International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

An Overview On iOS-14 Security and Study on Previous Attack On iOS

Siddharth Singh[1], Shubham Randive[2]

[1,2]*Student, Semester-IV, MSC(I.T.), Keraleeya Samajam's Model College, Dombivali East, Thane, Maharashtra, India*

Abstract - *In today's world, the iphone is the most overrated and over hyped mobile phone in the world. Mostly iOS security is been concerned to be the best for mobile phones for many mobile users comparing to android devices in the world. I have also discussed about the various new security features of iOS-14 related to application tracking, wifi security,etc. Some of the most concerning malwares attack, jailbreaking techniques and it's effect on the user have been discussed later in this paper.*

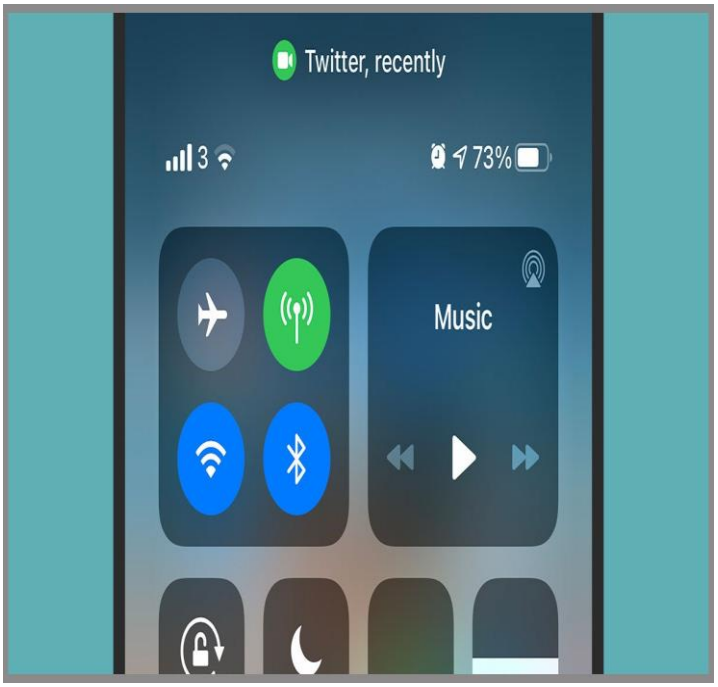
Key Words: Overview of iOS; Security features; camera and microphone tracking; wifi tracking; various malware attack; jailbreaking;

1. INTRODUCTION

The rise in demand for iphone is growing every day in the world, and the sale of iphone in the year 2020 was approximately 3.1 million in india alone and expected sale in india for the year 2021 is about 3.5 million. Since, demand for the iphone is increasing rapidly because of the operating system of the device called as iOS. The latest version of the operating system is iOS-14.4.2 which was released on march 26,2021 which is created and developed by Apple Inc. In today's life, the most important and concerning service which each and every user requires is 'security and privacy'. The privacy and security in iOS devices are considered to be the best with respect to the android devices in the world. Their are various researches conducted between these two operating systems which clearly shows that iOS is much more stable and secure. But their is a chance of our iOS device to get hacked through various techniques by an attacker. The hacker group known as 'Antisec' have released the records of one million hacked iOS device user so that, each and every people will know that not even iOS devices are completely secure. The jailbreak technique which allows the user to get access to various User Interfaces, altering the root access, changing the security patches of their device or getting the latest iOS version for the device which apple has not included in the some of their very old iphone model like iOS-14 not available for iphone 6 or below models. The various risk associated with jailbreaking has been explained later in this paper.

2. SECURITY FEATURES OF iOS-14

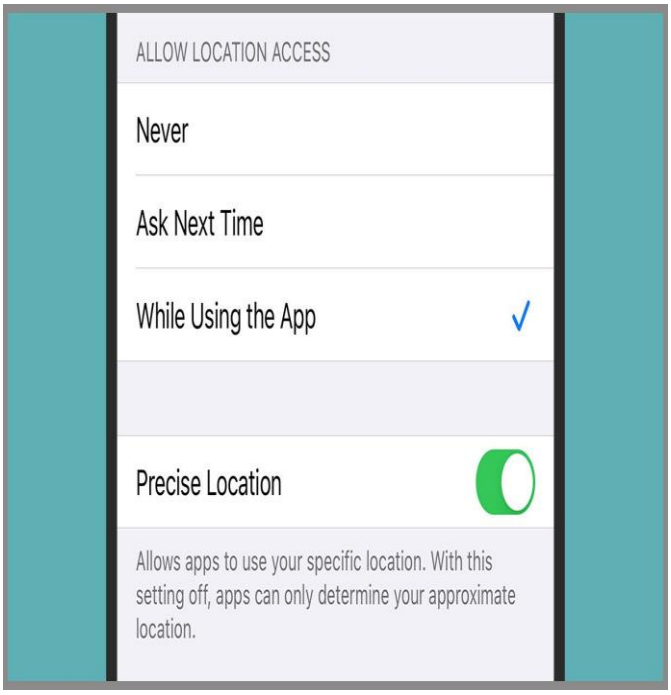
2.1. Know when the applications uses camera and microphone: Application working on iOS-14 operating system have to ask for the permission for the use of camera and microphone. An dotted indicator is displayed on top of the screen whenever any of this functions are running on system. Indicators for camera is in green colour and orange colour for microphone. This feature allows the device user to get consent from system about the camera or microphone permissions even after the user has trusted the application to give the access to camera and microphone. All the information is been recorded about the camera and microphone from the applications inside the control center.

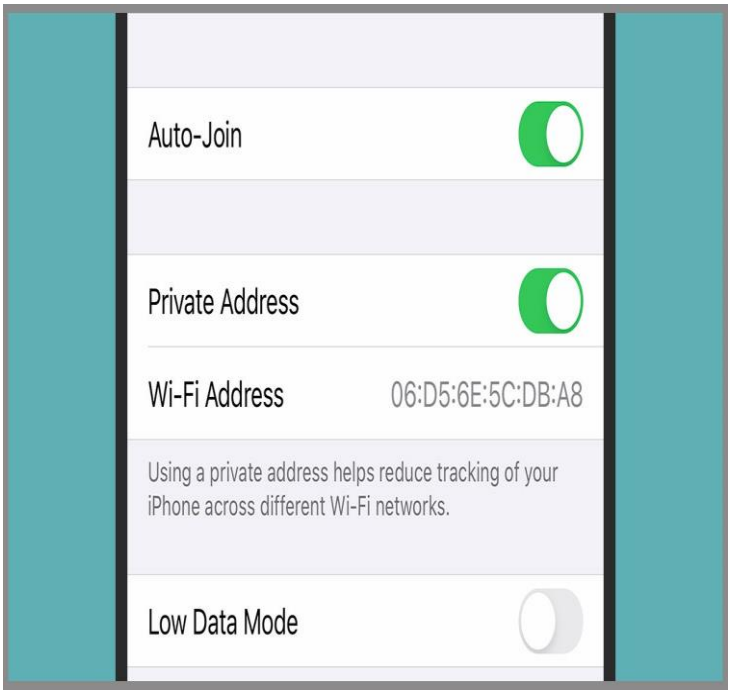


2.2. Limited access to location and photos: A new feature is been added to iOS-14 that gives application a certain permissions but only up-to certain limitation. Since, most of the user nowadays trust certain application more which can be a serious security concern like viewing the photos or tracking the location of the device.

But this issue can be overcome by iOS-14 setting known as 'Privacy and Location Services' and then select app configuration then select access your phone's location and you can then change the permissions. A new 'Precise Location' toggle switch is added which gives the exact GPS co-ordinates and the user can turn off this feature to hidden their exact GPS co-ordinates.

For photos security select the same privacy option and the user can give the application permission only within sub folder to read/write the photos and not the entire photo album. This feature makes the trusted application to view that photos only which user have given permission to view.





2.3. Sniff Out Bad Passwords: Apple synchronize all the password and other login credentials from every account in the device via iCloud. A user can view all the login credentials in the device cloud service since, iOS-14. A new feature called as password monitoring system, this feature helps to monitor if any of this login credentials is been spotted in a data security breaches, which means the account is been compromised and need to change the password for that account. Security Recommendation will help with password related problems.

2.4. Discourage WiFi Tracking: A small and significant feature is added to WiFi security in iOS 14 known as 'Use Private Address'. This features give the device a different MAC Address so that the Internet Service Provider have difficult to track the activity and this feature is enabled by default for new WiFi network which gets connected on the device.

2.5. Know When 3rd Party Apps Snoop on Your Clipboard:

In iOS-13, it was discovered that 3rd party apps can easily access your device's clipboard but this issue has been rectified in iOS-14. Whenever an application reads the information on clipboard, iOS-14 pops up a notification stating that which application has accessed the clipboard of your device. This feature helps the user to understand that whether an application has accessed the crucial data of the user without the user's consent.

3. PREVIOUS MALWARE ATTACKS ON iOS DEVICES

3.1. Trustjacking: Trustjacking is a malware reported by a user to apple in mid of july 2017. Trustjacking records all the information of an iOS device through the infected computer when both the devices are connected to a same wifi network after trusting the infected computer. iOS devices always ask to whether trust the computer or not but, people who wants to exchange the data or media they trust this device which makes the user to fall in the trap of the attacker. The most of the time infected computer can be the user's machine which is been infected remotely by an attacker to steal the user data. Various confidential information like credit/debit card details, bank details, ID and password of various accounts can be viewed by the attacker.

3.2. AceDeceiver: AceDeceiver is type of man in the middle(MITM) attack which was created around jan 2014. This attack was operated on iOS devices which were not jailbroken. This attack was the first to exploit the design flaws in apple's DRM mechanism. The attacker first uploaded the legitimate apps to the app store and had managed to bypass the apple's review process by adding it as a

wallpaper application. After approval from the apple store, the attacker purchase that app from the iTunes to capture the DRM Fairplay authorization code. A client software was developed by the attacker by masquerading it as a helper program for iOS device known as AiSi helper windows. This helper software install multiple copies of the app in the infected iOS devices.

3.3. XcodeGhost: Xcode is an environment used to create various iOS and mac osx apps. XcodeGhost is an infected compiler which was uploaded on baidu website in china. Since, Xcode compiler in china is very much time consuming so the people in china uses various 3rd party sites to download this compiler. XcodeGhost was uploaded on chinese file-sharing site known as baidu. The baidu has removed this malware from their web site. This malware effects was only in china and not over world wide. The apps which were created in this malware has caused largest breach in the apple store.

3.4.Safari Javascript pop-up scareware: Safari javascript pop-up scareware was used by scammers to lock the mobile safari browser to extort the ransom money from iOS device users which get infected by this scareware. In february 2017, a user reported that after visiting a website the user lost the control of it's safari browser and the pop-up was displayed whenever a new tab of the browser was open. Most of the device user accepted the offer of the scammer by sending a code of iTunes gift card worth 100 pounds. But this scareware can be easily removed from the safari browser by clearing history and websites data from the setting menu. This scareware was received by multiple user from phising emails, messages or websites.

3.5. YiSpecter: YiSpecter malware has infected both jailbroken and non-jailbroken iOS devices in china and taiwan. YiSpecter was the first malware that abuses the private APIs in the iOS system to implement malicious activities in the system. This malware can download and install random apps in the user's device and replace it with the user's downloaded apps. This malware can change the safari browser settings and also can hijack other apps so that it can display ads from that apps. This malware can easily hide in the iOS devices by hiding the icon or changing it's name and icon to system apps and system icons, so that the user cannot remove the malware. This malware was running inside many user's device upto 10 months.

3.6. WireLurker and Masque Attack: Wirelurker malware infects both Mac OS-X and iOS devices. This malware uses masque attack(A technique to gather devices information). Wirelurker malware was downloaded from infected mac os computer. The malware installs the trojanised version of common apps like email apps,etc. This malware records all the data from that trojanised apps for example if trojanised version of email app has been installed and the user opens the app to check the email in their phone than all the records of the email will be sent to attacker. This malware was not properly configured by the attacker which makes this attack less dangerous as compared to other malwares.

4. iOS JAILBREAKING

iOS jailbreaking is a technique used to exploit the flaws of the device to get the root privileges and to remove the software restrictions imposed by apple on iOS devices. This techniques helps the user to install software from other sources too. According to apple, jailbreaking is violation of end-user agreement. iOS jailbreaking has a very serious effect on device security as jailbreaking comes with various vulnerabilites included in the device. Some of the iOS user thinks, it's cool to have the root privileges of the system in their hand, as they can do anything with their device they want it to do without knowing the consequences they are going to face in the future. This technique have a various serious security issues which have been faced by multiple users in the past. Most of the software developers jailbreak their devices to learn more about the operating system and to cleanup the device and applications to exploit different vulnerabilities.

5. RISK RELATED TO JAILBREAKING AN iOS DEVICES

5.1. The jailbreaking makes various applications to request root access on the device i.e. if a malware is installed on that device than it can gain the root access and can have complete access to device data. The data can be from banking apps, stored passwords, social media accounts informations, work emails, etc.

5.2. The jailbroken phones comes with various bugs that could make the device to crash many times or disable the various features of the device.

5.3. The device battery life get depleted due to jailbreaking and can damage the device processors or other hardware

5.4. The device warranty gets void and apple store can refuse the repair or servicing of the device.

5.5. The device will be exposed to various threats and malwares which can effect the device security.

6. CONCLUSION

The new iOS-14 comes with enhanced security and privacy features which makes the device more stable and successful in today's world. The various added security features has made the device away from various malware attacks. The iOS-14 have managed to provide the user much more reliable and efficient devices for smooth and flexible use in daily life's. The hardware configuration has managed to increase it's performance with the iOS devices for gaming, camera and other apps. We have also discussed about how the various malware attacks have the effect on the previous devices and how the apple company has managed to

overcome that attack by fixing the vulnerabilites of the system in iOS-14 update.

REFERENCES

[1] https://en.wikipedia.org/wiki/IOS_14

[2] https://www.kaspersky.com/resource-center/definitions/what-is-jailbreaking#:~:text=Jailbreaking%20is%20the%20process%20of,and%20access%20all%20the%20features.

[3] https://blog.securityinnovation.com/jailbreaking-your-iphone-worth-the-security-risk#:~:text=Security%20Risks%20of%20Jailbreaking&text=Jailbreaking%20takes%20away%20the%20safety,and%20disable%20other%20important%20features.

[4] https://www.wired.com/story/ios-14-privacy-security-features/

[5] https://www.moneycontrol.com/news/technology/ipados-14-ios-14-features-app-library-widgets-better-privacy-and-more-5441691.html

[6] https://blog.malwarebytes.com/mac/2019/08/unprecedented-new-iphone-malware-discovered/