A Study of Security Issues of Eduroam Networks in Portugal

Luís Miguel Batista
DETI/IEETA, LASI, University of Aveiro, Portugal

Hélder Gomes
ESTGA/IEETA, LASI, University of Aveiro, Portugal

João Rafael Almeida
DETI/IEETA, LASI, University of Aveiro, Portugal

Abstract

Enterprise Wi-Fi networks provide seamless connectivity for businesses and public entities. In educational settings, these networks are essential for delivering services to students. Eduroam is one of the most widely recognized university Wi-Fi enterprise networks. It uses 802.1x protocols and TLS tunnels to establish mutual authentication. Eduroam caters to a diverse population of students and faculty worldwide, managing a vast number of unregulated devices, some of which, require manual configuration to operate in a secure setting. This study aims to evaluate the security robustness of the 802.1x protocol, particularly within the Eduroam framework. A comprehensive study was conducted to examine compliance with institutional instructions for network configuration guidance. The results from 91 Portuguese institutions using Eduroam revealed that many lacked knowledge of Wi-Fi security. This lack of awareness is then passed on to users, resulting in vulnerable connections.

2012 ACM Subject Classification Security and privacy → Operating systems security; Security and privacy → Intrusion detection systems; Security and privacy → Security requirements; Security and privacy → Formal security models

Keywords and phrases Eduroam, Wi-Fi, Credential stealing, Attack, Network, Security

Digital Object Identifier 10.4230/OASIcs.SLATE.2024.14

Funding This work has received support from the EU/CINEA Innovation and Networks Executive Agency under grant agreement No 29335026.

1 Introduction

Security resembles a key aspect of modern society and is defined by the lack of threats or danger. The way devices connect and offer exceptional mobility for users can be attributed to Wi-Fi technology, which emerged as an innovative and dominant force in digital communication. Nevertheless, this advancement in wireless communication has also raised various security concerns. The ease of data interception on these types of communications is alarming, only requiring a network card or a rogue Access Point (AP). This marks challenges in safeguarding data and user privacy. Business and governmental contexts where sensitive data is often transmitted, including personal information, pose even more critical concerns and raise the need for robust security measures [17].

Attacks often involve obtaining users' data and are performed by malicious actors attempting to inflict damage. Such occurrences are more common online, where some association exists between the participants. Cybersecurity has a crucial duty in leading with risks associated with the internet and inter-network communication, conveying the obligation of protecting the security and integrity of IT systems in the scene of evolving oppositions and common network vulnerabilities. As per the European Union Agency for Cybersecurity (ENISA), from their CWE 2023 records, bad authentication constitutes

© Luís Miguel Batista, Hélder Gomes, and João Rafael Almeida;
licensed under Creative Commons License CC-BY 4.0

4.79% of the top 10 Common Weakness Enumerations (CWE) in terms of critical severity. Vulnerabilities of such status are deemed extremely exploitable and pose significant risks to systems and related data [4].

Wi-Fi is a better solution for user network connection compared to the use of physical cables, it serves as a fitting method for providing internet access to enterprise frameworks. APs, the devices that establish and manage these connections, can be especially susceptible to exploitation. Most AP exploits come from the intrinsic attributes of Wi-Fi as a broadcast communication medium transmitted via radio frequencies [12, 19, 3]. The shared essence of Wi-Fi communication unfolds paths for numerous attacks, including Denial of Service (DoS) [23, 18], Traffic decryption [22], and Man-in-the-Middle (MitM) attacks [10, 2, 21].

Universities often feature mass-use Wi-Fi networks, with the Wi-Fi enterprise Eduroam network as a prominent example. The Eduroam scheme offers an overarching complete networking service globally, specially adapted for the educational and research community. It streamlines internet access for users on the go, making use of the customizable IEEE 802.1x authentication protocol suite. By inspecting the security of this network, three important constituents can be underlined: the Eduroam network infrastructure, the educational institution involved, and the end-users devices.

Eduroam's security is heavily dependent on the correct use and configuration of a certificate on each device. This certificate verifies the legitimacy of the Authentication Server (AS) responsible for authenticating users of a particular institution. Institutions are accountable for providing login details and correctly guiding users through the setup process. Nonetheless, problems arise with some setup guides, and many devices have vulnerable settings by default, failing to appropriately alert users about possible network risks. Such situations produce susceptibilities, with users prone to accidentally compromise their credentials to attackers using rogue APs. These problems are not exclusive to the Eduroam service but come from the underlying 802.1x and WPA-Enterprise authentication methods. Warnings related to untrusted certificates are frequently overlooked by users, or devices might not display alerts at all, allowing attackers to simulate legitimate networks and illicitly obtain credentials [16, 13, 5, 25, 23, 18, 22].

This paper investigates potential problems within Wi-Fi guides of the University of Aveiro (UA) and other national institutions adherent to the Eduroam networking service. In addition to performing practical assessments, it evaluates the reliability and correctness of publicly available configuration guides on all main Operating Systems (OSes) - Windows, ioS, macOS, Linux, and Android. Through the development of a thought questionnaire, various misconceptions are identified within many institutions' instructions, inadvertently guiding users to end with vulnerable connections. Also, this work aims to provide valuable insights and recommendations to facilitate a comprehensive evaluation and effective mitigation of these security concerns.

The remainder of this paper is structurally organized. Section 2 provides insights on Wi-Fi communication procedures, standards, and susceptibilities. Section 3 elucidates the process used to derive the experiments and provides the assessment results. The current landscape of national institutions' guidance on the Eduroam network configuration is inspected in Section 4. From the obtained results, various discussions and recommendations are given in Section 5. Finally, Section 6 summarizes this study's accomplishments.

2 Background

Wi-Fi communications have been targeted by various attacks, causing significant damage to countless devices. Common threats include data theft, eavesdropping, network disruption, denial of service, and unauthorized access. Compromised networks are often challenging to detect, and by the time a user exchanges confidential information, the damage is already done. Given the vulnerability of individuals accessing wireless networks to potential attacks, establishing secure connections becomes a crucial and effective means to mitigate further risks.

2.1 Eduroam

Eduroam is a widely adopted enterprise Wi-Fi provider used by numerous universities and educational institutions for seamless network roaming. It offers an infrastructure based on WPA-Enterprise, allowing users from one Eduroam member institution (home institution) to travel to another Eduroam member institution (guest institution) and connect to the Eduroam Wi-Fi network using their home institution credentials. A hierarchy of RADIUS servers facilitates this connectivity [15], as illustrated in Figure 1.

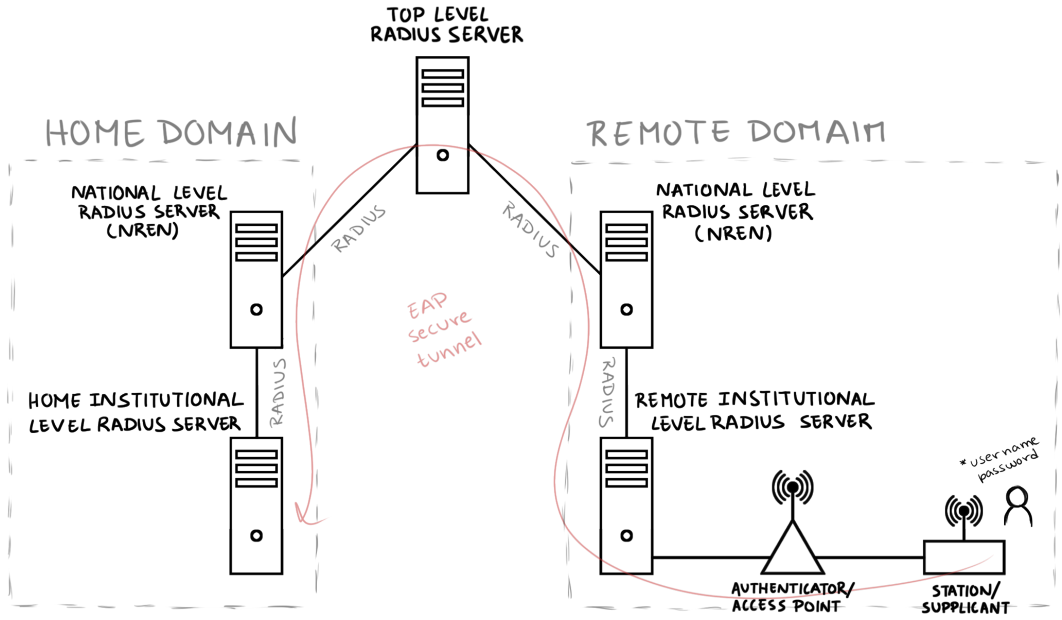

Figure 1 Eduroam hierarchy structure diagram.

Eduroam's widespread adoption is evident, with 79 distinct institutions in Portugal alone using this educational roaming service as of late 2023 [1].

When establishing a first-time connection to an educational institution´s Wi-Fi network, like Eduroam, users are typically prompted to input a set of authentication configurations, including a Certificate Authority (CA) Certificate. This process aims to provide a means for authentication of the network AS and, this way, prevent users from connecting to rogue networks, which could potentially jeopardize their credentials. This prompts the question of why users frequently neglect to configure a secure connection and raises concerns about which OSes are more susceptible to this oversight. Addressing these issues and understanding user behavior could pave the way for potential solutions or workarounds to enhance current configuration methods, with the ultimate goal of increasing the number of users with a secure Wi-Fi connection.

2.2 Evil Twin

The significant role that the internet plays in people's daily lives, combined with the need to stay updated with recent events, often leads individuals to make impulsive decisions when connecting to a network AP. The sphere of attacks surrounding networks is immeasurable [14, 23, 20, 11]. The Wi-Fi domain suffered various amendments, refactors, and new protocols over the years. In addition to performance improvements, most changes are made to overcome exploits. Even today, vulnerabilities should be a constant concern to network administrations.

Evil Twin attacks pose a serious threat in WPA enterprise environments, aiming to trick users into connecting to a fraudulent access point for data theft or surveillance. This risk is heightened when users leave their Wi-Fi settings enabled without considering the potential danger of connecting to a malicious access point. The severity of these connection attempts increases further when a device's Wi-Fi configuration is inadequate, especially if the device fails to verify the legitimacy of the authentication server's digital certificate [24].

Deploying Evil Twin attacks requires minimal equipment – a computer and an external medium to high-end AP with a capable Wi-Fi adapter are sufficient for this purpose [6]. The attack involves simulating an AP emitting the SSID of the target network along with a fake AS to capture the credentials of users with devices lacking a certificate for AS validation. This is adequate to lure devices familiar with the target network into attempting to connect to the fraudulent provider, potentially leading to the exchange of critical data if the users' devices are not properly configured.

2.3 Studies on Eduroam vulnerabilities

Other authors have already made studies focused on WPA-Enterprise Wi-Fi security analysis within several aspects [7, 16, 9, 15, 8, 24]. Bartoli et al. [7] assessed WPA-Enterprise vulnerabilities by deploying Evil Twin attacks at the University of University of Trieste, Italy. A couple of considerations, countermeasures, and ulterior analysis on discovered susceptibilities are presented. Their results show that clear text and hashed passwords captures sum to 200, corresponding to 36.1% of all captures. Their examinations were performed using a Raspberry Pi running the Kali Linux OS connected to an external wireless adapter. The Linux packages used to simulate the Evil Twin attack were hostapd-wpe and freeRadius-WPE, simulating the rogue AP and rogue authentication server respectively.

Very similarly, Perkovic et al.'s study [16] also verifies this wireless enterprise matter. Their experimental setup is identical to the previously described work. In addition, they analyze Eduroam CAT's reliability, indicating that these are often incorrectly configured, suggesting improvements and fixes.

An earlier research from Brenza et al. [9] uses MITM attacks to also verify credential capturing ratios. It is performed with a custom-modified version of the hostapd Linux package that keeps a connection between the user and their rogue network, effectively transforming an Evil Twin into a MITM attack. From 507 captures, they showed 264 wrongly configured devices vulnerable to the developed attack. Finally, some countermeasures were proposed.

Palama et al. [15] demonstrated a comprehensive study involving both OS susceptibilities analysis and users' questionnaires to break down user awareness of Wi-Fi security. They also performed real-world scenario evaluations in controlled environments at the University of Rome "Tor Vergata", Italy, and in the wild with aggregation by some student areas at the University of Brescia, Italy. Experiments indicate that users' vulnerability ratio can range from 18 to 39 percent.

Wang et al. [24] centered their attention on understanding OS' susceptibilities on certificate validation. They also examined problems presented by organizations when providing Wi-Fi configuration guides. They conclude that many OS are susceptible to Evil Twin attacks because of weak configuration interfaces and unnoticeable user interface security warnings.

3 Security Assessment Methodology

The survey procedure was straightforward: open the computer, launch a 15-minute attack, and wait for users to try to connect, without forcing their deauthentication. The attack follows a very concise set of interactions, depicted in Figure 2. As the fake AP must be compliant with the norms established for Wi-Fi communications, it starts with a common probe swapping. When the STA effectively tries to start a connection, an initial user identity request is performed and a series of authentication specifications are exchanged, including the supported cipher suites used to establish the EAP-protected tunnel.

The key nuance in the first phase is that the Supplicant (SUP) is not sent a trusted X.509 certificate to authenticate the AS, but a self-signed one instead. If the SUP is correctly configured with a proper certificate, it easily detects that it is in the presence of a fake AS since the received certificate is not valid. When not correctly configured, the SUP accepts the received certificate as valid and proceeds with the standard connection to the fake network, establishing the EAP-protected tunnel through which the user-specific authentication occurs. In the case of the MSCHAPv2 protocol, the authentication is conducted via an exchange of challenges. An initial challenge (a string of random bytes) is sent from the AS to the SUP. The SUP then takes the challenge and the user password, derives a hash, and sends it to the AS. Then, as the fake AS has no way of confirming the received hash, it simply accepts it and sends a success message to the SUP. Despite all this being done under a secure tunnel, the fake AS can read all the traffic inside it, meaning it can capture the hashed password. After the MSCHAPv2 authentication, the secure EAP tunnel is dismantled and the vulnerable device's association fails as it cannot establish a secure connection with the AP. The vulnerable device is added to a deny list to prevent further connection attempts.

All assembled data (user identifiers and hashes) served to acquire analytical metrics illustrating the percentage of users with vulnerable connections. These stats would be significantly leveraged by a possible differentiation of the underlying OSes, a challenging endeavor when considering the monotony of the Wi-Fi communication standard. As the mitigation of user DoS is prioritized, it is not possible to keep an open connection with the vulnerable STA and hope for the exchanging of packets containing OS-descriptor fields. With this, a tentative possibility could stand on analyzing any authentication packet exposing characteristics of its source. One of those packets is the "Client Hello", at the beginning of the establishment of the protected EAP tunnel, which manifests the STA TLS version, its compression methods, cipher suites, and other specifications. By analyzing a wide range of these types of packets, it might be possible to establish a pattern to uncover the intrinsic OSes.

To provide an initial overview of the Wi-Fi security landscape at the UA and showcase the tools in use, preliminary experiments were carried out at two different locations within the institution. Following the same procedure, these experiments were conducted with surveillance and permission from the appropriate entities. The collected data, utilized for statistical purposes, was subsequently discarded. Lastly, global experiments were conducted, categorizing users based on their level of IT expertise.

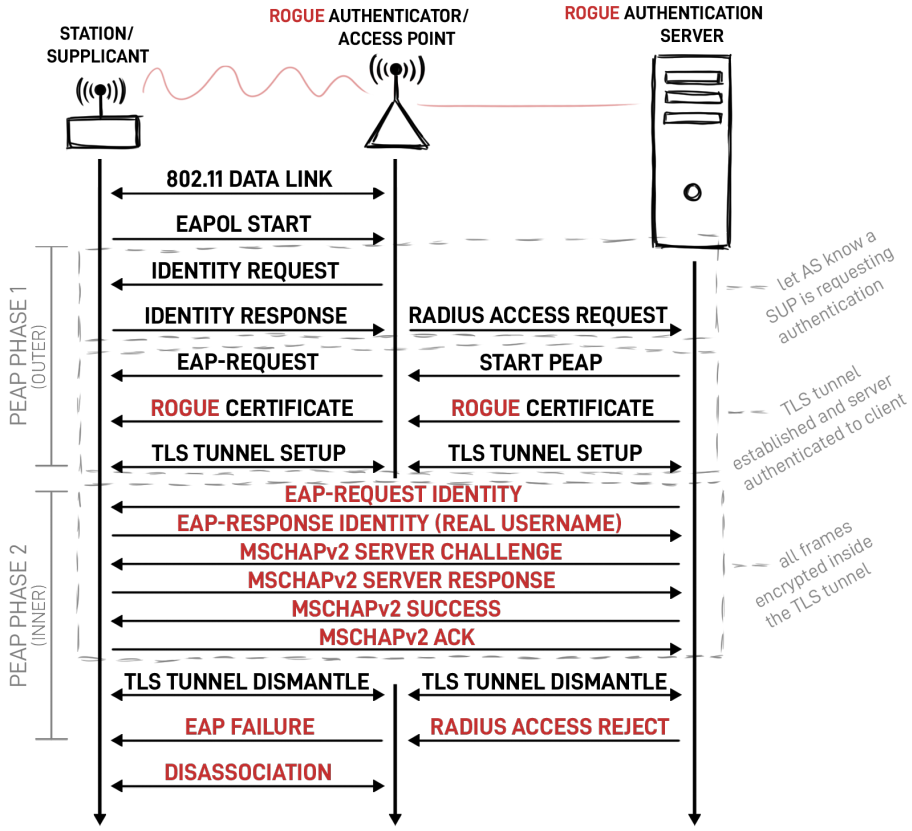

Figure 2 Attack interaction diagram.

The first phase took place within the university's library, where fewer users than anticipated connected to the fake network. The subsequent phase was conducted while walking through the central campus, resulting in a higher number of users being captured. This increase was attributed to the continuous movement of students, highlighting the vulnerability introduced by roaming. The selection of these two specific locations was merely based on the fact that these areas seemed to have a larger number of people during the times of the experiments.

Drawing insights from the initial study, areas for improvement were identified: i) enhancing attack mobility, ii) effectively inducing user deauthentication, and iii) refining real-time attack visualizations. Additionally, the prospect of analyzing specific student groups within study spheres was explored to identify those with the highest percentage of susceptible connections.

3.1 Experimental Setup

The experiments aimed to replicate an Evil Twin attack, involving the setup of a fake AP emitting Eduroam's SSID. Subsequently, client devices were deceived into incorrectly connecting to the rogue network. All procedures were carried out using the specified hardware and software modules.

The machine specifications included a VMware Workstation 17 Player instance allocated with 4GB of RAM and 4 processors. An external ALFA AWUS036ACHM wireless USB adapter was used for the network connectivity.

The chosen OS for the Virtual Machine (VM) was Kali Linux, as this specific Linux distribution already contains a lot of features pre-installed for attacking and analyzing results. The hostapd-mana[1] package was installed to provide an out-of-the-box almost ready-to-use software capable of transforming the Wi-Fi adapter into a forged enterprise AP linked to a fake AS configured with the certificate to be presented to the client for AS authentication. A Python script was developed to automate the process, initializing the AP, executing hostapd-mana, printing the desired output, and adding users to a deny list to mitigate further DoS.

3.2 Global Experiment with Segregated Users

The campus comprises of approximately 50 buildings housing various services and research areas. Evaluating each building individually is time-consuming and, in certain scenarios, may lead to duplicated results. To address this, users were categorized into groups based on the assumption that some would have more vulnerable connections than others. A fundamental classification of different departments by study areas facilitates a more concise and straightforward analysis. In light of this, the 16 research domains within the UA can be grouped into three study spheres: i) Information Technology; ii) Holistic Sciences and Management; and iii) Health and Education. Additionally, three additional regions have been established. The first represents a general environment accessible to any student, the second assesses the degree of secure connections for top-level positions (administration, rectory members), and the third simulates a boundary substantiating the actual extent of the attack.

3.3 Assessment Results

An assessment was planned at the UA to better demonstrate the tools' capabilities and obtain more data about users' wireless security. This assessment was carried out for three consecutive days. Each day every area was struck for around 10 minutes, and the MAC deny list was cleared at every new location, meaning a user could only be caught once per location on the same day, but could be caught again at a different location on the same day.

The gathered results depicted a general view with around 33.21 percentual points of vulnerable users. A total of 798 users were captured, of which 533 were considered secure and 265 were found vulnerable. Regarding local percentage descriptions, Information Technology departments had approximately 28% vulnerable users. Holistic Sciences and Management kept 38%, just like in the second assessment. The general campus area saw a small decrease to 28%. On the north side border of campus, a percentage of 40 was registered. In the Rectory area, 29 was the percentage recorded. Finally, Health and Education saw an increase to 31%.

4 National Landscape

Considering the results of this security assessment, several questions have arisen. While the assessment demonstrated a real problem, it remains unclear what is the source of the problem (whether this issue stems from user behavior or the services themselves). If it is a shared fault, is this situation unique to the UA, or is it a global problem?

[1] `https://github.com/sensepost/hostapd-mana`

4.1 Questionnaire

A questionnaire about Eduroam configuration instructions from all Portuguese institutions was developed to help understand how well national organizations instruct their users about enterprise Wi-Fi connections. A publicly available online Eduroam webpage allowed to take 90 institution names adherent to Eduroam [1], with one more later added to the list. The questions were based on aspects taken from previous studies that could be relevant to ensure that users end up with secure connections. The main questions include:

1. Can the instructions be found with a "[institution name] eduroam configuration" web search?
2. Are configuration instructions provided?
3. Are users led to not configure a CA Certificate?
4. What is the type of the CA Certificate that validates the Authentication Server?
5. What is recommended to be placed in the Anonymous Identity field?

Attained questionnaire data suggests that many institutions' administrations need more expertise and distress to provide correct, complete and concise guidance. For example, many of the provided instructions lead users to skip selecting a CA Certificate, which constitutes one of the main reasons for devices to fall into Evil Twin attacks.

4.2 Findings

Unexpectedly, upon filling out the questionnaire, the most bothersome misguides stand on leading users to misconfigure their Windows OSes. A lot of institutions' guides are found indicating users to deviate their path from using the automatic Windows configuration and go through advanced settings all to, after around 10 steps, having the OS completely ignoring whichever certificate is provided by the AS. When this happens, not even a warning indicating that the certificate could not be verified will appear. This type of misguiding is not registered on macOS and iOS, most likely due to these OSes not allowing it.

With the questionnaire results it is even more evident that most enterprise Wi-Fi vulnerabilities are caused by institutions' negligence. Of the 91 analyzed institutions, only 54 have Eduroam configuration instructions publicly available online. Of these 54 institutions, 34 had at least one wrong OS guide. Also, only 10 out of the 54 institutions present instructions for all main OSes, meaning the remaining 44 are missing at least one OS configuration guide. Figure 3 illustrates the percentage of instruction metrics. Figure 4 shows the number of wrong instructions per OS, and Figure 5 compares the recommendations of different institutions for filling in the "Anonymous Identity" field. Taking as an example the performed assessment at the UA which showed 33% of vulnerable users, it raises concerns about how much this percentage would be on other institutions with sparse configuration guides.

5 Discussion

The low mobility of users inside the library in the initial tests posed challenges for devices already connected to Eduroam, inhibiting smooth transitions between APs. Furthermore, only about one-fifth of the devices that detected the fake network had their hashes captured. The prevalent device types might contribute to the relatively low ratio of clients with vulnerable connections. Typically, users lean towards using laptops more than smartphones in study environments. In general, Windows and macOS devices (predominant laptop OSes) have robust self-guarding mechanisms against Wi-Fi configuration mishaps. Because of these adversities, the subsequent assessments related to the General area were performed near

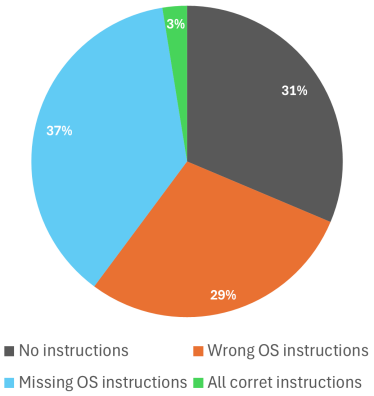

Figure 3 Institutions' instructions metrics percentage.

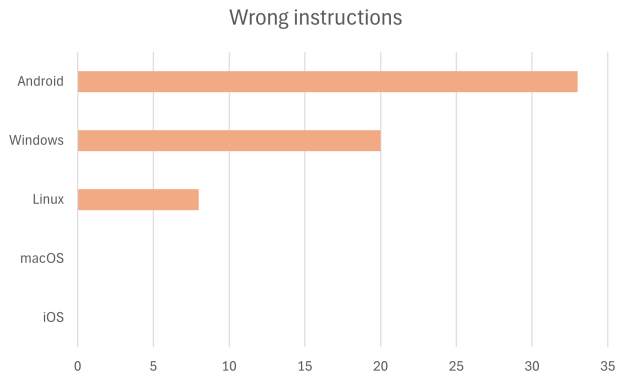

Figure 4 OSs' wrong instructions comparison.

the library entrance. During casual strolls across the campus, the ratio of captured hashes versus secure connections was approximately one-third. In this context, it is assumed that smartphones emerged as the primary category of connected devices. Given that Android is the most widely used and potentially susceptible phone OS due to its flexibility in Wi-Fi configuration, this elucidates the higher ratio of vulnerable clients in this scenario.

5.1 Organization Hurdles

Organizations affiliated with Eduroam provide users with a set of credentials for network access, which concurrently serve as login credentials for other platforms under a Single Sign-On (SSO) framework. Therefore, it becomes imperative to mandate the provision of reliable and regularly updated tutorials guiding users through the proper steps to establish secure connections. Even with brief preliminary experiments lasting no more than a couple of minutes, it became evident that approximately twenty to thirty percent of students exhibit insecure configurations for Eduroam. While this may be attributed to a misconception on the part of the users, UA and other institutions should proactively implement measures to minimize such occurrences. Recognizing that users are not inherently equipped with in-depth knowledge of Wi-Fi enterprise security is crucial, especially given that their initial exposure to enterprise networks typically occurs at the beginning of their university journey.

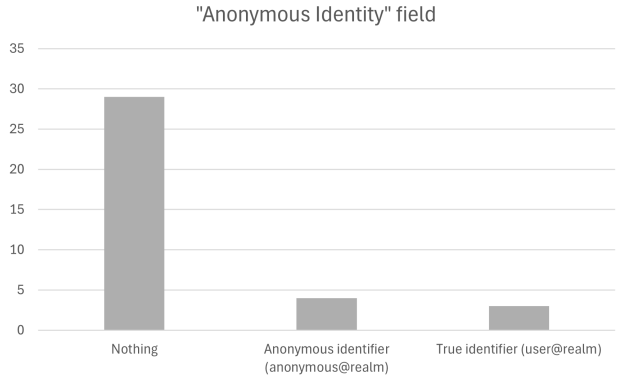

Figure 5 "Anonymous Identity" field filling comparison.

5.2 Assembling Findings

Experiments served as a foundation for initial considerations. In Phase 1 (outer phase), the process involves establishing a TLS-protected EAP tunnel, during which a device assesses the characteristics of available networks, including the presented AS certificate. Among the configuration options, "Anonymous Identity" stands as a relevant entry. When this field is specified, in Phase 1, the actual email is not transmitted; instead, the information filled in the "Anonymous Identity" is used. Conversely, if the "Anonymous Identity" field is left empty, the real email is transmitted.

A different scenario unfolds in Phase 2 (inner phase), which is associated with user-specific authentication. When a CA Certificate is established, and the connection is automatically aborted or users opt not to connect to a fraudulent AP when their OS presents that option, Phase 2 is bypassed. However, if users connect to the fraudulent AP, either due to the absence of a configured CA Certificate or by disregarding warnings about the lack of trust in the network, Phase 2 is activated. During this phase, it is possible to capture the user's identifier (often corresponding to the email) and the associated hashed password. The visual representation of both phases can be found in Figure 6.

Applying the acquired concepts, the next step involves pragmatically testing and validating any unresolved issues. To achieve this, a set of procedures essential for addressing vulnerabilities in Eduroam networks within organizations was delineated. The findings underscore the pivotal role of user awareness in mitigating risks associated with device misconfiguration. Notably, Apple showcases elevated levels of user awareness owing to its design and the user-friendly presentation of information. For instance, MacBooks consistently display certificates during network connections and promptly alert users to any new certificates, significantly enhancing user awareness and reducing the likelihood of device misconfiguration and susceptibility to attacks. However, it's crucial to acknowledge that the absence of information, poor configuration guides and ineptly trained IT staff may lead users to accept certificates without recognizing the change. This challenge necessitates awareness campaigns to educate users about these issues and promote a more vigilant approach to network security.

Conversely, Android devices exhibit diverse levels of user awareness, influenced by factors such as the phone model and manufacturer. While some Android devices have incorporated security enhancements, others lag, creating inconsistencies that could elevate risks for users on less secure devices. Emphasizing the importance of user education, it is acknowledged

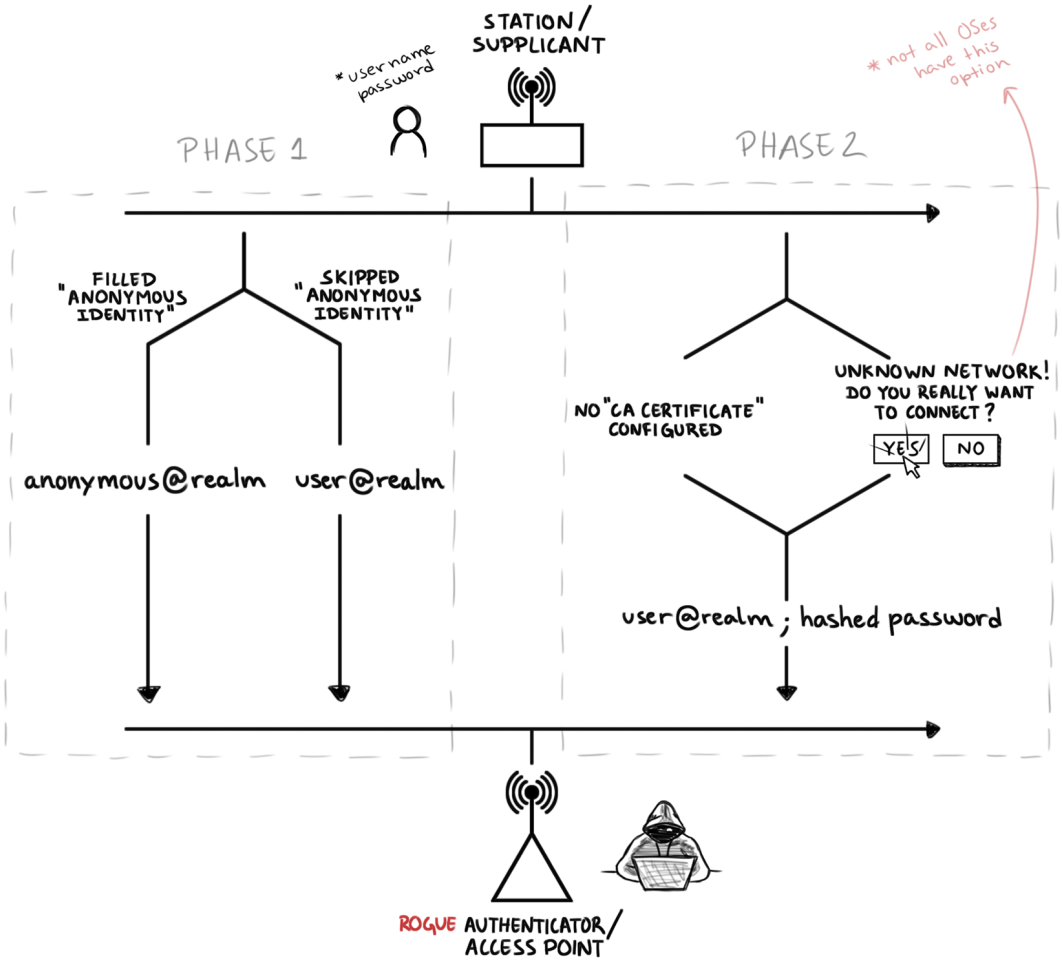

Figure 6 Authentication phases' susceptibilities.

that increasing awareness can significantly diminish the risks associated with improper device configuration. Educating users about potential risks and providing clear, concise configuration instructions can substantially bolster overall security.

5.3 Recommendations

The disclosed problems can only be mitigated with the active collaboration between institutions and their users. First of all, institutions should start by learning and properly consolidating the most common Wi-Fi vulnerabilities. Then, they should conduct impactful security awareness campaigns using a diverse range of media formats to engage and educate. Campaigns should dwell on the real-world consequences of security lapses, providing practical, actionable advice. Additionally, incorporating interactive elements, such as security assessments similar to the one conducted in this study, with direct user involvement, can enhance both learning and retention.

The development of clear, concise, and user-friendly guidelines to assist users in securely configuring their devices should be a priority for organizations. These guidelines hold particular importance for new users who may face challenges performing such configurations. In the Eduroam questionnaire investigation, it was examined how Portuguese institutions

guide users in configuring their devices and there were found instances of misleading information recommending against using certificates or suggesting default configurations. This information must be accurate, easily accessible, and presented in a user-friendly format. Providing instructions step-by-step with visual aids like screenshots or instructional videos can substantially enhance user understanding. Establishing a support channel for users to seek help or clarification is also instrumental in improving the configuration process and fostering compliance with secure practices.

More identified concerns relate to frequent certificate updates, leading to alerts from the systems of users' devices. Excess of these alters can potentially assuage users over time, making them accept whichever certificate is presented without bothering about it. To mitigate the impact of frequent certificate swaps and reduce user friction, organizations should consider implementing a certificate signed in a chain anchored by a CA root with long-term stability. Moreover, these warnings can be circumvented in some OSes by configuring them to not alert users when in the presence of untrusted AS certificates. This implies that users can never enter rogue networks as they cannot give acknowledgment for the OS to accept the fake certificate.

At last, performing assessments similar to those outlined in this study provides a comprehensive overview of the cybersecurity landscape of institutional users. This can also help institutions corroborate the efficacy of their security guidance.

6 Conclusion

This study's examination of institutional Eduroam security allowed us to understand the current state of network security, pointing out areas for improvement. The findings underline the crucial importance of systematic security examinations, the employment of strong security methods, and the constant need for user education and enhancement of device configuration guidance.

Lately, comprehensive research has been orchestrated to examine compliance from institutional instructions for network configuration guidance. The results show that many of the analyzed institutions lack knowledge of Wi-Fi security. This absence of awareness is then passed on to users, who end up with vulnerable connections. All this is reflected in the number of hashed passwords that were intercepted in empirical assessments. Current recommendations not only address these vulnerabilities but also fortify the resilience of users against various security threats.

References

1 Institutions in portugal that use eduroam. `https://eduroam.pt/instituicoes-ligadas/`. Accessed: 2023-11-14.

2 Mohamed A Abo-Soliman and Marianne A Azer. A study in wpa2 enterprise recent attacks. In *2017 13th International Computer Engineering Conference (ICENCO)*, pages 323–330. IEEE, 2017. `doi:10.1109/ICENCO.2017.8289808`.

3 Mohamed A Abo-Soliman and Marianne A Azer. Enterprise wlan security flaws: Current attacks and relative mitigations. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–8, 2018. `doi:10.1145/3230833.3230836`.

4 Claudio Ardagna, Stephen Corbiaux, Koen Van Impe, and Radim Ostadal. ENISA THREAT LANDSCAPE 2023, 2023. `doi:10.2824/782573`.

5 Alberto Bartoli, Eric Medvet, Andrea De Lorenzo, and Fabiano Tarlao. (in) secure configuration practices of wpa2 enterprise supplicants. In *Proceedings of the 13th International Conference*

on Availability, Reliability and Security, pages 1–6, 2018. arXiv:1806.03215, doi:10.48550/arXiv.1806.03215.

6 Alberto Bartoli, Eric Medvet, Andrea De Lorenzo, and Fabiano Tarlao. Enterprise wi-fi: We need devices that are secure by default. *Communications of the ACM*, 62(5):33–35, 2019. doi:10.1145/3319912.

7 Alberto Bartoli, Eric Medvet, and Filippo Onesti. Evil twins and wpa2 enterprise: A coming security disaster? *computers & security*, 74:1–11, 2018. doi:10.1016/J.COSE.2017.12.011.

8 Luís Miguel Batista, Hélder Gomes, and João Rafael Almeida. Challenges and Solutions for Eduroam Network Security. *Procedia Computer Science*, 2024.

9 Sebastian Brenza, Andre Pawlowski, and Christina Pöpper. A practical investigation of identity theft vulnerabilities in eduroam. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 1–11, 2015. doi:10.1145/2766498.2766512.

10 Xuewei Feng, Qi Li, Kun Sun, Yuxiang Yang, and Ke Xu. Man-in-the-middle attacks without rogue ap: when wpas meet icmp redirects. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 3162–3177. IEEE, 2023. doi:10.1109/SP46215.2023.10179441.

11 Matheus E Garbelini, Chundong Wang, and Sudipta Chattopadhyay. Greyhound: Directed greybox wi-fi fuzzing. *IEEE Transactions on Dependable and Secure Computing*, 19(2):817–834, 2020. doi:10.1109/TDSC.2020.3014624.

12 Seema B Hegde, Aditya Ranjan, Aman Raj, Krishanu Paul, and Smritimay Santra. Wpa2 based wireless enterprise configuration. In *2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, pages 1–8. IEEE, 2021. doi:10.1109/ICMNWC52512.2021.9688387.

13 Christopher P Kohlios and Thaier Hayajneh. A comprehensive attack flow model and security analysis for wi-fi and wpa3. *Electronics*, 7(11):284, 2018. doi:10.3390/electronics7110284.

14 Karim Lounis and Mohammad Zulkernine. Bad-token: denial of service attacks on wpa3. In *Proceedings of the 12th International Conference on Security of Information and Networks*, pages 1–8, 2019. doi:10.1145/3357613.3357629.

15 Ivan Palamà, Alessandro Amici, Gabriele Bellicini, Francesco Gringoli, Fabio Pedretti, and Giuseppe Bianchi. Attacks and vulnerabilities of wi-fi enterprise networks: User security awareness assessment through credential stealing attack experiments. *Computer Communications*, 212:129–140, 2023. doi:10.1016/j.comcom.2023.09.031.

16 T Perković, A Dagelić, M Bugarić, and M Čagalj. On wpa2-enterprise privacy in high education and science. *Security and Communication Networks*, 2020:1–11, 2020. doi:10.1155/2020/3731529.

17 Domien Schepers and Aanjhan Ranganathan. Privacy-preserving positioning in Wi-Fi fine timing measurement. *Proceedings on Privacy Enhancing Technologies*, 2022. doi:10.2478/popets-2022-0032.

18 Rajeev Singh and Teek Parval Sharma. On the ieee 802.11 i security: a denial-of-service perspective. *Security and Communication Networks*, 8(7):1378–1407, 2015. doi:10.1002/sec.1079.

19 Suroto Suroto. Wlan security: threats and countermeasures. *JOIV: International Journal on Informatics Visualization*, 2(4):232–238, 2018. doi:10.30630/joiv.2.4.133.

20 Erik Tews and Martin Beck. Practical attacks against wep and wpa. In *Proceedings of the second ACM conference on Wireless network security*, pages 79–86, 2009. doi:10.1145/1514274.1514286.

21 Mathy Vanhoef and Frank Piessens. Advanced wi-fi attacks using commodity hardware. In *Proceedings of the 30th Annual Computer Security Applications Conference*, pages 256–265, 2014. doi:10.1145/2664243.2664260.

22 Mathy Vanhoef and Frank Piessens. Key reinstallation attacks: Forcing nonce reuse in wpa2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1313–1328, 2017. doi:10.1145/3133956.3134027.

23 Mathy Vanhoef and Eyal Ronen. Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 517–533. IEEE, 2020. doi:10.1109/SP40000.2020.00031.

24 Kailong Wang, Yuwei Zheng, Qing Zhang, Guangdong Bai, Mingchuang Qin, Donghui Zhang, and Jin Song Dong. Assessing certificate validation user interfaces of wpa supplicants. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, pages 501–513, 2022. doi:10.1145/3495243.3517026.

25 Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9):1727–1765, 2016. doi:10.1109/JPROC.2016.2558521.