonably complex password. Enable encryption, remote wipe capabilities, and antivirus software if available. • Configure web accounts to use secure connections. Accounts for certain websites can be configured to use secure, encrypted connections (look for "HTTPS" or "SSL" in account options pages). Enabling this feature deters attackers from eavesdropping on web sessions. Many popular mail and social networking sites include this option.

• Do not follow links sent in suspicious email or text messages. Such links may lead to malicious websites.

• Limit exposure of your mobile phone number. Think carefully before posting your mobile phone number to a public website. Attackers can use software to collect mobile phone numbers from the web and then use those numbers to target attacks.

• Carefully consider what information you want stored on the device. Remember that with enough time, sophistication, and access to the device, any attacker could obtain your stored information.

• Be choosy when selecting and installing apps. Do a little research on apps before installing them. Check what permissions the app requires. If the permissions seem beyond what the app should require, do not install the app; it could be a Trojan horse, carrying malicious code in an attractive package.

• Maintain physical control of the device, especially in public or semi-public places. The portability of mobile phones makes them easy to lose or steal.

• Disable interfaces that are not currently in use, such as Bluetooth, infrared, or WiFi. Attackers can exploit vulnerabilities in software that use these interfaces.

• Set Bluetooth-enabled devices to non-discoverable. When in discoverable mode, your Bluetooth-enabled devices are visible to other nearby devices, which may alert an attacker or infected device to target you. When in non-discoverable mode, your Bluetooth-enabled devices are invisible to other unauthenticated devices.

• Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots. Attackers can create phony Wi-Fi hotspots designed to attack mobile phones and may patrol public Wi-Fi networks for unsecured devices. Also, enable encryption on your home Wi-Fi network.11

• Delete all information stored in a device prior to discarding it. Check the website of the device's manufacturer for information about securely deleting data. Your mobile phone provider may also have useful information on securely wiping your device.

• Be careful when using social networking applications. These apps may reveal more personal information than intended, and to unintended parties. Be especially careful when using services that track your location.

• Do not "root" or "jailbreak" the device. Third-party device firmware, which is sometimes used to get access to device features that are locked by default, can contain malicious code or unintentional security vulnerabilities. Altering the firmware could also prevent the device from receiving future operating system updates, which often contain valuable security updates and other feature upgrades.

CONCLUSION

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. 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 (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

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

Barrera, D. & Van Oorschot, P. (2011) Secure Software Installation on Smartphones, IEEE Security and Privacy, 9(3), pp. 42-48, Retrieved June 26, 2012

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

Canalys (2011, October 04) Mobile Security Investment to Climb 44% Each Year Through 2015, Retrieved April 22, 2012, 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, December). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications.

"Technical Information Paper: Cyber Threats to Mobile Devices" (http://www.us-cert.gov/reading_room/TIP10-105-01.pdf)

"Protecting Portable Devices: Physical Security" (http://www.us-cert.gov/cas/tips/ST04-017.html)

"Protecting Portable Devices: Data Security" (http://www.us-cert.gov/cas/tips/ST04-020.html)