International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 3, May -June 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

MAC Address Randomization- Protecting User Privacy at the Cost of Security

Sneh Bhajanka*
*(Computer Science and Engineering, R.V College of Engineering, Bengaluru
Email:snehbhajanka.cs17@rvce.edu.in)

----------**********----------

Abstract:

Userprivacy, particularly user monitoring, has always been a major worry, and it is much more so today that we are surrounded by Wi-Fi enabled gadgets (smartphones, tablets, wearables, etc.). These devices send out unencrypted signals carrying information such as the MAC (Media Access Control) address of the device. With inexpensive technology and a passive assault, such signals may be observed. Because each device's MAC address is unique, the device owners' privacy is unquestionably jeopardised. To preserve user privacy and prevent customers from being monitored when using public hotspots, MAC Address Randomization is the only countermeasure. It is becoming the de facto standard for mobile networking operators.

Keywords **—Mac Address Randomization, iOS, Android, Windows, Privacy, Security.**

----------**********----------

I. INTRODUCTION

The development of mobile devices and the wireless networks that allow them, provide a lot of benefits to their consumers but they were not designed with privacy and protecting user anonymity in account. Wi-Fi devices are periodically sending frames containing a unique identifier (the MAC address) which can be leveraged to track the owners of those devices [1].

Probe Requests are regularly sent by Wi-Fi radios in order to scan for accessible connection points. This has the unintended consequence of alerting any adjacent eavesdropper of their existence and possibly trackable identifying information. In response to these privacy issues, mobile phone manufacturers and software developers utilise a technique known as Media Access Control (MAC) addressrandomization for probing requests, which involvesrandomising previously persistent network identifiers to avoid user tracking. In this paper, anin depth study of mac randomization is done, how it effects the vendors and the network services that are affected.

II. WHAT IS MAC RANDOMIZATION?

The use of random hardware addresses by mobile devices to prevent observers from distinguishing their traffic or physical location from that of other nearby devices is known as Media Access Control (MAC) address randomization. Listeners cannot use MAC addresses to establish a background of device activity with MAC randomization, which increases user privacy.

Thus, user activity cannot be tied to a pool with Mac address randomization.

III. IDENTIFICATION OF A RANDOMIZED MAC ADDRESS

Randomized MAC addresses are simple to identify. A bit in the Organizationally Unique Identifier (OUI) portion of a MAC address is set to indicate a randomised or locally managed address. The key point is that if the second character is a 2, 6, A, or E, in the MAC address, then the address is randomised.

 ©IJSRED:All Rights are Reserved

IV. WHY IS MAC RANDOMIZATION TAKING OVER?

Mac Randomization was a call for privacy for the users. Privacy is an inviolable phenomenon for every individual. Although MAC addresses have traditionally been used for OSI communication (Layer 2), they have been increasingly popular in recent decades as personal identities for consumer service, device recognition, and traffic unloading in a variety of networks.Marketers leapt on using MAC addresses for monitoring consumers with the use of public Wi-Fi probe attempts, monitoring, beacons and some other privacy breaching technologies, just as they did with any otheridentifiable data point. The expansion and usage of randomised MACs has been aided by greater understanding of mobile privacy concerns.Most operating systems, including Android, iOS, and Windows, began to adopt their own variation of MAC address randomization while probing the Wifi network in response to these privacy flaws. The randomization of MAC addresses is a strategy that is intended to prevent potential observers from identifying which mobile devices are within reach of a sensor [3].

V. SECURITY ISSUES IN MAC RANDOMIZATION

Randomizing MAC addresses introduces a number of security concerns, the most critical of which are network stability and suspicious device activity. To guarantee steady associations for users around the world every second, both Wi-Fi steering and traffic offloading from mobile networks rely on discovering, recognising, and categorising devices. Considering that a network is unable to recognize a device, it will lead to the inability of directing the device to the most appropriate SSID.

Because MAC address is needed to trace a device on a network, operators and consumers will be unable to track devices connected to their routers if a large number of them utilise unexpected addresses. The drawback of not being able to monitor an endpoint is that malicious actors will find it easy to get access to the network using their own MAC address and conceal.

Finally, MAC address blacklists and whitelists are commonly used in device-based parental controls and dangerous content blocks. These safeguards must be re-enabled whenever a device's MAC address is changed. Unfortunately, doing this on a regular basis is not a smart security choice and renders such solutions outdated.

VI. COMMON SERVICES AFFECTED BY MAC RANDOMIZATION

The common services affected by MAC Address Randomization is explained as follows:-

A. Captive Web Portals

Captive portals are web sites that consumers are presented when they first connect to a network, usually for guest networks. They're used to communicate legal terms and agreements, to collect certain guest information in return for connection, and to authenticate and bill customers. The MAC address is used as the device anchor in such portals, and the user's authorisation state is linked to the MAC. The infrastructure will drive the user via the portal again if the MAC changes, causing a user-experience difficulty. Because portal processes are utilised in so many ways, it's difficult to provide particular advice for them. One option is to look at other authentication techniques that aren't MAC-keyed.

B. Policies based on MAC

Time and content limitations that may be applied to individual devices are becoming more common on home Wi-Fi routers. The MAC address is used to enforce these regulations. If they don't function anymore, it's because the MAC has been changed to a private address. Disabling the function for home networks is a simple solution. However, people may easily re-enable the functionality to circumvent security measures. As a result, policies should be established for both public and the private addresses.

C. Device Analytics

If private MAC addresses change, the new address is treated as a new exclusive device, potentially skewing device/user numbers. OUI databases will not map private addresses. Even though OUI is a simple technique for mapping a MAC address to a manufacturer, private addresses will obfuscate even that. Making a link between a scanning equipment and a connected one, to give an instance, identifying individual visits with “engaged” visitors, is getting increasingly difficult. Because the MAC for each SSID remains the same, it's still possible to distinguish between returning and new visitors, and eventually trace a user's behaviour over time to a single session.

VII. MAC RANDOMIZATION FOR IOS 14 DEVICES

Apple added MAC address randomization to its devices since iOS 8 [2]. It was accessible on all iOS devices, although it was turned off by default.

However, significant changes were seen in Apple's strategy while testing the beta version of iOS 14, as it randomised MAC addresses for every network, including the user's home Wi-Fi network, on a daily basis. For service providers who employ MAC addresses to enhance router performance, this would have resulted in chaos — the number of unique and unregistered gadgets would have multiplied every day,

 ©IJSRED: All Rights are Reserved

rendering typical traffic allocation and prioritisation methods outdated overnight.

However, Apple has changed its aggressive policy on MAC randomization in the official iOS 14 release. iPhones' MAC addresses are generated at random for each network, but only once unless the user decides to forget it.

VIII. MAC ADDRESS RANDOMIZATION ON ANDROID 10

Android 6.0 uses randomization for background scans if the driver and hardware support it [2].Since Android 9, the operating system has received complete MAC randomization. Earlier, randomization was turned off by default on all devices, but recently, certain vendors have begun to supply endpoints with randomization turned on by default. Randomization is now in use on the latest Samsung, Google, and OnePlus handsets, and as Android 10 usage grows, approximately 80% of all smartphones will have randomised MAC addresses in the foreseeable future.

IX. RANDOMIZED MAC ADDRESSES ON WINDOWS DEVICES

While we focus primarily on mobile devices, we mention Windows 10 briefly because it was the first widely available implementation of post-association randomization, and as a point of comparison for other implementations [4]. In Windows 10, post-association randomization is disabled by default. This setting can be enabled for specific networks or as a global setting that applies to all 802.11 networks; in either case, the device uses a random MAC address when **associated** to each SSID it **connects** to. Windows 10 also affords the user with the option to change the random MAC address for use with a specific SSID daily, rather than the random MAC address generated when the device first connected [4].

X. CONCLUSION

Everything engineers do in the realm of Wi-Fi is a balancing act, a trade-off. From the user's perspective, MAC Address randomization is a choice between anonymity and network accessibility. While protecting user privacy, it introduces vulnerabilities in network security and accessibility.

This paper discusses how MAC address randomization is increasingly being used by mobile device makers and operating system developers to preserve user privacy and prevent attackers from monitoring permanent hardware identifiers. Table 1 represents a summary of how different vendors are implementing Mac Address Randomization. It can be concluded that newer phones with updated operating systems provide considerable degree of privacy to the users using randomized mac addresses. However, implementation of on-by-default effective Mac Randomization will necessitate a considerable modification in the design of certain enterprise networks, and that it will require time to deploy across all devices.

 ©IJSRED: All Rights are Reserved

TABLE I.
SUMMARY OF HOW DIFFERENT VENDORSIMPLEMENT MAC RANDOMIZATION

Operating System	Supports MAC randomization	Default Status	Network based per SSID	Time Based (24 hours)
Apple iOS 13	No	N/A	N/A	N/A
Apple iPadOS 13	No	N/A	N/A	N/A
Apple iOS 14	Yes	Enabled	Enabled	No
Apple iPadOS 14	Yes	Enabled	Enabled	No
Android 9	Yes	Disabled	Optional	No
Android 10	Yes	Vendor/ Carrier specific	Vendor/ Carrier specific	No
Android 11	Yes	Enabled	Enabled	Optional
Windows 10	Yes	Disabled	Optional	Optional

ACKNOWLEDGMENT

I would like to acknowledge the support provided by teachers of Department of Computer Science and Engineering, RV College of Engineering, Bangalore, India through their assistance in the research work.

REFERENCES

[1] Célestin Matte, Mathieu Cunche, Franck Rousseau, and MathyVanhoef..*Defeating mac address randomization through timing attacks*. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2016.

[2] MathyVanhoef, Célestin Matte, Mathieu Cunche, Leonardo S Cardoso, and Frank Piessens. *Why mac address randomization is not enough: An analysis of wi-fi network discovery mechanisms*..In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pages 413–424. ACM, 2016.

[3] Luiz Oliveira, Daniel Schneider, Jano De Souzai, and Weiming Shen, *Mobile Device Detection Through WiFi Probe Request Analysis*, IEEE Access, 2019.

[4] Ellis Fenske, Dane Brown, Jeremy Martin, Travis Mayberry, Peter Ryan, and Erik Rye, *Three Years Later: A Study of MAC Address Randomization in Mobile Devices And When It Succeeds*, Sciendo, Proceedings on Privacy Enhancing Technologies, 2021.

[5] A.B. M. Musa and J. Eriksson. *Tracking unmodified smartphones using Wi-Fi monitors,* in Proc. 10th ACM Conf. Embedded Netw. Sensor Syst. (SenSys), vol. 12, 2012.

[6] A. Di Luzio, A. Mei, and J. Stefa,*Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests* in Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (IEEE INFOCOM), Apr. 2016.

 ©IJSRED: All Rights are Reserved