ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (345-350), Month: October - December 2015, Available at: www.researchpublish.com

Mobile Security And Privacy In Smartphone Technology

[1]Mohamed Ibrahim, [2]Ganesin Supayah, [3]Jamaluddin Bin Ibrahim

[1,2,3] Kuliyyah of Information Technology, International Islamic University, Kuala Lumpur 53100, Malaysia

Abstract: **Such is the case with mobile technology, particularly smartphones, which have exploded in popularity in recent years. According to market analysis firm ABI Research, 370 million smartphones were in use globally last year. Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they can also result from the poor security practices of consumers. Many researchers and practitioners are expecting a major security incident with mobile phones ever since these devices began to become more powerful: with increased processing power and memory, increased data transmission capabilities of the mobile phone networks, and with open and third-party extensible operating systems, phones become an interesting target for attackers. However, in this paper we highlighted mobile phone security and recommendation for mobile security.**

Keywords: **Mobile communication, smart phone, Android, apple ios, wifi,mobile security.**

I. INTRODUCTION

Mobile from the Latin mobilis - "to move" "able to move freely or easily" "able or willing to move freely or easily between occupations, places of residence and social classes". Mobile device means Mobile, wireless or cellular phone - a portable, handheld communications device connected to a wireless network that allows users to make voice calls, send text messages and run applications (Sharon, 2008). Mobile technology is promptly changing the appearance of communication in the most remote areas of the world. Now, out of the seven billion people in the world, approximately six billion are mobile phone subscribers. In response, companies, governments, and NGOS alike have comprehended the potential of this tool in addressing today's most pressing global challenges (Sonko, 2014).

Most people have at least a simple, if not sophisticated, mobile phone. These devices are convenient to carry around and you can use them on the go as long as there is network coverage wherever you are. Mobile phones have clearly made it easier to communicate (Katz & Aakhus, 2002). With the upgrades made year in, year out, mobile phones are becoming more like computers with the added benefit of portability. One can receive and send emails, browse websites, download games and videos, book flight tickets, money transfer to banks and even chat with friends. With a mobile phone , people connected to the internet throughout. People can search for places and directions for places that you are not familiar with, you can check out what your friends are up to on social media and you can even access your work PC remotely (Thornton & Houser, 2005).As well, built-in global positioning system (GPS) technology means users can be located via a signal sent from their mobile phone (Zhao, 2002). With appropriate guidelines in place, a mobile phone can significantly enhance the safety of its users and their families.

II. BACKGROUND INFORMATION

Thus, after years of warnings about mobile security, there finally appears to be a reason to worry. In fact, the number and types of mobile threats—including viruses, spyware, malicious downloadable applications, phishing, and spam—have spiked in recent months. Smart phones and other mobile devices are like a pocket computers. They now have the power and functionality of desktop computers – and the privacy and security risks inherent to the Internet. Like peoples desktop

and laptop computers, people's mobile devices may contain, or are capable of accessing, large amounts of personal information: contact information of their friends and associates, family photos and videos, and our web browsing history, among other details. And like personal computers, smart phones, and other mobile devices are targets for malware and spyware (Rastogi, Chen, & Jiang, 2013).

In an important step to strengthen the privacy protections for users of mobile applications, the California Attorney General in early 2012 announced a Joint Statement of Principles, endorsed by the companies whose platforms comprise the majority of the mobile app market (Amazon, Apple, Facebook, Google, Hewlett-Packard, Microsoft, and Research In Motion). The principles are intended to ensure that mobile apps comply with applicable privacy laws such as the California Online Privacy Protection Act, and include the conspicuous posting of a privacy policy by mobile apps when required by law, a means to make the policy available from the app platform before downloading, a way for users to report non-compliant apps to the platform provider, a process to respond to such reports, and a pledge to further work with the Attorney General on best practices for mobile privacy (Krleža-Jerić et al., 2005). For instance, McAfee Labs' threat report for 2010's fourth quarter reported a 46 percent increase in malware targeting mobile phones over the same time period the previous year.

III. DRAWBACK OF MOBILE PHONE

Possibility of Privacy Leak:

Over the past decade, privacy has gained significant attention in academia as well as in industry. The main reason behind this interest is the consequences of privacy violation on individuals. On the one hand, sensitive user data can be exploited by malicious identities to steal or expose personal information about the users and on the other hand it can be misused to harm users financially or socially. Moreover, companies can also use this data to learn sensitive personal identifiable information about users without their consent and awareness (Christin, Reinhardt, Kanhere, & Hollick, 2011).

Considering the nature of mobile and wearable devices, individuals are device owners as well as the people surrounding the device. Consent here means the degree of agreement between the user's awareness about data collection and the actual data handling by the application. Many surveys have been carried out to estimate user expectation and awareness with respect to privacy leaks through their devices (Sadeh et al., 2009).

Botnets:

A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms - currently pose the biggest threat to the Internet. A report from Symantec came to a similar conclusion(Mahajan). Last year, another mobile botnet targeted European customers of a Dutch online bank. The malware used in the attack included command logic that gave the hacker remote control of victims' smartphones. With PCs, hackers often use zombies within botnets to launch denial-of-service attacks. Thus far, though, there have been no major mobile DoS incidents.

Spyware:

With so many types of malicious software being spread around the Internet, it is important to be aware of what spyware is and what spyware does. Spyware is a general term used to describe software that performs certain behaviors, generally without appropriately obtaining your consent first, such as:

- Advertising
- Collecting personal information
- Changing the configuration of your computer

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. That does not mean all software that provides ads or tracks your online activities is bad. For example, you might sign up for a free music service, but you "pay" for the service by agreeing to receive targeted ads. If

you understand the terms and agree to them, you may have decided that it is a fair tradeoff. You might also agree to let the company track your online activities to determine which ads to show you (Moshchuk, Bragin, Gribble, & Levy, 2006).

Knowing what spyware does can be a very difficult process because most spyware is designed to be difficult to remove. Other kinds of spyware make changes to your computer that can be annoying and can cause your computer slow down or crash. These programs can change your web browser's home page or search page, or add additional components to your browser you don't need or want. They also make it very difficult for you to change your settings back to the way you had them (Kirda, Kruegel, Banks, Vigna, & Kemmerer, 2006).

The key in all cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer. A common trick is to covertly install the software during the installation of other software you want such as a music or video file sharing program. Whenever you install something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it might appear at the end of a license agreement or privacy statement (Egele, Kruegel, Kirda, Yin, & Song, 2007).

Social networking:

As smartphone use has grown, so has mobile social networking. Malicious links on social networks can effectively spread malware. Participants tend to trust such networks and are thus willing to click on links that are on "friends'" social networking sites, even though—unknown to the victim—a hacker may have placed them there, said M86's Antsis. Clicking on a link could download a malicious application on a victim's computer, said Network Box USA's Stella. This could let a hacker place Trojans, spyware, and backdoors on the machine and even conduct identity or information theft, he added. Some schemes use a sensational headline or promise information on a current hot topic to grab readers' attention and encourage them to click on a malicious link.

Bluetooth:

Bluetooth is best known as the wireless technology that powers hands-free earpieces. Depending on your point of view, people who wear them either: (1). Look ridiculous (especially if shining a bright blue LED from their ear); (2) Appear mad (when apparently talking to themselves); or (3) Are sensible, law-abiding, safety-conscious drivers.

Whichever letter you pick, insidious security issues remain around Bluetooth attacks and mobile devices. While most of the problems identified five to 10 years ago have been straightened out by now, some still remain. And there's also good reason to be cautious about new, undiscovered problems. Here are a few examples of the mobile security threats in which Bluetooth makes us vulnerable, along with tips to secure your mobile workforce devices. General software vulnerabilities- Software in Bluetooth devices – especially those using the newer Bluetooth 4.0 specification – will not be perfect. It's unheard of to find software that has zero security vulnerabilities. As Finnish security researchers Tommi Mäkilä, Jukka Taimisto and Miia Vuontisjärvi demonstrated in 2011, it's easy for attackers to discover new, previously unknown vulnerabilities in Bluetooth devices. Potential impacts could include charges for expensive premium-rate or international calls, theft of sensitive data or drive-by malware downloads. To combat this threat: Switch off your Bluetooth when you're not using it (Rights, 2001).

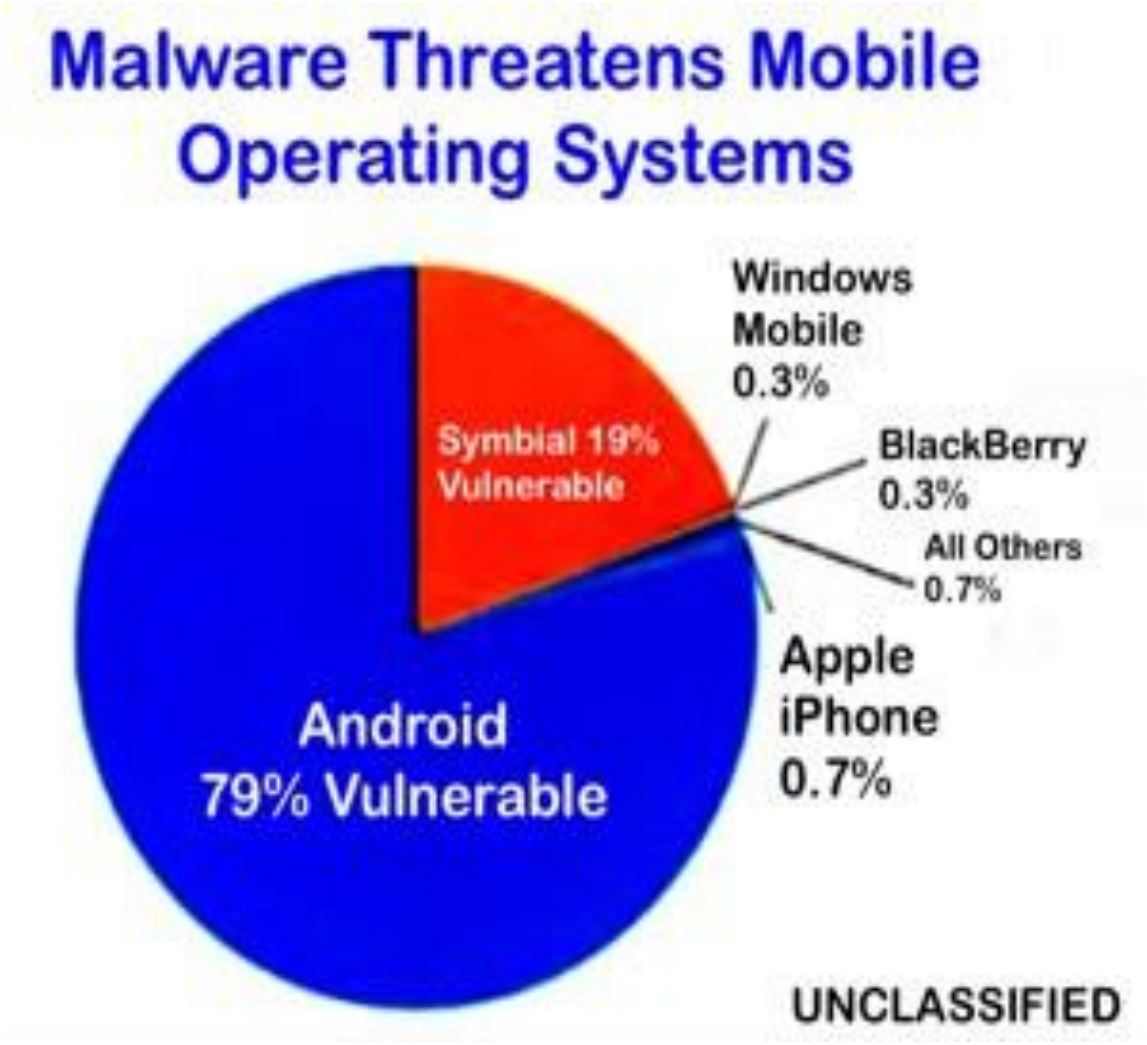
Wi-Fi:

Most Wi-Fi hotspots aren't encrypted, thus anyone within range can eavesdrop on the data you send and receive from the Internet and your mobile device. The same applies when using a laptop on a hotspot, or your computers at home on your own wireless router if it isn't encrypted with WEP, WPA, or WPA2 security. Eavesdropping on Wi-Fi connections isn't rocket science. It just takes a curious individual with free tools and some spare time. There are many software programs out there that can capture and display your data that's being transmitting through the air waves. Some programs show just the raw data packets but some make it much quicker and easier to get to the real prize. For example, some programs such as Firesheep and SniffPass simply listen for and show login credentials to unsecured sites or services, like social networking sites and Web-based or POP3/IMAP email accounts. Some programs such as EffeTechHTTPSniffer can even capture and reassemble the webpages you are viewing and files you transfer (Lee, Lee, Yi, Rhee, & Chong, 2010). Though eavesdroppers can capture data packets of your online banking and sensitive transactions when using Wi-Fi, the data is encrypted if it's secured with SSL (like most sensitive sites are). The eavesdropper just sees a bunch of gibberish.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (345-350), Month: October - December 2015, Available at: www.researchpublish.com

The same goes with other services. For instance, if you check your email through the browser or a client app on the device and it's secured with SSL, you don't have to worry (Oberheide, Veeraraghavan, Cooke, Flinn, & Jahanian, 2008).

If you're really concerned about your mobile Internet security, consider using a Virtual Private Network (VPN) on both your Wi-Fi and cell data connections. When connected to a VPN, all your Internet traffic travels through an encrypted tunnel, guarding it from local eavesdroppers (Henry & Luo, 2002). It protects your traffic and passwords not already encrypted and also gives encrypted traffic double encryption. In addition to encryption purposes, VPNs can also give you secure remote access to files and network resources at work or home. iOS - iPhone, iPad, and iPod Touch - and Android are two popular mobile platforms that include native VPN support. Most other platforms include some type of VPN functionality but usually require you to have a special server in addition to a VPN server (O'neill, 2008).

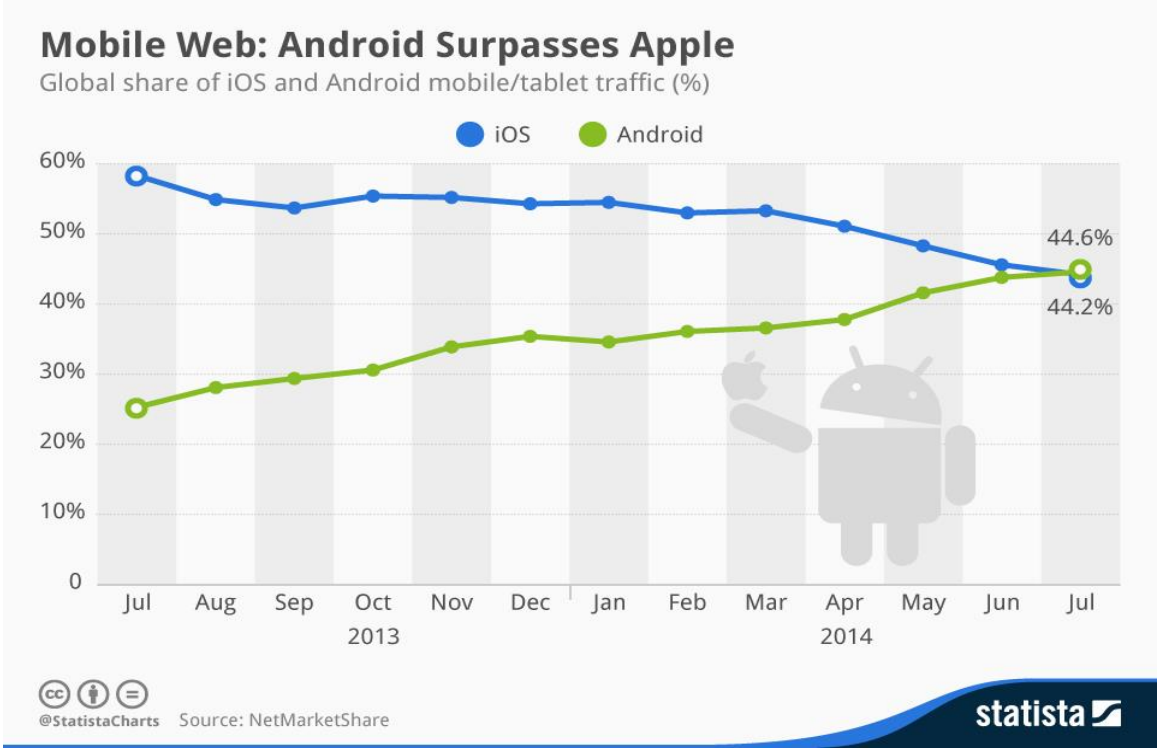


Figure(1) Malware threatens mobile operating systems

Phishing:

Phishing poses the same risk on smartphones as it does on desktop platforms. In fact, many users trust their mobile device more than their computers and thus are more vulnerable to phishing. Additionally, said Juniper Networks' Vennon, the lack of maturity in phishing filters and reputation-based services in mobile browsers, combined with the immediacy and portability of telephone communications, makes the platform attractive for phishers (Dhamija, Tygar, & Hearst, 2006). Mobile phishing is particularly tempting because wireless communications enable phishing not only via e-mail, as is the case with PCs, but also via SMS and MMS, noted AT&T's de Los Reyes. Social media phishing is becoming a major issue as social networking sites contain an increasing amount of personal information that phishers can use to make their attacks more effective, said Paul Henry, security and forensics analyst for market research firm Lumension Security.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (345-350), Month: October - December 2015, Available at: www.researchpublish.com



Figure(b) shows android surpasses Ios operating system

IV. RECOMMENDATION FOR MOBILE SECURITY

The greater visibility of mobile phone security will place an increasing importance on mobile device makers having enterprise-grade security features and configuration options in place. It will become necessary for security to be considered in all phases of application development to ensure that resiliency against attacks is built into mobile devices from the start," said Adrian Stone, director of security response for BlackBerry vendor Research in Motion. "Our dependence on an always- on, connected, mobile device environment is going to be profound in critical contexts that we can't imagine today," said Stammberger. "We have to be able to trust these devices, but we can't now. There's still a lot of work that needs to be done to get to the point where that trust is warranted." (Yi, Kim, Shin, & Hyun, 2012)

While users now often protect their PCs with antivirus software, such measures are not so widespread in cellular phones. Most users aren't aware of potential mobile malicious code problems and thus aren't vigilant in preventing or avoiding attacks on their phones, said Vanja Svajcer, principal virus researcher for SophosLabs, a global network of virus and spam analysis centers overseen by antivirus company Sophos. Also, few mobile phones currently have antivirus software, although companies are starting to install it. For example, Japan's NTT DoCoMo now provides buyers of its new Symbian-based FOMA 901i phones with McAfee's VirusScan technology.

Nokia has introduced two phones with Symantec Client Security software, which is preloaded on the memory card and can be updated wirelessly through Symantec Live Update. Antivirus-software vendor Trend Micro recently rolled out Trend Micro Mobile Security, which provides antivirus and antispam protection for mobile devices' SMS applications.

V. CONCLUSION

The area of mobile agent security is in a state of immaturity, but rapidly improving. The traditional orientation toward host-based security persists and, therefore, available protection mechanisms tend to focus on protecting the agent platform. Emphasis is beginning to move toward developing techniques that are oriented toward protecting the agent, a much more difficult problem. The initial efforts are encouraging and will hopefully continue. There are a number of agent-based application domains for which basic and conventional security techniques should prove adequate. The countermeasures reviewed in this paper complement those techniques to reach a wider range of application domains. However, applications are expected to require a more comprehensive set of mechanisms and a flexible framework .

REFERENCES

[1] Christin, D., Reinhardt, A., Kanhere, S. S., & Hollick, M. (2011). A survey on privacy in mobile participatory sensing applications. Journal of Systems and Software, 84(11), 1928-1946.

[2] Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

[3] Egele, M., Kruegel, C., Kirda, E., Yin, H., & Song, D. X. (2007). Dynamic Spyware Analysis. Paper presented at the USENIX annual technical conference.

[4] Henry, P. S., & Luo, H. (2002). WiFi: what's next? Communications Magazine, IEEE, 40(12), 66-72.

[5] Katz, J. E., & Aakhus, M. (2002). Perpetual contact: Mobile communication, private talk, public performance: Cambridge University Press.

[6] Kirda, E., Kruegel, C., Banks, G., Vigna, G., & Kemmerer, R. (2006). Behavior-based Spyware Detection. Paper presented at the Usenix Security.

[7] Krleža-Jerić, K., Chan, A.-W., Dickersin, K., Sim, I., Grimshaw, J., & Gluud, C. (2005). Principles for international registration of protocol information and results from human trials of health related interventions: Ottawa statement (part 1). BMJ: British Medical Journal, 330(7497), 956.

[8] Lee, K., Lee, J., Yi, Y., Rhee, I., & Chong, S. (2010). Mobile data offloading: how much can WiFi deliver? Paper presented at the Proceedings of the 6th International COnference.

[9] Mahajan, P. Digital Crime and Forensics Project Prashant Mahajan & Penelope Forbes. Moshchuk, A., Bragin, T., Gribble, S. D., & Levy, H. M. (2006). A Crawler-based Study of Spyware in the Web. Paper presented at the NDSS.

[10] O'neill, A. (2008). Methods and apparatus for efficient VPN server interface, address allocation, and signaling with a local addressing domain: Google Patents.

[11] Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J., & Jahanian, F. (2008). Virtualized in-cloud security services for mobile devices. Paper presented at the Proceedings of the First Workshop on Virtualization in Mobile Computing.

[12] Rastogi, V., Chen, Y., & Jiang, X. (2013). Droidchameleon: evaluating android anti-malware against transformation attacks. Paper presented at the Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security.

[13] Rights, R. F. (2001). SANS Institute InfoSec Reading Room. Risk, 1, 27. Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., & Rao, J. (2009).

[14] Sharon, M. (2008). An introduction to mobile technologies and services. Socialight, available at http://uberthings. com/mobile/intro_to_mobile. pdf. Accessed: Feb, 18.

[15] Sonko, J. (2014). The Benefits and Challenges of Mobile Technologies in Education: A Perspective for Sub-Saharan Africa. Promoting Active Learning through the Integration of Mobile and Ubiquitous Technologies, 55.

[16] Thornton, P., & Houser, C. (2005). Using mobile phones in English education in Japan. Journal of computer assisted learning, 21(3), 217-228.

[17] Yi, K.-H., Kim, H.-J., Shin, M.-S., & Hyun, A.-S. (2012). Wrist watch type mobile terminal: Google Patents.

[18] Zhao, Y. (2002). Standardization of mobile phone positioning for 3G systems. Communications Magazine, IEEE, 40(7), 108-116.