WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Security: Mobile Devices Security

Kevin Curran1, Vivian Manynes2, Haris Raghavendra. T3, Guru Harrish. N4

[1,2,3,4]B. Sc AI & ML, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore.

A B S T R A C T

Mobile Device are a big part of Human daily Life , and are integrated part of daily Business process. The first and Most important step against Computer Security attacks is Awareness and understanding of nature of threats and this Consequences. Some of the attacks on Mobile device are related to Social Engineering. It is preferred to apply Biometrics for Security of mobile devices and improve reliability over wireless services.The Standard desktop Operating system is quickly being overtaken by Computing on Mobile Device however many of us are unware of the Security Vulureabilites on mobile devices. This study aims to highlight the significance of creating a national security strategy for mobile devices in order to safeguard private and sensitive information.

Keywords: Mobile Device, Malware, Cyber Security, Data loss, IT audit.

INTRODUCTION

Looking at the smartphone operating systems in the world market, it is seen that 88% of all smartphones have Android OS in the second quarter of 2018 [1]. In the context of this study, awareness research was performed, and it was discovered that 61% of participants used Android OS-powered mobile devices. In June 2011, for the first time ever, people on average spent more time using mobile applications (81 minutes) than browsing the mobile web (74 minutes) [2].Previously only able to be used for basic voice communication, mobile devices may now now be used to send text messages, access email, browse the web, and even conduct financial transactions.Even more significant,Mobile applications are transforming the device into a multipurpose computer platform. Since the release of the Apple iPhone SDK in 2008, Apple has boasted over 425,000 applications for i-OS devices.

There is no fundamentally more secure mobile OS than another.Each has its advantages, and frequently the more well-liked option is also the most secure one, but because of its popularity, that is the target of the majority of hacker assaults. . Basically it is a numbers game. But I will say at this time that Android needs to improve its app security. Apple has an easier time as they have a more stringent entry test to getting an app into their app store. Google by default allow most people to post an app to the store but they are trying to become better at identifying rogue apps. The appropriate evaluation of their skills has not actually been done. It is common knowledge that phones have been hacked even with the latest mobile "security suite" installed. Easiest way to protect is to simply install the leading well know apps and to steer clear of ‘recent uploads’. A time stamp is important as most malware on phones is discovered but the first people to download it are the ones compromised. An overview of the security measures used to make mobile devices safe to use is provided below.

1. MOBILE DEVICE SECURITY

A mobile gadget is a piece of technology that can take on various shapes. These devices may store photos or document files with sensitive information (such as home addresses, credit card numbers, and personal photos). (Fling, 2009; Holzer and Ondrus, 2009). Mobile computers, personal digital assistants/enterprise digital assistants, pagers, personal navigation devices (PNDs), mobile phones, and portable media players are among the different types of mobile devices that are currently accessible. A mobile phone is now used by more than half of the world's populace. (ITU, 2008). Today, more than half of all corporate computers are portable, and the rise of Internet of Things (IoT) devices presents new difficulties for network security.As a result, IT must modify its protection strategy. Although you can take some easy steps to improve your mobile device security, a network security strategy must take into consideration all of the various locations and uses that employees demand of the company network.

Although it is not an easy job, securing mobile devices should be a top priority for any enterprise. Because users don't always protect their devices or follow safe practices, cybercriminals target mobile devices. To combat the growing threat of cybercrime, businesses need to take preventative measures. Cyber criminals target businesses every day looking for sensitive data they can use to steal identities and commit fraud.

2. MALWARE ATTACKS ON SMARTPHONE OS

Malware that targets smartphone working systems is also continuously changing. The malware known as "Zeus-in-the-Mobile" (ZitMo), which is unique to the Android operating system, serves as an illustration of this. In an effort to circumvent banking two-factor authentication, steal user credentials, and

eventually get access to customers' bank accounts and money, ZitMo targeted bank apps used by Android users. (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). IT specialists are attempting to stop a variety of cyberattacks, including this one. Malware assaults on mobile devices most frequently involve viruses, worms, mobile bots, phishing scams, ransomware, spyware, and Trojans. Some mobile malware mixes multiple attack types. Mobile viruses are created to propagate from one vulnerable phone to another and have been modified for the cellular environment.

In 2016, there were 8,526,221 malicious installation packages, which is a threefold rise over 2015, according to the most recent report from Kaspersky Lab [42]. In contrast, they found over 10 million malicious installation programmes between 2004 and 2013; in 2014 and 2015, those numbers were 2.4 million and 2.96 million. The most crucial issue is that a large number of unexpected (or unknown) attacks target smart devices. For instance, if a malware app pretends to be a legitimate app with logical permissions while concealing some malicious activities under its hood, how can the OS tell whether it is malware or not? Android does have some basic mechanisms to control the permissions of apps.

3. MOBILE OS VULNERABILITIES

The first and most crucial step in comprehending where, why, and how corporate devices might be vulnerable to attack is to have a comprehensive understanding of the known vulnerabilities in mobile operating systems. The first group is the group of software that exploits mobile software, called malwares (Types of mobile malware). The second category consists of software flaws that are not the result of malicious software. Third is the vulnerabilities common in corporate settings (data leakage). The fourth group is not a software intended to exploit the mobile devices but the vulnerabilities of the installed software itself.

Comparatively lengthier vulnerability windows exist for Android devices than for iOS. Enterprises may have significant security concerns due to Android ecosystem fragmentation. The biggest security issue with Android is the difficulty in getting hundreds of carriers and dozens of manufacturers to collaborate on routinely patching Android smartphones and tablets., according to Wired.

4. PRIVACY

Smartphone security in general is a problem. There are over two billion smartphones in use worldwide, with the majority of consumers using their devices for both personal and business use. Smartphones are becoming the PC of yesteryear with the added problem of mobility which can lead to physical theft which can then lead to identity theft as more of use store important financial information on smartphones such as credit card and bank account information, e-mails, photos, notes, contacts and messages. The number of identity fraud incidents is increasing year on year. Smartphones running the Android operating system represent the majority of all new phone purchases.

The International Telecommunication Union estimates that there are already more mobile devices in use worldwide than there are humans. Additionally, mobile gadgets are becoming more and more sophisticated.Modern smartphones are actually just as powerful as desktop computers, but they "know" a lot more about their owners: their present and previous locations, the contents of their private text messages, pictures, and Their online banking login details, along with other sensitive information, and other financial information. They are also constantly linked to the Internet, making them particularly susceptible to malware exploits and hacking.

5. SECURITY ISSUES IN MOBILE DEVICES

Because security concerns impede the growth of mobile services, mobile devices should be seriously considered. At the very beginning of the service creation process, every security concern needs to be resolved. For the creators of mobile services, the complexity of technological solutions, unauthorised copying of software and content, and dangers posed by the Internet are the main sources of mobile security threats.

Mobile device security threats are on the rise. On more than 1 million user devices, Kaspersky discovered nearly 3.5 million bits of malware in 2014. . Kaspersky's in-lab detection tools processed 360,000 malicious files per day by the end of 2017. Additionally, 78% of those files were malware programs, for a daily discovery rate of over 280,000 malware files, many of which were created with mobile devices in mind. Here are the top seven dangers to mobile devices today, along with predictions for the future.

CONCLUSIONS

It is difficult to generate a common security structure which addresses all the vulnerabilities in the mobile device world. Therefore it is quite ossible that no one lone solution will resolve all potential problems. Firstly the operators of the networks mainly wireless need to take responsibility for providing a secure, efficient mechanism of communication. To maintain the security of mobile devices, such communication channels must include robust authentication processes. To guarantee they are impervious to network and virus attacks, mobile devices themselves must include system-level security.The manufactures of mobile device applications and services need to once again incorporate strong authentication, authorisation and accounting procedures. Even if all these mechanisms are deployed further issues that need addressing to ensure mobile devices are secure are political and cultural concerns, social engineering and business practices and policies.

Therefore, how to achieve new security challenges isa thinkable question. Further research is needed in order to face the security challenges in mobile environment and it should be given because their security risk poses an obstacle for users. Participants at the 2019 World Economic Forum [106] came

to the opinion that the global cybersecurity journey has only just begun over the last ten years. As we approach a new age of cybercrime, which will be fueled by new and emerging technology, new architectures and cooperation are still necessary. The convergence of 5G networks and infrastructure, artificial intelligence, and biometrics are the three technologies that will shape the next ten years of worldwide cybersecurity

References

[1] Statista, Smartphones—Statistics & Facts, Statista, Hamburg,Germany, 2020, https://www.statista.com/topics/840/smartphones/.

[2] B. Guo, Y. Ouyang, T. Guo, L. Cao, and Z. Yu, "Enhancingmobile app user understanding and marketing with het-erogeneous crowdsourced data: a review," IEEE Access,vol. 7, pp. 68557–68571, 2019

[3] Pasquinucci, A. (2009). The security challenges ofmobile devices. Computer Fraud & Security,2009(3), 16-18.

[4] Eckert, C. (2005). Security issues of mobiledevices Security in Pervasive Computing (pp.163-163): Springer

[5] S. Coorporation, "Symantec Internet Security Threat Report VolumeXVI," Whitepaper, vol. 16, Apr 2011.

[6] Kasperksy Lab, "Popular Porn Sites Distribute a New TrojanTargeting Android Smartphones," 2010. [Online]. Available: http://www.kaspersky.com/news?id=207576175

[7] C. Papathanasiou and N. J. Percoco, "This is not the droid you'relooking for..." in DEFCON 18, July 2010

[8] B'far, R. (2005) Mobile Computing Principles: Designing and Developing Mobile Applications, Cambridge University Press, London, UK. Burns, J. (2008) Developing Secure Mobile Applications for Android, iSec Partners, NY, USA.

[9] Chetan-Sharma (2013), Chetan Sharma: Technology and Strategy Consulting, available at: www.chetansharma.com/index.htm (accessed 4 March 2013).

[10] Commission of European Communities (2003), "Commission recommendation concerning thedefinition of micro, small- and medium-sized enterprise adopted by the commission",Official Journal of the European Union, 2003/361/EC.