International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 10, pp: 92-94 www.ijaem.net ISSN: 2395-5252

Case Study On Mobile Device Security On Different Os

Vikash V, Gokul J, Aathish M,

Dr.M. Sujithra M.C.A, M.Phil., PhD, Dr.A.D. Chitra M.C.A, M.Phil., PhD,

2 nd Year, M.Sc. Software Systems, Computing Department
Coimbatore Institute of Technology,
Coimbatore
sujithra@cit.edu.in Assistant Professor,
dchitra@cit.edu.in Assistant Professor,
Department of Data Science, Department of Software Systems,
Coimbatore Institute of Technology, Coimbatore Institute of Technology,
Coimbatore Coimbatore

Date of Submission: 20-11-2020 Date of Acceptance: 03-12-2020

ABSTRACT: This paper provides an overview of the mobile device security and identifies the challenges in it. The sudden increase in smartphone malware has become one of the most serious security problems. The Android platform has taken amajor and unique position in smartphone environment, the number of Android malware has grown sequentially. This rise in malware is primarily referable to the occurrence of variants of existing malware. A convenient technique for defeatingmalwareistheuseofsignature matching which is efficient from a time perspective but not very practical because of its lack of resistance against the malwarevariants.

KEYWORDS: Mobile Device Security, Malware, OS updates, Android, iOS

INTRODUCTION

Mobile device security encloses the overall mobile ecosystem including endpoint device and data security, WiFi and cellular communications, and the secure access to undertaking applications and data.It also encloses the secure development, testand delivery of applications through web sites andapp stores. This paper is organized into sections, each of which describes a major area of concern in mobile devicesecurity.

WHAT IS MOBILEDEVICE SECURITY?

Mobile Device Security refers to the measures made to protect sensitive information stored and transmitted through laptops, smartphones, tabs, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the undertaking network.

Why Is Mobile Device Security Important?

Nearly more than a half of the business PCs, mobile, portable devices face **d**istinct challenges to network security, which must be the reason for all of the locations and uses that employees require of the company network.

There are many threats to devices include harmful mobile apps,scams, data leakage, and unsecure Wi-Fi networks. On top of that, undertakings have to account for the possibility for an employee losing his/her mobile device or the device being stolen. To avoid a security breach, companies should take proper, preventative steps to reduce the risk.

MALWARE AND APP STORES

Respectively, Android apps can be downloaded from third-party app stores and through web sites and there is no control of digital certificates used to sign Android apps. Consequently, it is easy to hijack it, inject code intoit, re-sign it, and redistribute it.Distributing apps through appstoresis expected to prevent the introduction of malware through effective and cross-check mechanisms. The Apple I Store recently distributed many malicious apps created by XcodeGhost, theallarelistedontheApple website.

SECURE STORAGE

Mobile devices are used in unique ways thatmakeitdifficulttosecurelystore data. Aimportant challenge for encrypting data is its key storage. On

mobile devices, the encrypting key needs to be available for the user to access the data. Storing an encryption key on a remote server generally does not solve the problem, as an attacker who has access to the device can easily request the encryption key from the server and decrypt it.
Most mobile devices make use of some method of passcode or password which is used in a codedsecure way to derive an encryption key that is then used to encryptit.

SECURE COMMUNICATIONS

Secure communication is when two entities are communicating and do not want a third party to hearit. For thisreason they need to communicate in a way not an easy target to interception. Other than spoken face-to-face communication with no possible overhear, it is probably safe to say that no communication is guaranteed secure in this sense, although practical obstacles such as law enactment, resources, technical issues , and the complete volume of communication serve to limit surveillance.

MOBILE OS UPDATES

Installing the latest mobile OS version is important for device security.Asa result, newer OS versions are more resistant to misuse. Many Android devices have a long supply chain, which makes set up the OS updates a slow and uncertain process. For a device running Apple iOS, Apple releases the iOS update for the device and the customer is notified that the update can be installed. For most Android phones, the customer should wait for Google to patch the importantAndroid OS, for the device manufacturers it takes the stock Android OS andcustomizeitfor theirplatform.

SECURE CODING

Vulnerabilities in mobile devices are frequently the result of insecure coding practices. Android's Stage fright engine is a media playback service for Android which contains multiple vulnerabilities that allow a remote attacker to access files or even execute code on the device.

Other attack modes include: web browsers, downloads, email, Bluetooth, SD card, Picture Transfer Protocol, gallery, and possible others .

MOBILE MALWARE EXAMPLES

DroidDream(Android)

- Nearly62 apps uploaded to Google appmarket
- Send credentials tothose attackers

Ikee (iOS)

- Worm capabilities
- Worked only on breakoutphones with SSH installed.

Zitmo (Symbian,BlackBerry,Windows,Android)

- Propagates through SMS; claimstoinstall a “security certificate”
- CapturesinfofromSMS;aimedat defeating 2-factorauthorization
- Timed with user PCinfection

How Does Mobile Device Securitywork?

Securing mobile devices requiresa multi-layered approach in undertaking solutions. While there are key elements to mobile device security, each organization needs to find what is the best fits itsnetwork.
To get started, here are few mobile security best practices:

1. **Establish, enforce, and share clear processes and policies**

Mobile device security must include clear ruleson:

- What devices can beused
- Allowed OSlevels
- What the company can andcannot

access on a personal phone

- Password requirements andfrequency

for updating passwords

2. Password protection

One of the most basic ways to prevent unauthorized access to a mobile device is to create a strong password, and yet weak passwords are still a constant problemthatcontributetothemajorityof data hacks. Another common security problem is workers using the same password for their email, mobile device, and every work-related account. It is critical that employees create strong, unique passwords and create different passwords for differentaccounts.

3. Biometrics

Instead of standing on traditionalmethods of mobile access security, such as passwords, some companies are looking to biometrics as a safer alternative. Biometric authentication is when a computer uses measurable characteristics such as face, fingerprint, voice, or the iris recognition foridentification and access. Multiple biometric authentication methods arenow available on smartphones and are easy for workers to set up and use.

4.Avoid publicWi-Fi

A mobile device is only as secure as the networkthroughwhichittransmitsdata. It’s the companies responsibility to develop employees about the cons of using public Wi-Fi's, which are being a at risk to attacks from hackers who can easily breakout a device, access the network, and steal data. The best defense to be done is smart user behavior and prohibit the use of open Wi-Fi networks.

4. Beware ofapps

Harmful apps are some of the fastest growing threats to mobile devices. When an employee without his/her knowledge downloads one, either for work or personal reasons, it provides unauthorized access to the company's network and data.

To combat this rising threat, companies have two options: instruct employees about the dangers of downloading unapproved apps, or ban employees from downloading certain apps on their phones altogether.

5. Mobile deviceen cryption:

Most mobile devices are bundled with a built-inencryptionfeature.Usersneedto locate this feature on their device and enter a password to encrypt their device. With this method, data is converted into a code that can only be accessed by authorized users. This is important in case of theft, and it prevents unauthorizedaccess.

Different Mobile Os And Their Security platforms:

ANDROID OSSECURITY

- Android security has a questionable security reputation, mainly because no one owns it. In other words, no one regulates whatcanorcannotbeofferedasan Android app, or even what can be sold as an Android phone.
- Fortunately, Google constantly works to provide security to Android users. Here, the users can have their own control overtheir own security and privacy by modifying theAndroid.

APPLE IOS SECURITY

- Apple's iOS mobile operating system is tightly controlled by Apple itself, which also tightly controls the apps available in the Apple App Store.
- Additionally,theclosedecosystem only permits apps that don't access the phone's root coding, which reduces both the need for iOS antivirus and makes an iOS antivirus impossible to create for App Storeapproval.

WINDOWS OS SECURITY

- Windows Phone also has a degree of centralized control, but has a history of security weaknesses, though its performance is improving as more and more users are comingonboard.
- Previous phone hardware models are not developed anymoreeither, leaving the market void of any security fixes for existing products. With the future of new Windows phone products in question, there is currently no established security upkeep for the platform.

REFERENCES:

WEBSITES

- https://www.sciencedirect.com/science/article/pii/S0167404815000188
- https://www.kaspersky.com/resource-center/threats/android-vs-iphone-mobile-security
- https://www.cisco.com/c/en_in/solutions/small-business/resource-center/security/mobile-device- security.html

BOOKS:

- **Wireless and Mobile DeviceSecurity**

By Jim Doherty

- **Mobile Security and Privacy:Advances, Challenges and FutureResearchDirections**

By Man Ho Au and Raymond Choo