ANDROID DEVICE ATTACKS AND THREATS

A Manisha Yadav[1], Dr. B. Indira Reddy[2]

[1]Student, Dept. of Information Technology, Sreenidhi Institute of Science and Technology, Telangana, India
[2]Professor, Dept. of Information Technology, Sreenidhi Institute of Science and Technology, Telangana, India

Abstract: *In this modern era, people believe that a mobile is everything. Each and every person has a mobile phone most preferably a smart phone. Anything and everything available on the web can be accessed from anywhere by anyone possessing a smartphone. This has widely reduced the use of Personal computers for simple things as it has been replaced by a simple and small smartphone. In each and every act of a person a mobile is involved in some or the other way. Mobiles were traditionally used for communicating with people. But now a mobile has replaced the role of a camera, radio, iPod, play stations etc. Mobile devices are also used for financial transactions by making use of mobile wallets and applications involving online banking. Thus, a mobile device has almost all every sensitive information about the user. It is very important that the device and the information contained on the device is secured. Even a simple reckless attitude from the user can result is security attacks as most of the information is available on the device. In this paper we present the details about Mobile technology, Android operating System, different types of attacks and the threats recognized by the potentially harmful applications*

Key Words: Mobile technology, Android, BYOD, Kernel security, Linux security, Application security, PHA.

Introduction:

Mobile Technology was a mystery few years ago. But now, mobile technology is a noteworthy achievement in the world of technology. When mobiles were first introduced, they were fundamentally used for calls, SMS and games. But now this rapid growing technology and portability of the mobile devices has made an evolution into a digital world and made life and business much easier. The functionalities of a mobile device have been increased. The mobile devices are equipped with internet connectivity through which one can gain information from anywhere in the world. The mobile has made it possible to transfer file via Bluetooth and WIFI. It has also made it possible to locate places on the globe and also navigate to the places using the Global Positioning System (GPS). It is now easy to catch up with the entertainment comfortably from your home. Mobile technology has its own importance in the business World. With the use of Mobile technology marketers are now able to sell their products online with ease and comfort. The availability of many Operating systems for smart phones all of which have their own unique characteristics is the important fact behind the diversity of mobile technology. Android, blackberry, webos, iOS, Symbian windows are some of the mobile operating systems. The Android operating system developed by google is the very commonly used operating systems in smart phones which uses simple touch gestures for the operations. Android is the first and the only open source Operating system with the ability to be ported to any cellphone. Mobiles are very important in case of emergencies. They have made communication much easier and has been connecting people throughout the world.

Mobile technology has reached miles in a short span. While these devices offer many functionalities and internet connectivity, they also have security risks. More and more data is generated everyday with the use of mobiles at home, work places, storing, sharing and accessing huge amount of personal and corporate data. More amount of data will be more danger with mobile devices. Now-a-days cyberattacks on mobile devices have become more common. There are two may causes of data loss on mobile devices. Physical device loss and misuse of the mobile applications. The physical devices are not only holding huge amounts of data but also have our identities attached which when lost can lead to data breach.

Mobile Devices at workplace:

There has been a massive influx of mobile technology into the workplace. And now mobile security is of great importance to almost every company. Almost all workers access the corporate data from smartphones and tablets. This is nothing but possessing sensitive information in wrong hands. The policy of Bring your own devices (BYOD) is an increasing trend of employees bringing their own devices to the workplaces. These devices include smartphones, tablets, laptops and USB drives. These devices are sometimes sanctioned by the company and some are owned by the employee. Regardless of whether these devices are supported or not at the workplace, they pose security risks to the organization when connected to the corporate network or by accessing corporate data. This leads to corporate data breach. The cost of this is whopping and is estimated to be increasing more and more every year.

Mobile Device Security:

[1]Over 50% of the business PC's are mobiles and these devices possess new challenges to network security. So, IT has to develop its security. A full protection of data on the mobile devices and the network to which it is connected is important. This is called as Mobile device security. With all the available functionalities, mobile devices are vulnerable and susceptible to online threats and physical attacks[2]. Security threats to such data could include malware like worms unauthorized access, spyware, phishing and theft. Surfing the web, booking appointments, setting reminders, sharing files, video calling instant messaging and mobile banking are few day-to-day activities which possess our personal data and identity and the loss of this data would have devastating results. So, we need to minimize the exposure of our mobile devices to such threats

Threats:

The following are the few security threats that one should have an eye on.

1. Data breach:
   It is the very basic and troublesome threat in almost every field. It is the release of secure and confidential information to an untrusted person or environment. The attackers will have unauthorized access to databases with sensitive data, steal the data of the customers or the users contained in those databases. Data breach is a consequence of cyberattack. By the time you are aware of the data loss the damage is already done.
2. Social Engineering:
   It is an attack which involves tricking the people and gaining sensitive information by interacting with the user. Social engineering is one of the greatest threats Organizations are facing. The data an attacker gains by this is used for gaining access to the systems and for the carrying out cybercrimes.
3. Wi-Fi interference:
   The Network through which a mobile device transmits the data defines the security of the device. A mobile device is as secure as the network to which it is connected. Connecting to the public networks and open WI-FI networks will lead to Man-in-the-middle attacks. So, it is very important to know to which network is the device connected and also ensure if the connected network is safe or not.
4. Out-of-date devices:
   When an out of date device is connected to the network it is prone to many inherent risks and security vulnerabilities. With the changing technologies and the security software and policies it is very important that the mobile device is updated regularly and is up to date. The extensive use of mobile platforms leads to data breach. Thus, it is important that the Out-of-date devices are not used.
5. Cryptojacking attacks:
   Cryptojacking is an attack wherein an attacker gains Cryptocurrency b illegally mining someone else's computer. The victim is forced to click on a malicious link in the email by the hacker. On clicking the link, a crypto mining code is being loaded on to the victim's computer. The code auto executes on the victim's browser. The victim finds no sign of the attack except the slower performance of the system or lags in execution. Now this attack is on rise. The Percentage of cryptojacking has been growing as it doesn't require significant technical skills.
6. Poor password hygiene:
   Password provides authorization to the mobile device. It is very important the device is protected with a password as it is the very basic security feature. It is also important that the password used is a strong one that cannot be easily identified by brute force. The password should not lead to birthday attack. It is important to maintain a strong and secure password.

These are the important threats one should be aware of to limit the mobile malware.

Android:

Android is one of the most widely used open source Operating system. It offers an endless combination of software and hardware. Android was developed on the open Linux Kernel. It was designed to optimize memory and hardware resources in a mobile environment. It provides access to wide range of useful libraries and tools that can be used to develop applications.

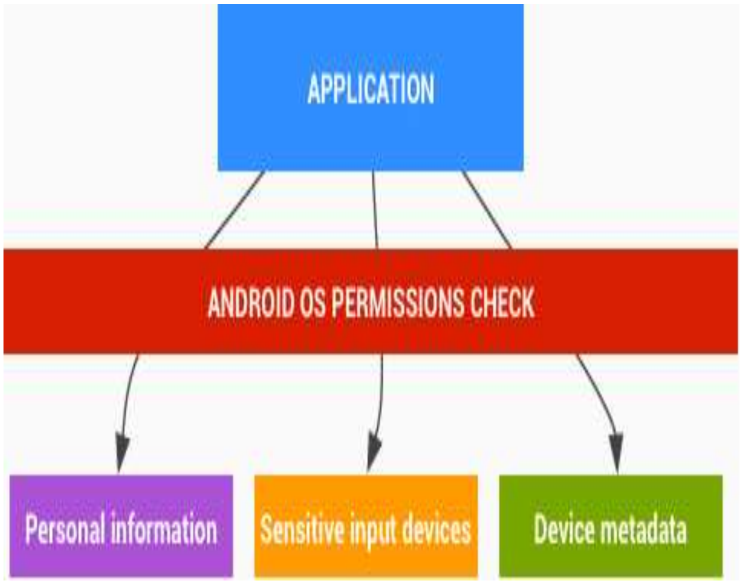
Android is backed by Google. It has layered Security. Each part of the android ecosystem works together to build a strong defense mechanism. Security starts at the application layer with the built-in malware defense. The google play protect[5] automatically scans all the apps on Android phones and prevents harmful apps. Regular security updates keep everything in order.

Overview of Android Security:

1. Kernel Security:
   To empower secure communications between the applications running in different processes, an inter process communication (IPC) facility has been enabled at the operating system level by the Android platform. These security features at the OS level ensures that the code is the result of comprised application behavior or an exploitation of an application vulnerability. It is intended to prevent applications from harming the device.
2. Linux Security:
   It is the foundation of Android platform. Linux is the stable and secure kernel trusted by many security professionals. Linux Kernel offers Android with several key features like 1. User based permission model 2. Process seclusion 3. Extensible mechanism for secure IPC 4. Removal of unnecessary and insecure parts of kernel.
3. System Partition and Safe Mode:
   The android Kernel, Operating system libraries, application framework and the applications are included in the system partition. System partition is in Read only mode. When the safe mode is switched by the user, the third-party applications can be manually launched by the user but not by default.
4. Cryptography:
   A set of cryptographic APIs for the applications have been provided by Android which include AES, RSA, DSA, SHA.
5. Password Protection:
   Unauthorized use of the mobile device can be prevented by configuring the Android to authenticate a user specified password prior to providing access to the device. The cryptographic key for the full filesystem encryption can be protected by using password.

Application Security:

Any access to sensitive data is available only through protected APIs. If any third-party application that is installed by the user on the device wishes to share the information accumulated by it can seek the android OS permissions check to protect the data. Upon installation few applications will request user’s information. Even these requests also pass through the permission checks.



Application Verification:

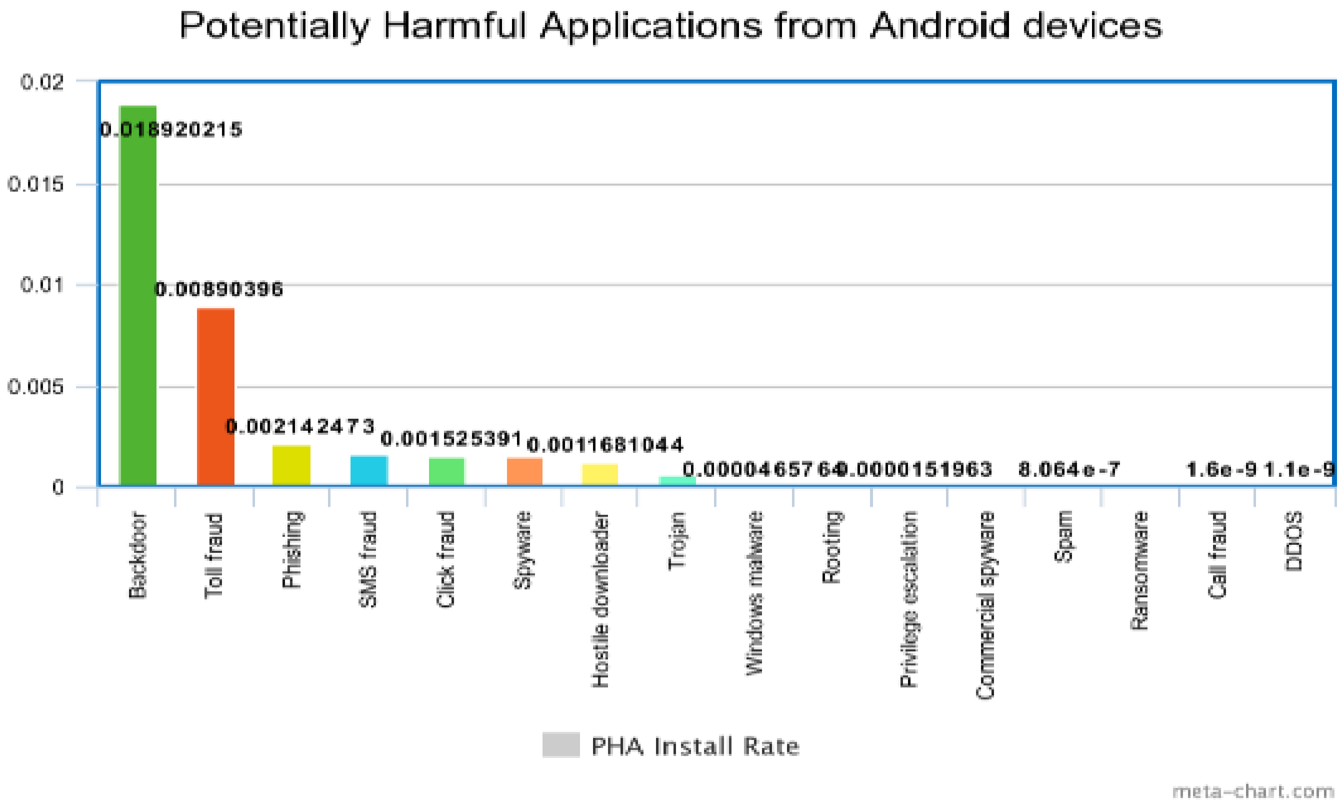
Android application verification is performed by the google play protect. Users can enable "Verify Apps" and then a user can perform application installation of verified apps. If the application is found to be bad or malicious then the user can block installation.

Removing Potentially Harmful Applications (PHA):

PHA's on the android devices can be detected and removed by google play protect. This is done by the following:

- Online and Offline scans of regularly scheduled and on demand PHA.
- Disabling PHA threats automatically.
- Scanning of the new apps being uploaded into the cloud.
- SafetyNet signal detection.
- Machine learning models.

Even after having many inbuilt security features many PHA have been recorded and the following are the attacks being recorded by Google play protect.



Attacks:

The following are the attacks caused by the Potentially Harmful Applications which are installed on to the mobile devices.

1.Backdoor:

A backdoor is an unauthorized remote access by the hacker to install malware into the device to exploit the vulnerabilities. The backdoor virus is hidden and run on the background making it quite difficult to detect. This works making use of DoS attack. By installing few malicious apps containing the hidden code on to the mobile devices leads to backdoor attack.

2. Toll fraud:

Toll fraud is also called as VoIP fraud. The hacker takes control of a mobile device, access the phone system and makes fraudulent calls from the victims account. This fraud is also called as International Revenue Sharing Fraud. The revenue obtained by the information from the Premium Rate numbers is shared by the International Premium Rate Number providers and the Fraudsters.

3. Phishing:

By phishing the attacker tries to obtain sensitive information and personal details like Username, Passwords and credit card details and then attempts a fraud through electronic communications. The attackers after performing phishing will try to impersonate banks. It is important to download the apps from the authorized vendors to prevent phishing.

4. SMS fraud:

SMS Fraud is nothing but phishing by sending fraudulent SMSs. This is also called Smishing. For example, a fraud sends message to the victim as if the message is from a bank or from IT department and then lure the victim to call him back. Smishing by initiating prize money, lottery, job offers etc. which are fraudulent.

5. Click fraud:

Many a times one comes across advertisements while surfing the web. The user is forced to click the advertisement to continue his work. In this way the user illegally clicks on the website or the advertisement. The Owners of the websites are paid an amount of money which is determined by the number of clicks or by the number of the visitors who click the ad or view the website.

6.Spyware:

Any Malware, malicious software or code which is designed to gain access or to damage the computer and steal the browsing data and sensitive information is called Spyware[4]. Spyware include Adware, Trojans, Keystroke loggers etc. Any spy app on the mobile device can monitor and record the outgoing and incoming calls, SMSs, MMSs, GPS tracking, Images, Social networking sites etc.

7. Root exploits:

Rooting an Android device is called root exploits or jailbreaking an iOS device. It is another way that mobile malware uses to infect devices. Such exploits give a user or application superuser privilege to the attacker which allows him to download all sorts of applications, many of which are either malware or have been diseased by malware. The attacker is provided with full access to the device remotely without user knowledge.

Conclusion:

Security solutions for mobile devices and smartphones must defend against viruses, malware, botnets, intrusion attacks, threats amassed through the deployment of a wide spectrum of mobile applications, and attacks that are specific to mobile devices.

Due to the explosion of mobile device deployment in the enterprise environment—that those research activities have truly focused on solving real-world security challenges.

References:

[1]. M. Becher et al., "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," Proc. 2011 IEEE Symp. Security and Privacy, IEEE CS, 2011, pp. 96–111.

[2] T. Vidas, D. Votipka, and N. Christin, "All Your Droid Are Belong to Us: A Survey of Current Android Attacks," Proc. 5th Usenix Conf. on Offensive Technologies (WOOT 11), Usenix, 2011, pp. 81–90.

[3]T. Luo et al., “Attacks on WebView in the Android System,” Proc. 27th Ann. Computer Security Applications Conf. (ACSAC 11), ACM, 2011, pp. 343–352.

[4]. A. Porter Felt et al., “A Survey of Mobile Malware in the Wild,” Proc. 1st ACM Workshop Security and Privacy in Smartphones and Mobile Devices (SPSM 11), ACM, 2011, pp. 3–14.

[5]. "Number of Google play store apps 2016 | statistic," Statista, 2014. [Online]. Available: http://www.statista.com/statistics/266210/number-ofavailable-applications-in-the-google-play-store.

[6]Android Vulnerability Statistics, http://www.cvedetails.com/product/19997/GoogleAndroid.html?vendor_id=1224

[7] Keman Huang, Jia Zhang, Wei Tan, Zhiyong Feng, “An Empirical Analysis of Contemporary Android Mobile Vulnerability Market” International Conference on Mobile Services IEEE 2015

[8]Android Vulnerability NVD Results https://web.nvd.nist.gov/view/vuln/searchresults?adv_search=true&cpe=cpe%3A%2Fo%3Agoogle%3Aandroid

[9]OSVDB, https://blog.osvdb.org/category/vulnerability-databases/

[10]CVE-ID Syntex, https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

[11] Darko Hrestak, Stjepan Picek, Željko Rumenjak, “Improving the Android Smartphone Security against Various Malware Threats” MIPRO 2015, 25- 29 May 2015, Opatija, Croatia.

[12] R.Dhaya, M.Poongodj, “Detecting Software Vulnerabilities in Android Using Static Analysis” 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[13] V. Savov, "Only 7.5 percent of Android phones are running marshmallow," The Verge, 2016. [Online]. Available: http://www.theverge.com/circuitbreaker/2016/5/4/11589630/ android-6-marshmallow-os-distribution-statistics.

[14] "Normal Permissions,". [Online]. Available: https://developer.android.com/guide/topics/security/normalpermissions.html.

[15] "Dangerous Permissions,". [Online]. Available: https://developer.android.com/guide/topics/security/permissions.html#normal-dangerous.

[16] J.-K. Park and S.-Y. Choi, "Studying security weaknesses of Android system," International Journal of Security and Its Applications, vol. 9, no. 3, pp. 7–12, Mar. 2015.

[17] "Smartphone users worldwide 2014-2020 | statistic," Statista, 2016. [Online]. Available: https://www.statista.com/statistics/330695/number-ofsmartphone-users-worldwide.

[18]Jeon, Woongryul, et al. "A practical analysis of smartphone security." Human Interface and the Management of Information. Interacting with Information. Springer Berlin Heidelberg, 2011. 311-320.

[19] Mylonas, Alexios, et al. "Smartphone security evaluation the malware attack case." Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on. IEEE, 2011

[20] Enck, William, et al. "A Study of Android Application Security." USENIX security symposium. Vol. 2. 2011.

[21] Lu, Long, et al. "Chex: statically vetting android apps for component hijacking vulnerabilities." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.