Privacy-Enhancing Technologies Against Physical-Layer and Link-Layer Device Tracking: Trends, Challenges, and Future Directions

Apolline Zehner
Université libre de Bruxelles
apolline.zehner@ulb.be

Iness Ben Guirat
Université libre de Bruxelles
iness.ben.guirat@ulb.be

Jan Tobias Mühlberg
Université libre de Bruxelles
jan.tobias.muehlberg@ulb.be

***Abstract*—Wireless devices, especially Bluetooth and Wi-Fi devices, emit radio communication both to scan for neighboring devices and to advertise themselves. For example, a mobile phone would typically be searching for Wi-Fi access points and Bluetooth devices, e.g., headsets, and advertise itself for connections. For this purpose, communication interfaces use a Medium Access Control (MAC) address which is a unique identifier to differentiate one device from another. However, the use of such unique identifiers can violate the privacy of the device and hence of the user; an attacker is able to use such unique identifiers in order to passively track a device. MAC address randomization – techniques that periodically change the MAC addresses of a device – were developed as a privacy-enhancing measure against such attacks. However research shows that this can be easily circumvented. In this paper, we survey approaches and techniques for metadata anonymization in Bluetooth and Wi-Fi, as well as the de-anonymization attacks. Many of these attacks rely on physical characteristics of the communication medium and on implementation flaws of both wireless protocols and MAC address randomization protocols. We conclude by discussing open challenges both in metadata protection and de-anonymization.**

***Keywords*—Bluetooth, Wi-Fi, Device Tracking, MAC Address Randomization, Metadata Privacy, Received Signal Strength Indicator (RSSI)**

I. Introduction

Both Bluetooth [1] and Wi-Fi [2] devices send packets at regular and predictable intervals to announce their presence to eventual known devices, such as Access Points (APs) or paired Bluetooth devices. Moreover, those probe requests are also useful to scan the device's surroundings for the presence of networks or other trusted devices. Probe requests can be automated (i.e. a device tries to connect to the closest Wi-Fi AP or trusted Bluetooth device) or manual (i.e. when performing a manual scan in search of nearby Bluetooth devices or Wi-Fi APs). This feature is therefore essential to allow connections between devices that were either connected to each other or not. However, this also opens the door to privacy violation by allowing an attacker to track a specific device for an extended period of time.

MAC address randomization was thus introduced in multiple IETF drafts since 2020 [3] as an anti-tracking and privacy-enhancing feature in multiple mobile operating systems, such as Google's Android 8 [4] in August of 2017 and Apple mobile operating systems in September of 2014 [5]. It should be noted that this was only the default setting on Android 10 [6], an operating system that was released in September of 2019.

While important, various research papers have shown that flaws and weaknesses exist in the implementation of the MAC address randomization algorithms which leads to de-anonymization attacks [1], [2], [5], [7], [8], [9]. Furthermore, even when MAC address randomization algorithms are implemented properly, the metadata leaked by both probe requests and Bluetooth LE advertisements have also led to the de-anonymization of devices [1], [10], [11], [12], [13]. Metadata such as the Received Signal Strength Indicator (RSSI) [9], [14], [15] make device re-identification and hence tracking possible, albeit with more constraints. We first describe our threat model in Section II. Next we outline the main de-anonymization attacks due to implementation flaws in Section III. In Section IV, we present the main side-channel attacks and in Section V we discuss counter-measures against common attacks alongside their assessed accuracy. Finally, we address open challenges and new directions of device de-anonymization through MAC address randomization in Section VI and we conclude in Section VII.

II. Attacker Model

Throughout this paper, we consider a passive attacker, meaning that the adversary does not break any cryptographic protocols and schemes. Rather, we assume an adversary who listens to Bluetooth and Wi-Fi communications of a target device for a period of time t and is able to collect and analyze metadata such as the emitting power, the timing of MAC randomization and frequency etc. Additionally, we consider an attacker who is able to exploit implementation flaws in cryptographic or hashing functions used in the wireless communication protocols. The attacker considered under our threat model aims to identify (and hence track) a device through its Bluetooth and Wi-Fi signals for various purposes. For

Workshop on Innovation in Metadata Privacy: Analysis and Construction Techniques (IMPACT) 2025
28 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-2-8
https://dx.doi.org/10.14722/impact.2025.23080
www.ndss-symposium.org

example, an adversary may want to target an individual and thus tracking their location through their devices, or it could be used for commercial purposes such as knowing customers' habits inside a store or proximity marketing.

III. De-anonymization through implementation flaws

A. Implementation flaws in MAC address randomization

In 2016, Vanhoef et al. [7] showed several techniques that allowed an attacker to de-anonymize a Wi-Fi device through both their probe requests (i.e. when a Wi-Fi client is searching for a known Wi-Fi AP) and the use of poorly chosen scrambling seeds that are used to anonymize its MAC address. While in theory those seeds should be initialized with pseudo-random and non-zero values [16], some devices analyzed by Vanhoef et al. used fixed seeds and most devices did not reset the state of their scrambler, thus rendering predictable the seeds produced. Predicting seeds produced by the Wi-Fi device's scrambler made the prediction of future "randomized" MAC addresses possible, which allows an attacker to track a specific device over a greater period of time than the one between two MAC address changes. Based on these attacks, Martin et al. studied the robustness of MAC address randomization implementation on a variety of mobile devices and find out that 90% were vulnerable [2]. The authors therefore argued that MAC address randomization techniques should be standardized and widely adopted in order to achieve privacy.

B. Implementation flaws in Wi-Fi Protected Setup

Some Wi-Fi APs provide Wi-Fi Protected Setup (WPS) as a mean to facilitate user's device connection. This functionality uses an Universally Unique Identifier (UUID), generated by hashing the MAC address of one of the interfaces of the Wi-Fi AP with a fixed seed [7]. However, in 2014, Demir et al. [17] reversed the MAC address' hashing, thus recovering and leaking the MAC address, de-anonymizing the device in the process. Vanhoef et al. [7] confirmed those findings in their paper and discovered, at the same time, that some devices were using bad UUIDs such as "`00:00:00...`".

C. Fingerprinting through metadata

While the MAC address randomization process have flaws in itself, metadata transmitted by Bluetooth LE (or BLE) devices also enables tracking [1], [10]. Devices, such as temperature sensors or object trackers, regularly emits payloads that contains application data as well as Bluetooth protocol-specific data. These payloads are not always subject to change and could therefore allow an attacker to identify a device even when the MAC address is randomized [1], [10], [11]. To illustrate more specific cases, Celosia and Cunche [10] demonstrated that payloads advertised by Apple and Microsoft devices through Bluetooth LE both included metadata that allowed an attacker to identify which kind of device is emitting (i.e. a certain mobile phone model from a specific brand or even a hearing aid device.) and included unique identifiers that were not changed when randomizing their MAC address.

D. Implementation flaws in security features

The *filter accept list* is a feature in Bluetooth that allows a device to filter transmissions by only accepting those from accepted devices and filtering out the rest [12]. Although useful, this can be used as a side channel due to the fact that a device may behave differently while in the presence of a trusted device or not [13], meaning that a Bluetooth device might not advertise its presence while connected to a trusted device, while it will advertise otherwise.

Zhang and Lin [13] showed that the *filter accept list* used by some Bluetooth LE devices significantly changed the device's behavior while interacting with other devices. While paired devices would get an answer (or a *SCAN_RSP) packet* while probing through *SCAN_REQ* packets, non-paired devices would not get such an answer.

An attacker could thus be able, through sniffing of Bluetooth LE communications, to identify the accepted MAC addresses for a certain period of time. While those devices may perform MAC address randomization, the authors speculate that there could be a period of time during which one of the devices has changed its MAC address while the other did not.

E. Probabilistic de-anonymization

Jouans et al. [8] show that regular MAC address changes still allow an attacker to identify a given device due to the fact that the probability of multiple devices changing their MAC address at the same time is low, hence differentiating a Bluetooth device from one another. Tan and Gary Chan [18] also presented techniques to connect multiple probe requests coming from a single Wi-Fi device that uses MAC address randomization, as this privacy-enhancing feature hinders statistical uses of Wi-Fi networks such as people counting.

These above attacks, mainly related to implementation flaws such as poorly-chosen cryptographic seeds, communication of identifiable data without any change when randomizing the MAC address, or even change of discernible behavior for an external attacker depending on the device's state are related to the data link layer of the OSI model [19].

IV. De-anonymization through physical side-channels

A. Usage of both RSSI and payload data for fingerprinting

Novel attacks in device de-anonymization rely on the physical layer of the OSI model [19], mainly through the emitting power of both Bluetooth and Wi-Fi devices. While older attacks such as those from Li and Zhu [20] and Cheng and Wang [21] did not have to deal with new security features like MAC address randomization, research from Ribeiro et al. [22] revealed in 2021 a passive Wi-Fi device tracking tool that used the Received Signal Strength Indicator (RSSI), combined with data contained in each data frame. This attack thus allowed an attacker to de-anonymize devices that used MAC address randomization in some cases. Akiyama and Taniguchi [9] combined both emitting power and payload contents from devices to de-anonymize these in 2024. They chose to formulate the set of generated MAC addresses as a linear

assignment problem, assuming that multiple devices might neither change their MAC addresses at the same time nor randomly change their RSSI. Moreover, the authors suggest re-using older generated MAC addresses to decrease accuracy of their de-anonymization technique.

B. Pure use of RSSI for de-anonymization

Despres et al. [14] proposed in 2023 a detection algorithm with the purpose to identify a tracking device through its RSSI. While MAC address randomization is a good way to prevent both device and user tracking, it also hinders the ability to identify a tracking device that follows a non-consenting person. In the same year, Gagnon et al. [15] also proposed the use of RSSI measurements as a way to fingerprint a device despite its MAC address changes. While it is really successful in a static environment (i.e. where neither the device nor the user moves) with a success rate of 97%, Gagnon et al. recognizes that their technique is not as effective against mobile targets (i.e. when the device and its user are in motion), mainly due to the fact that the relative position of the target device from the attacker's one plays a substantial role. However, as Gagnon et al. [15] mentioned in their paper, RSSI implementation is manufacturer-specific and could therefore lead to different results depending on the receiver used. The authors therefore proceeded with pre-processing of RSSI values in order to de-anonymize accurately. The authors also measured the accuracy difference of their attack using both a single receiver and multiple ones and noted that the use of multiple receivers improved the de-anonymization process and thereby device identification.

V. Possible counter-measures

A. RSSI randomizing

Gagnon et al. [15] proposed and evaluated several counter-measures against Bluetooth devices de-anonymization through their transmitting power, such as modulating its RSSI to make fingerprinting a specific device more difficult. It is both possible to change the RSSI of the device and that the device is not continuously transmitting at its full transmitting power. However, their results showed that, while not hindering significantly fingerprinting and de-anonymization, it hindered functionalities of those devices by increasing packet loss rates and reducing their connection range. It might then both increase power consumption of those devices due to the packet losses, while hindering their usability. Results from Gagnon et al. [15] are nevertheless incomplete due to the fact that their measurements were performed with sudden movements and not gradual ones. Moreover, both emitters and receivers were moving during the experiments. Gagnon et al. acknowledged in their paper that more realistic movements, instead of brutal ones, combined with static receivers might improve the accuracy of their attack.

B. Silent periods and location shifts

Huang et al. [23] proposed in 2005 the use of silent periods for wireless communications as a mean to enhance wireless devices location privacy. They suggested implementing the silent periods by combining a static period with a randomized one. It would thus make harder for an attacker to follow closely a given device user through its wireless connection. Gagnon et al. [15] built, based on previous work from Huang et al. [23], a similar counter-measure where the device would not emit any data (including the new randomized MAC address) for a defined period of time. They argue that the location change during this period will necessarily be greater than between two usual probing requests, rendering tracking more difficult. In their experiment, they chose to use physical behaviors like location shifts detected by the device's sensors, to randomize those periods of non-communication.

Both evaluations from Huang et al. [23] and Gagnon et al. [15] of these counter-measures demonstrated their effectiveness in hindering the ability of an attacker to pinpoint a specific device based only on its MAC addresses changes. It required however a significant location change while the device is not communicating to ensure that an attacker could not receive upcoming probe requests.

C. Extend randomization scope

Fenske et al. [5] suggested extending the use of randomized MAC addresses both before and after devices are associated with a Wi-Fi AP. While this could hinder AP features such as MAC address-based filtering, it still allows some kind of device fingerprinting on some devices evaluated by them.

While current operating systems, such as Apple's iOS, Google's Android or Microsoft's Windows do implement post-association MAC address randomization, implementations of this privacy feature can have flaws. Fenske et al. [5] observed that Android devices such as the Xiaomi Mi 9 Lite, do not perform any MAC address randomization even though it runs an operating system version with MAC address randomization enabled by default. Additionally, an attacker has the ability to know that a given device is nearby when it reconnects to a known Wi-Fi network, as the MAC address is randomized at the first connection but not re-randomized periodically. While this could be necessary for security measures such as MAC address filtering on Wi-Fi APs, it further hinders device users privacy. As Vanhoef et al. [7] shown, one could set-up Wi-Fi APs with commonly used SSID, such as university-specific wireless network *eduroam* to trick Wi-Fi devices into trying to connect to those, hence gaining the ability to collect their MAC addresses for the given network. This gives the ability for an attacker to track this specific device when it happens to be close to the real Wi-Fi APs, as its MAC address for this particular network is now known.

Moreover, "forgetting" a network does not necessarily reset the randomized MAC address. According to Apple documentation [24], the MAC address is only deleted immediately if it was not already forgotten in the last two weeks for older operating systems, or in the last 24 hours on latest operating systems versions such as iOS 18. In other cases, Apple claims to delete the MAC address as soon as the network is "forgotten" by the user. Google, on the other hand, claims in

their documentation [6] that, depending on the kind of Wi-Fi AP, it either uses a consistent but randomized MAC address in cases where a constant MAC address is required (i.e. for Wi-Fi networks relying on MAC address filtering), or randomizes it if some conditions are met related to both the DHCP lease expiry time and the time since the MAC address was generated. It should be noted that, although persistent randomization was introduced and enabled by default in Google's Android 10, released in 2019, the non-persistent one was introduced with Google's Android 12 in 2021.

D. Avoid leaking traceable and unique identifiers

While probing for known devices and Wi-Fi APs, devices transmit a wide range of metadata to facilitate connections [7], such as AP's SSID if it is probing for a Wi-Fi network or a device's MAC address to enable Bluetooth connection between two paired devices [13]. Even though exchanging those kind of data is essential to establish a link between two devices, some metadata exchanged during the process might help fingerprinting a device and thus greatly reduce the efficiency of the privacy enhancements of MAC address randomizing. For instance, Wi-Fi devices exchange "Information Element" (IEs) that are not mandatory [7] about the capabilities of the device such as its data rate. The presence or absence of such data, as well as the data in itself can greatly improve the fingerprinting accuracy of a device. Another Wi-Fi features found in those IEs, known as Wi-Fi Protected Setup (WPS), is used to announce its support by the probing device. It contains however an Universally Unique Identifier (UUID) [7], rendering it distinguishable from other devices, even if its MAC address was changed at some point. Furthermore, an attacker could retrieve the MAC address used to generate this UUID thus leaking other identifiable and unique data that could help de-anonymize a device. While not used as much nowadays, probe requests can also contain the Service Set Identifier (SSID) of the Wi-Fi AP to which the device would like to connect. The combination of probe requests for multiple SSIDs in a short period of time could thus be used to fingerprint a specific device [7]. Newer operating systems do not send the SSIDs they are looking for while probing, rendering it increasingly less useful to fingerprint and de-anonymize a Wi-Fi device. Furthermore, within each 802.11 frame lies a sequence number that is incrementally changed with each new packet, regardless of the operating system used [7]. While some devices reset this counter at some point, it is another identifiable piece of information that could be used to identify a specific device. Fenske et al. [5] also suggested using generic signatures for probe requests, and not including non-mandatory data. While some generic signature methods to generate probes exists [5], none are commonly used. Moreover, their research showed that most analyzed devices did not consistently use a single signature, either generic or not, but used a different one while being in idle state. For instance, some Android devices only used generic signatures while in idle mode.

E. Reusing previously generated MAC addresses

Akiyama and Taniguchi [9] argue that many Bluetooth LE devices identification methods relied on the presumption that, whenever a device changes its MAC address, the previous one will never be reused by the same device. They thus suggest to reuse those previously used MAC addresses, along with newly generated ones, albeit only for a certain period of time and not indefinitely. An optimal time interval is not specified.

F. Timing MAC addresses changes between multiple devices

Akiyama and Taniguchi [9] discovered that, in cases where a group of devices randomized their MAC address simultaneously, or at least in a short range of time, the accuracy of de-anonymization tools decreased significantly. An attacker would have trouble finding which MAC address matches with the tracked device due to this timing proximity, as multiple MAC addresses could correspond to it. It would however require coordination between those devices in order to decide when they have to change their MAC addresses. Such countermeasure, while only feasible in some contexts where devices are connected to one another, still appears to be quite effective.

VI. Challenges and New Directions

Although implementation-related de-anonymization techniques of both Bluetooth and Wi-Fi devices are now well-documented, the combination of both these techniques as well as metadata-related attacks (mainly using RSSI) may make it harder for a device (and its owner) to achieve privacy. Some research has already been done on this subject [22]; targeting other unique identifiers advertised by both, Bluetooth and Wi-Fi devices, such as device names, service UUIDs and above all manufacturer specific data [10], combined with RSSI tracking and the use of multiple receivers [15] could improve tracking techniques' accuracy and further impede users' privacy.

On the defensive side, reducing identifying metadata, such as aforementioned manufacturer specific data [10], as well as implementing silent periods [15] would make it more difficult for an attacker to follow a specific device. Research on the effectiveness of those silent periods relative to their duration, as well as its impact on device usability could consequently enable new countermeasures to be used at a larger scale.

An special but important case to discuss stems from the proliferation of devices such as Apple AirTags that are designed help people to find personal objects through the crowdsourced reporting of Bluetooth signals, and which bear substantial abuse potential. In order to prevent abuse in stalking and to allow stalking victims to detect AirTags following them, the iPhone OS does use tracking mechanism to see if an unwanted device (e.g., a not-registered AirTag) is being seen multiple time over a long period of time. Research into enhancing privacy of Bluetooth and Wi-Fi-enabled devices' users while not hindering the detectability of trackers or enabling stalking with AirTags and similar devices might be of interest.

VII. Conclusion

In this paper, we comprehensively survey both de-anonymization attacks and their corresponding countermeasures in wireless communication. Privacy-enhancing techniques that prevent an attacker from identifying and tracking a device in Bluetooth and Wi-Fi communication have been implemented for many years, perhaps the main one is MAC address randomization. In our paper, we consider a passive adversary who does not break cryptographic schemes and protocols. Our adversary is able to de-anonymize a device based on metadata such as RSSI, timings of MAC randomization and presence of manufacturer-specific fields [10].

Likewise, we also considered an adversary who is able to exploit flawed implementation. MAC address randomization can happen at different levels, either during both probing and association for Wi-Fi APs [4], or at regular intervals like in Bluetooth LE devices [12]. Recent operating systems chose to implement randomization at every stage, from probing to the association between devices and Wi-Fi APs. However, those implementations leave gaps that could lead an attacker to identify a device. First, randomization needs a seed that should be initialized according to defined standards [16]. Second, some devices are not implementing those standards correctly [7], making randomized MAC addresses predictable. Moreover, probe requests and advertisement packets send metadata beyond the required ones. Wi-Fi devices are not immune to fingerprinting through sent metadata. For example, Wi-Fi Protected Setup (WPS) uses a Universally Unique Identifier (UUID) that is generated through a flawed implementation when no hard-coded identifier is available.

Acknowledgment

We gratefully acknowledge the Brussels-Capital Region - Innoviris for financial support under grant numbers 2024-RPF-2 and 2024-RPF-4, and the CyberExcellence programme of the Walloon Region, Belgium (grant 2110186).

References

[1] J. K. Becker, D. Li, and D. Starobinski, "Tracking anonymized bluetooth devices," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 3, pp. 50–65. [Online]. Available: https://doi.org/10.2478/popets-2019-0036

[2] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, "A study of MAC address randomization in mobile devices and when it fails," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 365–383. [Online]. Available: https://doi.org/10.1515/popets-2017-0054

[3] J.-C. Zúñiga, C. J. Bernardos, and A. Andersdotter, "Randomized and changing MAC address state of affairs," num Pages: 19. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-madinas-mac-address-randomization

[4] Implement MAC randomization. Consulted on 12-01-2025. [Online]. Available: https://source.android.com/docs/core/connect/wifi-mac-randomization

[5] E. Fenske, D. Brown, J. Martin, T. Mayberry, P. Ryan, and E. Rye, "Three years later: A study of MAC address randomization in mobile devices and when it succeeds," *Proceedings on Privacy Enhancing Technologies*, vol. 2021, no. 3, pp. 164–181. [Online]. Available: https://doi.org/10.2478/popets-2021-0042

[6] MAC randomization behavior. Consulted on 12-01-2025. [Online]. Available: https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

[7] 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 *AsiaCCS 2016*. ACM, pp. 413–424. [Online]. Available: https://doi.org/10.1145/2897845.2897883

[8] L. Jouans, A. C. Viana, N. Achir, and A. Fladenmuller, "Associating the randomized bluetooth MAC addresses of a device," in *CCNC 2021*, pp. 1–6, ISSN: 2331-9860. [Online]. Available: https://doi.org/10.1109/CCNC49032.2021.9369628

[9] S. Akiyama and Y. Taniguchi, "A device identification method from BLE advertising packets with randomized MAC addresses based on regression of received signal strength," *IEICE Communications Express*, vol. 13, no. 3, pp. 64–67. [Online]. Available: https://doi.org/10.23919/comex.2023XBL0157

[10] G. Celosia and M. Cunche, "Saving private addresses: an analysis of privacy issues in the bluetooth-low-energy advertising mechanism," in *MobiQuitous 2019*. ACM, pp. 444–453. [Online]. Available: https://doi.org/10.1145/3360774.3360777

[11] J. Wu, P. Traynor, D. Xu, D. J. Tian, and A. Bianchi, "Finding traceability attacks in the bluetooth low energy specification and its implementations," in *USENIX Security 2024*, ser. SEC '24. USA: USENIX Association, 2025. [Online]. Available: https://www.usenix.org/system/files/usenixsecurity24-wu-jianliang.pdf

[12] Core specification 6.0. Consulted on 12-01-2025. [Online]. Available: https://www.bluetooth.com/specifications/specs/core60-html/

[13] Y. Zhang and Z. Lin, "When good becomes evil: Tracking bluetooth low energy devices via allowlist-based side channel and its countermeasure," in *CCS 2022*, ser. CCS '22. Association for Computing Machinery, pp. 3181–3194. [Online]. Available: https://doi.org/10.1145/3548606.3559372

[14] T. Despres, N. Davis, P. Dutta, and D. Wagner, "DeTagTive: Linking MACs to protect against malicious BLE trackers," in *SNIP2+ 2023*, ser. SNIP2+ '23. Association for Computing Machinery, pp. 1–7. [Online]. Available: https://doi.org/10.1145/3609396.3610544

[15] G. Gagnon, S. Gambs, and M. Cunche, "RSSI-based attacks for identification of BLE devices," *Computers & Security*, vol. 147, p. 104080. [Online]. Available: https://doi.org/10.1016/j.cose.2024.104080

[16] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ser. IEEE Standard for Information Technology Part 11, 2012. [Online]. Available: https://ieeexplore.ieee.org/document/STDSU97218

[17] L. Demir, M. Cunche, and C. Lauradoux, "Analysing the privacy policies of wi-fi trackers," in *WPA 2014*. ACM, pp. 39–44. [Online]. Available: https://doi.org/10.1145/2611264.2611266

[18] J. Tan and S.-H. Gary Chan, "Efficient association of wi-fi probe requests under MAC address randomization," in *INFOCOM 2021*, pp. 1–10, ISSN: 2641-9874. [Online]. Available: https://doi.org/10.1109/INFOCOM42981.2021.9488769

[19] H. Zimmermann, "OSI reference model—the ISO model of architecture for open systems interconnection," in *Innovations in Internetworking*. Artech House, Inc., pp. 2–9.

[20] Y. Li and T. Zhu, "Gait-based wi-fi signatures for privacy-preserving," in *AsiaCCS 2016*. ACM, pp. 571–582. [Online]. Available: https://doi.org/10.1145/2897845.2897909

[21] L. Cheng and J. Wang, "How can i guard my AP?: non-intrusive user identification for mobile devices using WiFi signals," in *MobiHoc 2016*. ACM, pp. 91–100. [Online]. Available: https://doi.org/10.1145/2942358.2942373

[22] R. H. Ribeiro, B. B. Rodrigues, C. Killer, L. Baumann, M. F. Franco, E. J. Scheid, and B. Stiller, "ASIMOV: a fully passive WiFi device tracking," in *IFIP Networking 2021*, pp. 1–3, ISSN: 1861-2288. [Online]. Available: https://doi.org/10.23919/IFIPNetworking52078.2021.9472786

[23] Leping Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *WCNC 2005*, vol. 2. IEEE, pp. 1187–1192. [Online]. Available: https://doi.org/10.1109/WCNC.2005.1424677

[24] Use private wi-fi addresses on apple devices. Consulted on 12-01-2025. [Online]. Available: https://support.apple.com/en-us/102509