Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/14609
DOI URL: http://dx.doi.org/10.21474/IJAR01/14609

RESEARCH ARTICLE

SOK: IS IPHONE ACTUALLY SECURE?

Sanjeev Kumar Paul

Manuscript Info

Manuscript History
Received: 25 February 2022
Final Accepted: 27 March 2022
Published: April 2022

Abstract

iOS is considered a secure operating system that considers privacy as a primary feature for the user. This review is intended to find is it true and can it be sufficient to persuade hardcore Android users.

Introduction:-

Ever since my human brain has developed an interest in technology and cybersecurity, one thing I have always heard has been common regardless of the location, APPLE iPhone is more secure than Android smartphones. The word of mouth is so fiercely strong with such exquisite brand promotion that a simple middle-class smartphone user would think of buyinsg oneonce in his life. I am a fan of Android Smartphones as it brings features such as customizable icons, fonts, and packs. Despite that, iPhone still dominates the American Market and is expanding in other areas of technology.

Apple as a company is not only a pioneer in the innovation but also, holds such a strong presence in the market that other companies will follow suit barring some months of criticism of the move. For example, the move to remove charging adapters (but can be bought on websites separately and in a separate box) to prevent our environment from extra e-waste.

Here, my objective is todeeply understand what Apple does, in terms of security perspective and try to have deeper insight using a few research papers and understand why some cybersecurityleaders recommend this and maybe come up with a few questions for future work.

Launch of iPhone

When in the summer of 2007, it was declared that iPhone would be hitting the market, independent evaluators wanted to check on the device that has acquireda massive chunk of the market for itself. An Evaluation done by {cmiller, jake, josh} AT securityevaluators.comdiscussedthe fact that specific processes have an administrative privilege for smooth operation that can lead to various vulnerabilities. As discussed by Charlie Miller and his colleagues in the paper the iPhone steadily has developed stripped-down versions of its browser and email. And can best describe the security architecture as “Minimize the Attack surfaces”. C. Miller also emphasizes the fact that third party libraries/ applications are prohibited because of no support provided for similar SDKs.

(Mark Stamp, Vaibhav Pandya) discussed in their analysis of the iPhone that although this minimization of attack surface brings a “closed” environment, it also brings forward the opportunity of jailbreaking the system which is like rooting the device in Android. Rather than allowing users the ability to have freedom of choosing widgets and various other games, Apple has stuck by its rulebook and kept the system closed even in 2022 which is exactly why I still do not own an iPhone and probably never will.

Corresponding Author:- Sanjeev Kumar Paul

Although Apple did listen to initial critiques and implemented Address space layout randomization in iOS 4.3 released in March 2011 [3].

iCloud & iPhone

One of the most exclusive features that set Apple apart from its competitors is the iCloud. The user requires an Apple ID.iCloud not only helps in providing the essential extra storage required to make backups for security reasons but also aids in tracking down the iPhone using Find My iPhone. “Find my iPhone” is considerably known as the best application for finding lost or stolen phones and erasing the data to ensure no personal data is disclosed. However, as shown in the experimentsconducted byMaheshwari, Sampreshita& Agal, Sanjay for their research paper, it was conclusive that iCloud was able to give direct access to the home screen using functions provided in the application.

Researchers took three test scenarios that were subdivided into two phases either Offline mode or Online mode.Whenever the iPhone is misplaced, the user must log in to iCloud's web-based portal and use the Find My iPhone app's online application. The user's phone's most recent location is synchronized with the servers of Apple. If the phone is still operational (that is, it is alive and well), When one is online and connected to the internet, one can accomplish a variety of tasks. Erase the iPhone, Lock the iPhone, play a sound, display a message, and turn on the lost mode.

If the user issues any commands, they will only be carried out once the device reconnects to the internet or comes online. At the server end, the commands are queued for execution while the device reconnects. This procedure still holds the same as of April 24, 2022.

The trickiest part about the entire process is that people with the stealthy mind will remove the SIM and turn it off, this test case was also considered. Since the limitation of the application is being reliant on Internet, harm to the phone and stealing data is a significant possibility. I tested the scenario where I made my friend turn her cell phone OFF and sign intoiCloud and use the same app, Similar conclusions still hold their value as the commands were only queuedwith immediate suspension of Apple Pay as shown in figures 1 & 2 in Appendix.

Face ID & iPhone

Face detection services that are used by android are quite prone to erroneous authentication as it has authenticated a few of my friends who do not even look like my facial patterns, but I always believed that the technique used by Apple would be secure however researchers were able to find that by using three simple factors: Spectacles, Tape and a sleeping entity, Liveness detection function could be exploited [4].

Face detection was also exploited by researchers on iPhone X [6] this only brings more suspicion towards the ability to authenticate however as of April 24, 2022, a new update has been sent by Apple that allows the user with masks to be successfully authenticated on iOS 15.4 or iPhone 12 and above.

What about the User itself

Here is the attack surface that all technological advancements are vulnerable to because young enthusiasts are willing to go to various ends to make sure their systems can have high-end specifications which can be exploited by the malicious attacker by using social engineering. Normal security practices need to be followed in any case and thwarting any Phishing attempt becomes of utmost importance.

Case study #1: PEGASUS

Even the recent iPhones are vulnerable to the most sophisticated attacks sponsored by the government albeit Apple has been trying to reduce attack surfaces. This spyware was able to retrieve Personally identifiable information(PII) without any user input in what is called “Zero-click” attacks simply by calling over WhatsApp even if the call was never picked up.

Case Study #2: NoReboot

An ultimate persistence bug as reported by ZecOps because "The ultimate persistence bug" since it prevents even transient hacker-affected iPhones from escaping their hacker. Furthermore, it affects every iPhone model and every version of iOS, and Apple is unable to repair it, which raises red flags [7].

NoReboot's concept is simple: it fools users into thinking they have turned off or rebooted their iPhones. When users try to commence either procedure, it hijacks the **InCallService**, **SpringBoard**, and **backboardd** background processes that manage the reboot process on iPhones and displays a bogus shutdown or Startup sequence instead. In actuality, the iPhone is always turned on [7].

Conclusion:-

1. The evaluation done by the independent evaluators was extremely concise and well documented,especially the fact that they were able to find that most of the important applications were already running with higher privileges unnecessarily.
2. After reading "iPhone Security Analysis" by Mark Stamp and Vaibhav Pandya, it was clear that high emphasis was put on the fact that the Apple ecosystem will be a closed space where APKs cannot be downloaded from third-party websites, as this paper focused on first few iPhones,**attacks via Bluetooth** could have been discussed apart from the Jailbreaking concept as I feel this analysis came almost a year after {cmiller, jake, josh}did the evaluation.
3. "iCloud and its security issues"had a major core topic: Find my iPhone that still holds, although various new features surely have been added with better UI.
4. Independent Articles read on the latest iPhones did show that attackers still can find a way to breach even though the walls have been built high as supported by case studies.

Future Scope

The systematic review presented here demonstrates the reigning fact that no technology is secure from threats that are related to the human mind, although it does state that iPhone has done a tremendous job in making sure threat vectors are minimized by enforcing developers to comply with various programs and NDAs while utilizing Digital signatures to identify identities.Human beings like to enjoy the freedom of choice which Apple does not provide but that has provided the stable base on which they can experiment which is why people in cybersecurity tend to suggest the usage of Apple products.The Future of apple relies on answering the following questions that have arisen from the above research and my personal questions as well:

1. Can Apple enhance dataset samples for Liveness detection for Biometric Authentication?
2. Can iPhone automate the spam removal/detection on mail providers as it already provides features for blocking phone calls?
3. Can Apple regulate the text conversations between android and iOS to provide equal security features?
4. How will iPhone attract a userbase that cherishes freedom of choice but does not compromise its standards?
5. How will Apple counter the APT threats?

Appendix

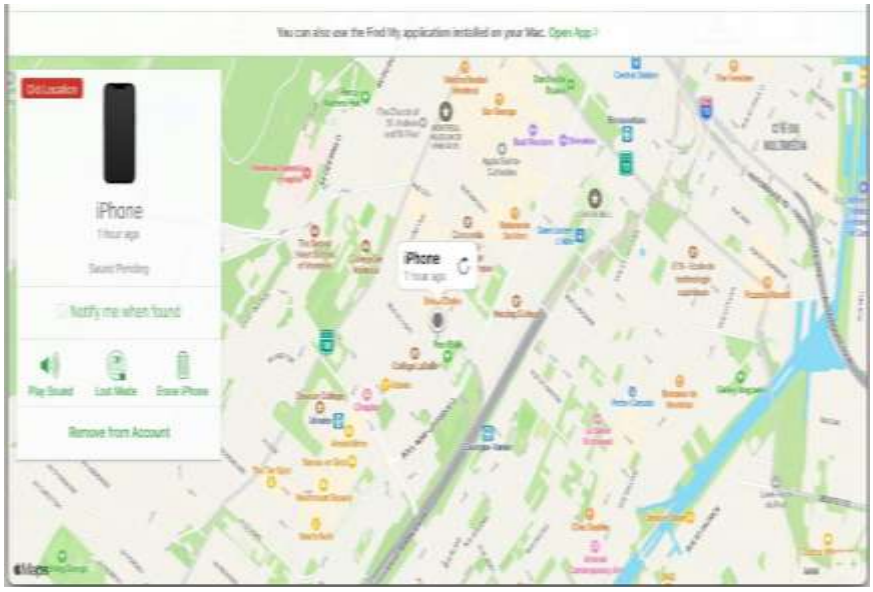

Figure 1:- first command sent in offline mode.

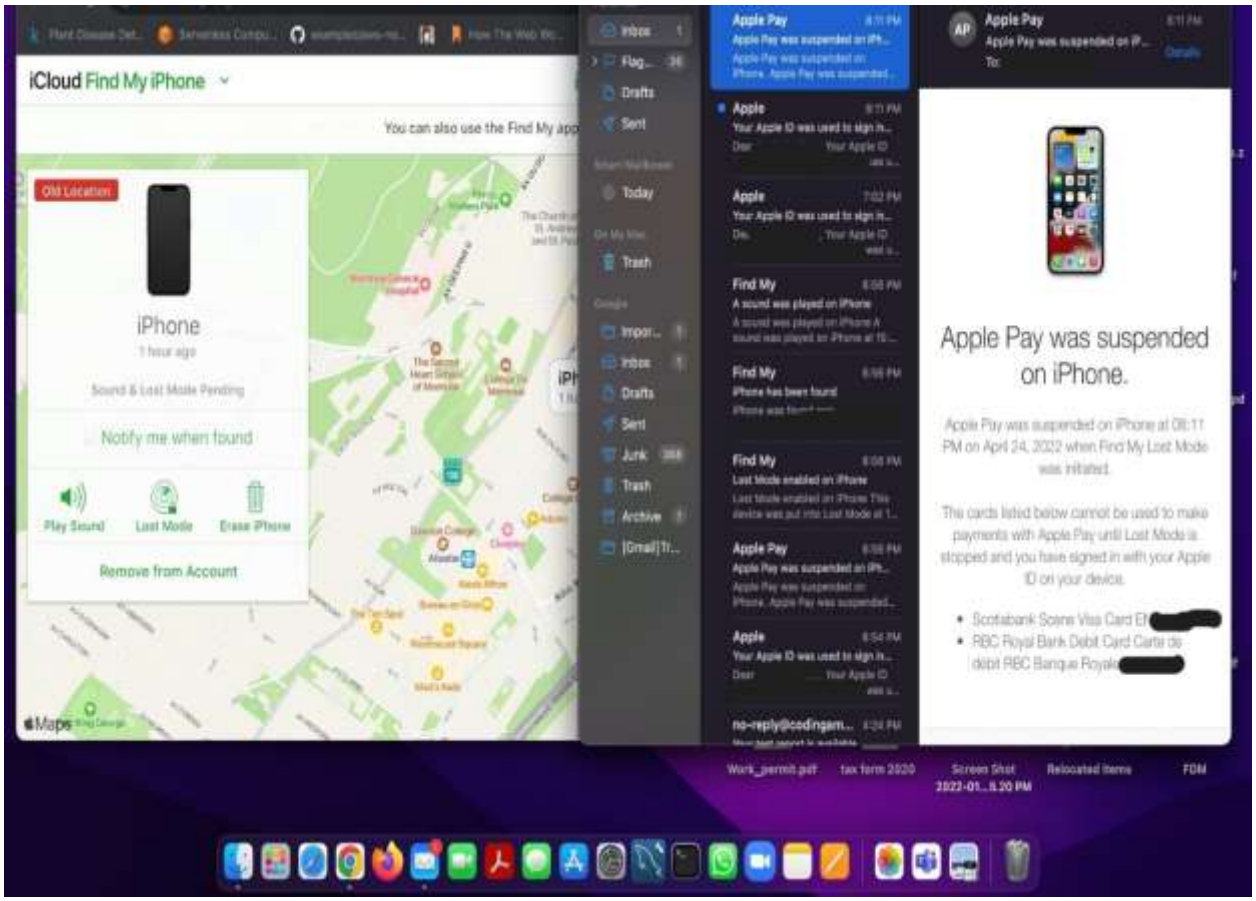

Figure 2:- Second command in the queue and immediate suspension of Apple Pay.

References:-

[1] Mark Stamp, Vaibhav Pandya. "iPhone Security Analysis". International Journal of Multimedia Intelligence and Security, 2010.

[2] {cmiller, jake, josh} "Security Evaluation of iPhone" at securityevaluators.com

[3] Address space layout randomization - Wikipedia (2018). Available at: https://en.wikipedia.org/wiki/Address_space_layout_randomization#:~:text=Apple%20introduced%20ASLR%20in%20iOS%204.3%20(released%20March%202011). (Accessed: 13 April 2022).

[4] Winder, D. (2022) Apple's iPhone FaceID Hacked In Less Than 120 Seconds, Forbes. Available at: https://www.forbes.com/sites/daveywinder/2019/08/10/apples-iphone-faceid-hacked-in-less-than-120-seconds/ (Accessed: 16 April 2022).

[5] Maheshwari, Sampreshita& Agal, Sanjay. (2015). iCloud and its security issues.

[6] Brewster, Thomas. "Apple Face ID 'Fooled' By $150 Mask -- But Big Questions Remain". Forbes, 2022, https://www.forbes.com/sites/thomasbrewster/2017/11/13/apple-face-id-hacked-by-vietnamese-researchers-mask/?sh=2ae599584987. Accessed 25 Apr 2022.

[7] Kelly, Gordon. "New 'Noreboot' Hack Can Keep Malware OnIphones Longer". Forbes, 2022, https://www.forbes.com/sites/gordonkelly/2022/01/08/apple-warning-iphone-hack-attack-vulnerability-new-iphone-update/?sh=5ccfb6b5659e. Accessed 25 Apr 2022.