Hide and Seek: On Privacy and Security In Modern 802.11 Wireless Networks

Florian Schmidt, Leander Seidlitz*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: fs.schmidt@tum.de, seidlitz@net.in.tum.de

***Abstract*—Given the widespread adoption of network-enabled devices, security and privacy considerations are of great importance. Since the introduction of IEEE 802.11 in 1997, the wireless standard's associated security and authentication measures have evolved. Insecure methods like WEP have been replaced by the now widespread frameworks WPA2 and WPA3 which, given a correct configuration, reliably ensure confidentiality and integrity of the exchanged traffic. While randomization schemes exist to avoid sending globally unique MAC addresses, fingerprinting and tracking of users using information obtained from the PHY or MAC layer is still an open issue even in modern networks. Comparable mobile networks like 5G offer robust security with concealed identifiers and mutual authentication by default, whereas the security of Wi-Fi networks depends on the specific configuration of the access point. In this work, we provide a comprehensive analysis of security and privacy aspects in modern IEEE 802.11 wireless networks. Over the years, 802.11 has seen a significant improvement in the security level. Nevertheless, some challenges remain regarding fingerprinting, misconfiguration and circumvention of MAC address randomization schemes.**

***Index Terms*—802.11, security, privacy, wi-fi, tracking, fingerprinting, RCM, fuzzing**

1. Introduction

Since the release of the initial Wi-Fi standard in 1997 [1], the growth and technological progress in mobile devices has led to widespread adoption of the standard around the world. This ubiquity necessitates the careful consideration of security and privacy aspects concerning the standard and its implementation in devices, as vulnerabilities or design flaws in the employed protocols can have far-reaching ramifications. It is critical to ensure the confidentiality and integrity of the traffic exchanged over the Wi-Fi networks to protect users from attacks like eavesdropping, Man-in-the-Middle (MitM) or malicious networks. Even when the payload is encrypted, careful examination of the data that can be read from frame headers or is leaked by other layers is critical to safeguard the privacy of users.

This paper aims to explore the 802.11 standard with a specific focus on security and privacy aspects of the offered services. The rest of this work is structured as follows: Section 2 provides an overview over IEEE 802.11 with a focus on historical development, the MAC layer and protocol security measures. Section 3 analyses the security and privacy aspects of Wi-Fi fingerprinting, tracking, MAC address randomization, and fuzzing. Section 4 compares these aspects to 5G mobile networks. Finally, Section 5 concludes.

2. 802.11 Wireless Networks

The IEEE 802.11 standard for wireless networks was released in its original form in the year 1997. The following section will give a brief introduction to the standard.

2.1. Overview and Historical Development

Since its origin in the 1980s, the IEEE 802 project served to standardize communication in local area networks (LANs), with the other most widely used standards also including 802.3 CSMA/CD Ethernet [2].

The 802 standards generally follow a reference model closely related to the ISO/OSI model, but with a few distinct modifications. The main functionality of 802.11 is incorporated to the Physical (PHY) and Data Link Layer (DLL). The DLL is further subdivided into the two sublayers Logical Link Control (LLC) and Media Access Control (MAC) [3].

Definitions for several key terms closely associated with the standard will be provided here. A station (STA) is any device with a wireless interface capable of communication within 802.11 networks. A Basic Service Set (BSS) consists of a number of STAs communicating with each other. An Access Point (AP) is a type of STA which manages the network communication [1]. Imporant identifiers include the Service Set Identifier (SSID), the natural language label for a single network, as well as the BSS Identifier (BSSID) consisting of the MAC layer address of the AP [4].

The original 802.11-1997 standard [1] has since been amended and superseded a significant number of times with a concrete focus on the performance, reliability and security of 802.11 networks.

2.2. MAC Layer Services

This section will discuss the services specified on the MAC layer of 802.11 networks. For the sake of brevity, the PHY layer will not be discussed in this work in much detail. It shall nevertheless be noted that the PHY layer may still be a source of information disclosure from a security perspective.

 doi: 10.2313/NET-2024-09-1_16

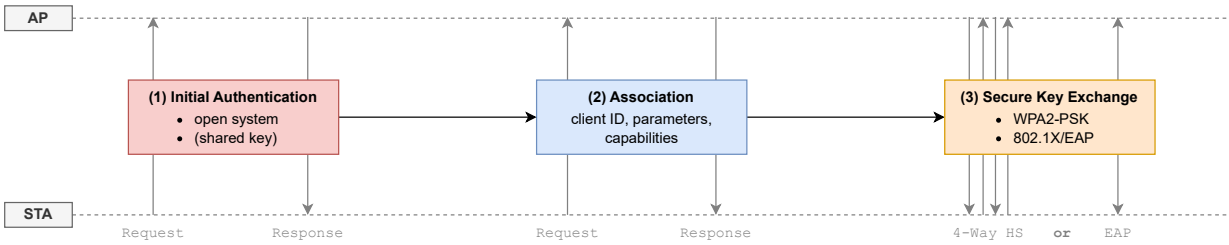

Figure 1: IEEE 802.11 association and authentication procedure, adapted from [4].

Addressing. For addressing communication partners on the MAC layer, the 48-bit LAN MAC addresses standardized in 802-2001 are used. The first 3 octets of this address make up the Organizationally Unique Identifier (OUI) assigned by the IEEE, leaving the remaining 3 octets to be assigned by the organization or device vendor [5]. The second last bit in the first octet of the address constitues the Universally or Locally administered (U/L) flag, indicating that, when set to 0, this address is universally administered and therefore globally unique.

Frame Structure. The primary transmission unit of 802.11 networks is called a frame, comprised of frame control information, sequence numbering, a checksum, the payload, and four MAC addresses. Frames are generally classified into three distinct types by their purpose. Data frames carry payload from the higher reference model layers, which commonly takes the form of Internet Protocol (IP) packets. Management frames are used for network management and can, for example, take the form of beacon frames or probe requests. Lastly, control frames are used to coordinate access to the wireless medium for carrier sensing and collision detection [4].

A critical point to mention is that management frames are typically sent over the medium in plaintext and without integrity protection. This vulnerability has been somewhat rectified by the 802.11w-2009 amendment's introduction of Protected Management Frames (PMF) [4].

Association and Authentication. In order to communicate over a Wi-Fi network, a STA must associate with the corresponding AP. In this process, the STA is assigned an association ID and parameters indicating specific capabilities are exchanged between the STA and the AP [4].

Prior to the association, a device must authenticate itself to the AP. Originally, Wired Equivalent Privacy (WEP) shared key authentication was intended to be used for this purpose in the authentication phase. However, since its deprecation due to critical security flaws, the procedure typically realizes an open system authentication leading to an always positive authentication response by the AP (essentially realizing a dummy authentication), followed by the actual, security-relevant cryptographic authentication handshake *after* the above-mentioned association phase [2], [4]. This procedure is illustrated in figure 1. More details on 802.11 security measures will be discussed in section 2.3.

Network Discovery. There are both active and passive scanning procedures for discovering APs in range of a given STA. With passive scanning, a STA listens for beacon frames broadcast by APs at regular intervals to advertise their networks. When actively scanning, a STA sends out explicit probe requests which may or may not be specific to a single, searched-for SSID. Addressed APs respond with probe responses containing detailed information about its network [2], [4].

2.3. Authentication and Security Measures

Security mechanisms in 802.11 networks are frequently divided into the classes Pre-RSNA and RSNA in literature, with the name stemming from the Robust Security Network Association (RSNA) specified in the 802.11i amendment [2].

Pre-RSNA. Networks using Pre-RSNA security rely on WEP for confidentiality and the procedures *shared key* or *open system* for authentication. The insecurity of the key scheduling algorithm employed in WEP was shown in 2001 by Fluhrer, Maintin and Shamir [10], where the authors outline a well-scaling ciphertext-only attack. Since this original work, even more rapid attacks have been developed, leading to the effect that any WEP key can be recovered within a negligable time period using non-specialized hardware. The mechanisms of shared key authentication and WEP are therefore completely insecure and have consequently been deprecated with 802.11i in 2004. What remains of Pre-RSNA security in modern networks is the open system authentication mentioned in section 2.2 [2].

RSNA. As part of RSNA security, 802.11i specifies the authentication mechanisms pre-shared key (PSK) and 802.1X [2]. The Wi-Fi security frameworks predominantly used today are the above-mentioned open system authentication, WPA2 and WPA3 [4].

First, PSK works by relying on a secret key known to both the STA and AP and performing a 4-way handshake for authentication. In WPA2, the key material is derived from the SSID and network password, where the latter is required to be shared out-of-band prior to the authentication process.

The second option, 802.1X, is a centralized network access control protocol that uses the Extensible Authentication Protocol (EAP). It ensures that unauthenticated devices can only transmit and receive 802.1X traffic. In contrast to PSK, a session key is derived upon positive authentication in 802.1X, from which the encryption key is then generated by the STA.

Statistics based on Wi-Fi network datasets gathered in the context of global open data initiatives indicate that the vast majority of networks still rely on WPA2 (74.5 %), with the more secure WPA3 (1.4 %) alarmingly being less represented than the deprecated WEP (3.0 %) [11].

	iOS/iPadOS 14+	Android 10+	macOS 13	Windows 10+
Randomized for Probe Requests	Always	Always	Never	Optional (default: off)
MAC generated using	BSSID	SSID, security parameters, (FQDN)	–	SSID
Randomized per Network	Always	Always	Never	Always
Randomized per Session	Never	Never	Never	Never
Randomized per Day	Never	Non-persistent in some cases (v12+)	Never	Optional (default: off)
Re-randomized on 'Forget' Network	Always	Never	Never	Always

TABLE 1: Vendor adoption of MAC address randomization schemes (from [6]–[9] and own experiments).

3. Security and Privacy Considerations

Ensuring the security and privacy of user data exchanged over a network is crucial, even more so when the network in question uses a broadcast medium. This section will therefore discuss aspects of security and privacy in modern IEEE 802.11 networks.

3.1. Wi-Fi Fingerprinting and Tracking

The fingerprinting and tracking of users is a sizeable concern in the widespread use of wireless networks, since the messages exchanged by the STAs and APs contain unique identifiers. These identifiers can be used to determine whether a specific STA, and thereby a particular person, is present at a given location.

In the simplest case, the 802.11 frame headers contain the actual universally-administered MAC address of the STA in question, distinctly identifying this specific STA. On older devices, probe requests sent during active scanning also leak the real MAC address of the STA while it is not connected to any network. This fact allows for passive tracking of the STA by eavesdropping on 802.11 frames exchanged over the medium [12].

For mitigating this vulnerability, several vendors have implemented randomization schemes allowing the STA to hide its actual, globally-unique MAC address in favor of a disposable address. The implementation details, adoption and shortfalls of these schemes are further discussed in section 3.2.

Next to the MAC address, other information is also sent over the medium, all of which can potentially be used for fingerprinting. This practice consists of the collection of enough information to either construct a full identifier of the STA, or at least to classify it based on various features.

On the PHY layer, it is conceivable to identify the network interface card used to transmit a frame by analyzing distinctive artifacts contained in the transmission. Moreover, a scrambling process is applied to 802.11 frames prior to transmission to reduce transmission errors. It is possible to correlate the scrambler values used across multiple transmissions to identify the device even if the MAC address has changed [4], [13].

On the MAC layer, it is possible to fingerprint the STA by analyzing the device class, involved operating system, driver software, chipset, and may even include device-specific fingerprinting techniques that are not broadly applicable [12]. Linking multiple frames together is simplified by the sequence number field contained in the frame header. The number, presence, order and contents of Information Elements (IEs) contained in probe requests for advertising device capabilities can also be used for fingerprinting and may even indirectly leak the STA's MAC address [14]. It is further possible to exploit the significant amount of information contained in 802.11 management frames, for example to fingerprint the AP and the environment it is operating in [4].

While fingerprinting is generally possible on all layers of the reference model, considering cost and efficacy yields the MAC layer as the optimal information source: PHY requires dedicated equipment to observe, and transport layer traffic is only sent once a STA is associated and authenticated to the network, thereby limiting the observable information exchange [12].

The procedures and techniques outlined above yield identifiers of the users, either through the actual MAC address of the STA in the simplest case, or through a combination of other information collected during the communication. These identifiers can then be used to detect whether a user is present in a specific location and to track this user through space and over time. In many cases, this involves little effort and requires no specialized hardware, as typical Wi-Fi interfaces in consumer devices support sniffing and recording the frames exchanged over the medium using monitor mode.

3.2. Randomized and Changing MAC Address

The tracking concerns outlined in the section above have led to a wide adoption of Randomized and Changing MAC Address (RCM) schemes by device vendors. The core idea is to ensure that not a single, globally-unique MAC address can be associated with a STA by replacing it with a virtual, randomly generated address.

All modern versions of general purpose operating systems support RCM. However, since there is no standardized specification for this scheme, the concrete implementation varies somewhat across vendors. An excerpt overview of the implementation details can be seen in table 1. While generally the same randomized MAC address is used per network in order to minimize service disruptions resulting from frequently changing addresses, it can be sensible to randomize more frequently in some cases like open networks for better protection. Interestingly, as seen in table 1, macOS 13 does not implement a native MAC address randomization scheme [9].

Even though RCM schemes significantly enhance user privacy, it has been shown that it is still possible, though only with an increased effort, to track and fingerprint RCM-enabled devices [4]. In a sense, it is possible to de-randomize the MAC address, thereby constructing a pseudo-identifier for the tracked STA.

As an example, a passive technique can rely on associating probe requests sent out using randomized addresses with different devices based on their inter-frame

arrival times, frequency, sequence numbers, inter-burst time deltas and contained IEs. Some active attacks also include exploiting BSSIDs found in probe requests to create malicous APs or taking advantage of WPS parameters directly linked to the factory MAC address [4], [6].

3.3. Privacy Risks

As described in the sections above, the fingerprinting and tracking possibilities in 802.11 networks come with significant privacy considerations.

Privacy can be defined as the "fair and and authorized processing of Personally Identifiable Information (PII)" [4], a concept that describes information that can be used to either directly or indirectly identify an individual. In this sense, a MAC address of a STA can also be considered PII, given that it allows for determining the presence of the STA's owner in a particular location. It may also be noted that the collection of PII alone does not always pose a direct threat. In some cases, it may even be desirable for an individual to opt-in to the collection of certain data in exchange for easier usage of a system – or it may be necessary from a technical perspective to provide the sought-after service. Nevertheless, the use cases for the extracted PII include broad surveillance and tracking, directed probing, targeted advertisement, profiling of users, or mobility research and statistical analysis [4], [12].

In the context of Wi-Fi networks, the act of observation itself is fairly trivial given the broadcast nature of the medium. Any observer within range of a STA is capable of intercepting the transmitted signals and extracting PII. The possibility for Wi-Fi tracking enabled by this fact therefore carries risks, as the distinctiveness of mobility data is high enough that only few data records in space and time suffice to uniquely identify a large proportion of individuals [4], [15].

In earlier versions of well-known operating systems, STAs using active scanning to discover nearby APs sent out bursts of probe requests targeted to specific SSIDs contained in their Preferred Network List (PNL). The networks contained in a device's PNL can also be considered PII, as it has been shown to be possible to reconstruct the social graph of individuals in a large group by correlating the observed networks. In newer OS releases, this procedure has been replaced with sending wildcard probe requests directed at all APs in the vicinity, with directed probe requests only being used for discovering hidden APs that do not announce their presence by answering wildcard probes or by sending beacon frames [12], [16].

3.4. Wi-Fi Fuzzing

A holistic analysis of the security of 802.11 networks also includes checking for vulnerabilities in the implementations of STAs and APs. A useful technique in this context is fuzzing, which works by supplying the program with large quantities of (semi-)invalid input data with the aim of triggering erroneous behavior. Due to the fact that 802.11 is standardized, no reverse-engineering is required to generate the fuzzing inputs on the protocol level. Various entry points for fuzzing have been used in past works, e.g. kernel hooks or firmware emulation, but the method with the widest applicability to all STAs is over-the-air (OTA) fuzzing.

The latter transmits the fuzzing data as actual 802.11 frames to the target device and can therefore fuzz all types of frames and emulate a STA as well as an AP [17]. Since the 802.11 security frameworks generally only encrypt the payload data carried in the frame, it is possible to forge and send arbitrary management and control frames to STAs as long as PMF is not used to ensure the integrity and confidentiality of these frames. Since PMF is only mandatory on STAs using WPA3, OTA fuzzing frames are in fact processed by a large proportion of devices.

In practice, Wi-Fi fuzzing can reveal a number of implementation issues. For instance, Cao et al. found 23 vulnerabilities in their analysis, including denial of service attacks and memory corruption issues [17].

4. Comparison with 5G Networks

Even though the standards and network architectures differ quite greatly, we aim to compare the security and privacy of 802.11 Wi-Fi with 5G mobile networks.

A first observation is that 5G traffic is encrypted on the network in all cases, whereas Wi-Fi security depends on the configuration of the AP.

Secondly, similar to MAC addresses in Wi-Fi headers, mobile networks also use permanent identifiers: In 4G, the International Mobile Subscriber Identity (IMSI) is used, whereas 5G relies on the Subscription Permanent Identifier (SUPI). Since tracking is possible wherever such permanent identifiers are in use, networks up to 4G suffered from the privacy issues presented by the use of IMSI-catchers (fake base stations that actively request an end user's IMSI) [18], [19]. 5G networks aim to solve this issue by optionally encrypting the SUPI with the public key of the network operator and rotating this identifier for every session, yielding the Subscription Concealed Identifier (SUCI). However, similar to the MAC address de-randomization techniques discussed in section 3.2, it can still be possible to link user identities to SUCIs despite the encryption scheme due to weaknesses in the authentication procedure [18].

Thirdly, contrary to the personal-level Wi-Fi security measures discussed in section 2.3, the 5G authentication procedure performs mutual authentication of both the network and the user's device. In Wi-Fi, proper mutual authentication is only performed in enterprise-level protocols like 802.1X, thereby enabling attacks exploiting rogue APs like the evil-twin attack [4].

5. Conclusion

Through the evolution of the standard over time, the security and privacy of IEEE 802.11 networks improved significantly, especially with the introduction of RSNA networks and WPA3.

In correctly configured, mature networks using WPA2 or WPA3 with good passwords, the security level is very high and barring implementation flaws or elaborate attacks, users are generally not at risk of confidentiality or integrity violations. Fuzzing can help discover implementation flaws and make devices more secure. Nevertheless,

privacy risks associated with the practice of Wi-Fi fingerprinting and tracking remain.

Tracking is mainly performed using information obtained from the PHY and MAC layer that, in the worst case, uniquely identifies the device in question. In case the STA uses its factory MAC address for sending probe requests or connecting to the network, this address can be directly used as an identifier. RCM schemes prevent this type of direct tracking by randomizing the exposed address, therefore significantly increasing the level of protection. Still, it is possible in many cases to de-randomize the addresses and track the devices, albeit under an increased level of effort.

Mobile networks like 5G offer a robust security and privacy framework by default, whereas the security of 802.11 networks depends on the configuration of the AP.

The concluding recommendation is twofold: Firstly, given the importance of proper configuration for the security of Wi-Fi networks, up-to-date devices and strong passwords, security-aware users with knowledge of the risks involved are essential. Secondly, ongoing research into improving protective techniques like RCM is vital to further restrict an attacker's ability of address de-randomization and fingerprinting. These measures will further enhance the security and privacy of IEEE 802.11 users in an era of ubiquitous devices.

References

[1] "IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," *IEEE Std 802.11-1997*, 1997.

[2] A. Holt and C.-Y. Huang, *802.11 wireless networks: security and analysis*. Springer Science & Business Media, 2010.

[3] "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture," *IEEE Std 802-2014 (Revision to IEEE Std 802-2001)*, 2014.

[4] D. Ficara, R. G. Garroppo, and J. Henry, "A Tutorial on Privacy, RCM and Its Implications in WLAN," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 1003–1040, 2024.

[5] "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture," *IEEE Std 802-2001 (Revision of IEEE Std 802-1990)*, 2002.

[6] M. Uras, E. Ferrara, R. Cossu, A. Liotta, and L. Atzori, "MAC address de-randomization for WiFi device counting: Combining temporal- and content-based fingerprints," *Computer Networks*, vol. 218, p. 109393, 2022.

[7] J.-C. Zúñiga, C. J. Bernardos, and A. Andersdotter, "Randomized and Changing MAC Address state of affairs," Internet Engineering Task Force, Internet-Draft draft-ietf-madinas-mac-address-randomization-12, Feb. 2024, work in Progress (Last Accessed: June 10, 2024). [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-madinas-mac-address-randomization/12/

[8] Android Open Source Project, "MAC Randomization Behavior," 2024, (Last Accessed: May 27, 2024). [Online]. Available: https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

[9] Apple Inc., "Apple Platform Security: Wi-Fi privacy," 2024, (Last Accessed: Aug 6, 2024). [Online]. Available: https://support.apple.com/guide/security/wi-fi-privacy-secb9cb3140c/web

[10] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," in *Selected Areas in Cryptography: 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16–17, 2001 Revised Papers 8*. Springer, 2001.

[11] "WiGLE: Wireless Network Mapping," (Last Accessed: July 25, 2024). [Online]. Available: https://wigle.net/index

[12] C. Matte, "Wi-Fi tracking : Fingerprinting attacks and countermeasures," Theses, Université de Lyon, Dec. 2017, (Last Accessed: June 10, 2024). [Online]. Available: https://theses.hal.science/tel-01921596

[13] B. Bloessl, C. Sommer, F. Dressler, and D. Eckhoff, "The scrambler attack: A robust physical layer attack on location privacy in vehicular networks," in *2015 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2015, pp. 395–400.

[14] M. Vanhoef, C. Matte, M. Cunche, L. S. Cardoso, and F. 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*, ser. ASIA CCS '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 413–424.

[15] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Scientific reports*, vol. 3, no. 1, pp. 1–5, 2013.

[16] M. V. Barbera, A. Epasto, A. Mei, V. C. Perta, and J. Stefa, "Signals from the crowd: uncovering social relationships through smartphone probes," in *Proceedings of the 2013 Conference on Internet Measurement Conference*, ser. IMC '13. New York, NY, USA: Association for Computing Machinery, 2013, p. 265–276.

[17] H. Cao, L. Huang, S. Hu, S. Shi, and Y. Liu, "Owfuzz: Discovering Wi-Fi Flaws in Modern Devices through Over-The-Air Fuzzing," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 263–273.

[18] M. Chlosta, D. Rupprecht, C. Pöpper, and T. Holz, "5G SUCI-catchers: still catching them all?" in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 359–364.

[19] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291, 2020.