International Journal of Advanced Technology in Engineering and Science
Vol. No. 10, Issue No. 07, July 2022
www.ijates.com
ijates
ISSN 2348 - 7550

Cyber Security And Mobile Threats : The Need For Antivirus Applications For Smart Phones

[1]Mrs.M.Angelin Rosy, [2]Dr M Felix Xavier Muthu, [3]Ms.S.Elamathi,

[1]Assistant Professor, [2]Associate Professor, [3]I MCA,

[1, 3]Master of Computer Application, [2]Mechanical Engineering

[1,3]Er Perumal Manimekalai College of Engineering, [2]St Xavier's Caholic college of Engineering

[1]angel_rosym@yahoo.co.in, [2]umilfelix@gmail.com, [3]Mathishanmugam.pem@gmail.com

ABSTRACT

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. Thus, thispaper examines the importance of developing a national security policy created for mobile devices in order to protect sensitive, personal data.

Keywords: *Cyber Security, Smartphones, Botnets, Toolkits, National Security Policy.*

I. 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. 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.

II. SOCIAL NETWORKING AND ELECTRONIC COMMERCE (E-COMMERCE) APPLICATIONS:

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 (Facebook, Twitter, Google+) are another loophole for cyber attackers to gain personal data from unsuspecting users (Ruggiero, 2011). Social networking sites are host to a surplus of personal data. That is why malicious applications that use social networking sites to steal data yield severe consequences. Recently, M-Commerce or "mobile e-commerce" has gained popularity in our society. Many smartphone users can now conduct monetary transactions, such as buying goods and applications, redeeming coupons and tickets, banking and processing point-of-sale payments. 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.

III. 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 . 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.

IV. CHALLENGES WITH A MOBILE BROWSER:

One cyber security challenge for mobile devices is the screen size. For example, web address bars (which appear once the user clicks on the browser app) disappear after a few seconds on a smartphone because of the small screen size . 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 browsers. 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.

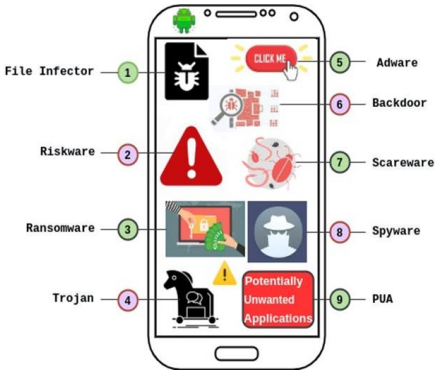
V. COMMON MOBILE DEVICE OS – IOS AND LINUX:

Apple debuted iOS, or iPhone OS, in 2007, with the inception of the iPhone to the cell phone market. Presently, the iOS platform not only runs on iPhone but also iPod Touch and iPad. 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". 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". This mechanism employs policy files that restrict access to certain device features and data . App developers use registered ApplicationProgramming Interface (APIs) to restrict apps from accessing protected resources . 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".

VI. MALWARE ATTACKS ON SMARTPHONE OS:

Along with this, malware that targets smartphone operating systems is constantly evolving. An example of this is seen with "Zeus-in-the-Mobile" (ZitMo), a specific form of malware common to the Android operating system. ZitMo targeted Android users' bank apps; it attempted to bypass the banking two-factor authentication, steal credentials and gain access to users' bank accounts, and ultimately money. 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

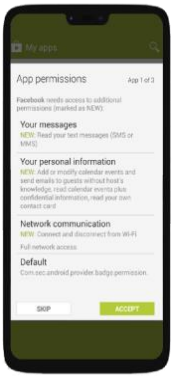
vector for targeting network and critical systems. According to the report, smartphones are an excellent way to spread malware because phones are great storage devices. A hypothetical example of a cyber attack against a company's network is seen when malware is implanted in a smartphone.



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.

VII. THE ANDROID PLATFORM :

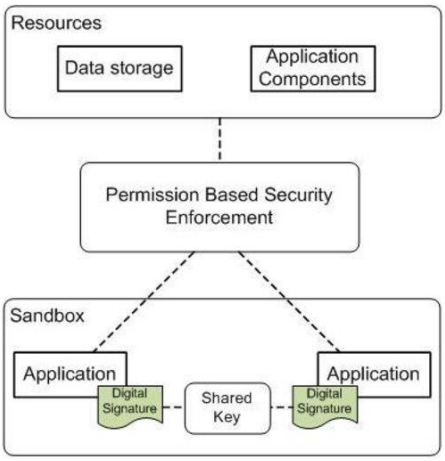
Android is an opensource application execution environment that includes an operating system, application framework, and core applications. Android was designed and released originally by Android Inc. to provide a user-friendly, open, and easy-to-use mobile-based development environment. This open-source 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.

VIII. THE ANDROID SECURITY MODEL:

Android is a multi-process system where each application (and parts of the system) runs its own process. The standard Linux facilities enforce security between applications and the system at the process level; those applications are assigned by users and group IDs. Applications are restricted in what they can perform by a permission mechanism, called permission labels, that uses an access control to control what applications can be performed. This permission mechanism is fine-grained in that it even controls what operations a particular process can perform. 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 PayPalservice in this case is an application that asserts permissions that must be granted to the other applications that use its interfaces". 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.

IX. STEPS TO PROTECT MOBILE PHONE:

- When choosing a mobile phone, consider its security features:
- Configure the device to be more secure:
- Configure web accounts to use secure connections:
- Do not follow links sent in suspicious email or text messages:
- Limit exposure of your mobile phone number:
- Carefully consider what information you want stored on the device:
- Be choosy when selecting and installing apps:
- Maintain physical control of the device, especially in public or semi-public places:
- Disable interfaces that are not currently in use, such as Bluetooth, infrared, or Wi- Fi:
- Set Bluetooth-enabled devices to non-discoverable:
- Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots:
- Delete all information stored in a device prior to discarding it:
- Be careful when using social networking applications:
- Do not "root" or "jailbreak" the device:

X. 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.

REFERENCES

1. S. J. Alsunaidi and A. M. Almuhaideb, "Security Methods Against Potential Physical Attacks on Smartphones," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769458.

2. D. Teixeira, L. Assunção and S. Paiva, "Security of Smart HomeSmartphones Systems," 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain, 2020, pp. 1-5, doi: 10.23919/CISTI49556.2020.9141025.

3. Madhavi LathaChalla and K.L.S.Soujanya, 2021. Secured smart mobile app for smart home environment. [online] Volume 37, Part 2(ISSN 2214-7853), pp.2109-2113. Available at: <https://www.sciencedirect.com/science/article/pii/S22147853203564 67> [Accessed 11 March 2021].

4. Z. Zahid, A. Haider, N. Sabahat and A. Tanwir, "Vulnerabilities in Biometric Authentication of Smartphones," 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan,

2020, pp. 1-5, doi: 10.1109/INMIC50486.2020.9318094. 5. Marion Lara Tan, Raj Prasanna, Kristin Stock, Emma Hudson-Doyle, Graham Leonard, David Johnston,Mobile applications in crisis informatics literature: A systematic review,International Journal of Disaster Risk Reduction,Volume 24, 2017, Pages 297-311, ISSN 2212- 4209, https://doi.org/10.1016/j.ijdrr.2017.06.009 .

6. Yan, Ping. (2018). A survey on dynamic mobile malware detection. Software Quality Journal. 26. 1-29. doi: 10.1007/s11219-017-9368-4.

7. Goel, Diksha & Jain, Ankit. (2017). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. Computers & Security. 73. doi: 10.1016/j.cose.2017.12.006.

8. PMD Nagarjun and Shaik Shakeel Ahamad, " Review of Mobile Security Problems and Defensive Methods," 2018 International Journal of Applied Engineering Research ISSN 0973-4562, Volume 13, Number 12 (2018) pp. doi: 10256-10259.

9. Ibrahim Osman Adam, MuftawuDzang Alhassan, The effect of mobile phone penetration on the quality of life, Telecommunications Policy, Volume 45, Issue 4, 2021,102109,ISSN 0308-5961, doi.org/10.1016/j.telpol.2021.102109.

10.Y. Wang, C. Hahn and K. Sutrave, "Mobile payment security, threats, and challenges," 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), Gainesville, FL, USA, 2016, pp. 1-5, doi: 10.1109/MOBISECSERV.2016.7440226.

11. Ahmed, Lawal &Cavus, Nadire. (2019). DETECTION AND PREVENTION OF SOCIAL MEDIA CYBERCRIME AMONG STUDENTS. 3773-3779. doi: 10.21125/edulearn.2019.0977.

12. Butler, Rika. (2020). A systematic literature review of the factors affecting smartphone user threat avoidance behaviour. Information and Computer Security. 28. 555-574. doi: 10.1108/ICS-01-2020-0016.

13. K. Karimi and S. Krit, "Smart home-Smartphone Systems: Threats, Security Requirements and Open research Challenges," 2019 International Conference of Computer Science and Renewable Energies (ICCSRE), Agadir, Morocco, 2019, pp. 1-5, doi: 10.1109/ICCSRE.2019.8807756.

14. Faris Auid Alharbi, Abdurhman Mansour Alghamdi, Ahmed S Alghamdi (2021). "A Systematic Review of Android Malware Detection Techniques". International Journal of Computer Science and Security (IJCSS), Volume (15): Issue (1): 2021.

15. Milad TalebyAhvanooey, Qianmu Li, Mahdi Rabbani, Ahmed Raza Rajput. (2017). "A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks". International Journal of Advanced Computer Science and Applications, 8(10), p.2017. doi: 10.14569/IJACSA.2017.081005.