"Careful with that Roam, Edu": experimental analysis of Eduroam credential stealing attacks

1st Ivan Palamà
CNIT/University of Rome - Tor Vergata
ivan.palama@uniroma2.it

3rd Francesco Gringoli
CNIT/University of Brescia
francesco.gringoli@unibs.it

2nd Alessandro Amici
University of Rome - Tor Vergata
a.amici@outlook.it

4th Giuseppe Bianchi
CNIT/University of Rome - Tor Vergata
giuseppe.bianchi@uniroma2.it

***Abstract*—Eduroam, which stands for education roaming, is a world-wide Wi-Fi access and roaming service largely exploited by the international research and education community. Eduroam's authentication relies on the same long-term credentials used by students and professors to access critical education/research services. To assess the real-world security of Eduroam, we i) implemented a credential stealing attack based on a rogue Eduroam setup, ii) ran a controlled experiment with 37 relatively skilled real world users (mainly electrical or computer engineering students), and iii) for four heterogeneous selected devices, we investigated their more detailed dependence on different WPA-enterprise configurations and certificate settings. The aftermath is that, even with a completely passive attack (users were keeping devices in their pocket), we stole credentials from more than one third of the participants. While most of the Eduroam vulnerabilities employed in this work should be considered somewhat known (being disclosed in former technical papers), our work appears to raise a threefold concern: i) most pragmatic Eduroam configurations appear to be grossly insecure; ii) no Apple's iPhone felt in our attack, owing to its reduced possibility for an user to misconfigure the terminal; and iii) there is a limited awareness of Wi-Fi authentication threats even in relatively skilled end users.**

I. Introduction

Eduroam offers a worldwide connection service dedicated to all users in the education and scientific research sector. Eduroam allows organizations to easily provide Internet access to their users in mobile conditions thanks to the flexibility of the IEEE 802.1X authentication protocol family. Students, researchers and professors belonging to organizations that are part of Eduroam can use their own credentials when connecting to the network of a visited institution: the visited authentication server is configured, in fact, to securely forward the provided username and password to the home authentication server for local verification. By analyzing the security aspects of such a scenario, it is possible to identify 3 important entities: the Eduroam network, the institutions, and the user's terminal. The security infrastructure of the Eduroam network relies on the use, verification, and proper configuration of the Eduroam root CA certificate within each of the user's devices. Eduroam institutions provide login credentials and should instruct users to properly configure the network on their devices. Unfortunately, these guides are often outdated or incorrect, e.g., instructions provided by our university suggest to leave the certificate field at its default value, thus introducing serious vulnerabilities in the configuration of the network access. In addition, the majority of the tested devices not only do not advertise the users about the risks, they are also pre-configured with vulnerable profiles. For these reasons users can unconsciously expose their credentials to attackers that set up rogue access-points, also called Evil Twins, or use some man-in-the-middle mechanism. An attacker can, in fact, easily trick a user by recreating a malicious 802.1X network that advertises the Eduroam SSID in order to steal users' access credentials. In some countries the same credentials are also used to authenticate university professors to services like electronic marksheets: attacking students might in principle modify the marks in the system before they are digitally signed. The reported vulnerability becomes hence a serious problem of identity privacy worldwide, since the attacker has the potential to identify himself as a university professor and use all the services related to him (e.g. GèANT eduGAIN). In addition, these credentials are often the same as those of the professors' university-personal email accounts, which would allow a malicious attacker to access all services connected to them, thus increasing the severity of the vulnerability. In addition to the demonstration of the attack aimed at capturing the user's credentials, a further contribution of this paper is its assessment in the wild, over a non marginal set of real-world end users (due to COVID-19 restrictions we had to limit to a few tens of users, specifically 37). Quite interestingly, even if our reference group of end users was relatively skilled, being mainly composed of students in computer and electronic engineering with some cybersecurity background, our results show a remarkable lack of awareness about the risks and the vulnerabilities that affect the Eduroam system. Finally, we find perhaps surprising that, in front of a non marginal literature which has documented Eduroam's vulnerabilities in the course of many past years [1], [2], [3], [4], [5], [6], [7], our attack was still successful in more than one third of the cases (17 users over 37), pointing out the substantial difference between literary theory awareness and practical awareness in the real world. Mainly driven by the curiosity

to understand whether certain brands of mobile phones had a certain "resilience" to such attacks, another contribution of this paper is an experimental analysis designed to understand how different devices react to different forms of rogue AP attacks. We ran our test using three different network certificate (self-signed, expired and valid), four network authentication protocols and four different certificate control strategies. The rest of the article is organized as follows: after some necessary background in section II, we describe the experimental attack and results in section III and IV. The in-depth experimental analysis of the device behaviour on different WPA-enterprise configurations is described in section V. Finally, Section VI draws conclusions and outlines further directions for research.

II. Background

We provide in this Section a quick overview of authentication in Eduroam: we focus on the necessary aspects for understanding the vulnerabilities that make the attack possible. We refer interested readers to the standards [8], [9], [10], [11], [12] for further details.

A. Eduroam authentication

In Eduroam, the authentication is based on the IEEE 802.1X standard for port-based network authentication, which ensures that only authorized users get access. 802.1X includes the usage of EAP (Extensible Authentication Protocol), which allows different authentication methods. Depending on the configured EAP method, i.e., EAP-TTLS, PEAP or EAP-TLS, a secure tunnel from the user's terminal to his/her own institution authentication server is established: this tunnel is used for mutually authenticating users to their own networks, by exchanging public X.509 certificates and users' credentials. IEEE 802.1X authentication involves three main actors: a supplicant, an authenticator and an authentication server. In Eduroam these entities are represented by the user client terminal, the Access Point (AP) belonging to the Service Provider (SP), i.e., the visited institution, and the Authentication Server (AS) belonging to the Identity Provider (IdP) of the user's home institution. To ensure that users can connect internationally using the credentials provided by their home institutions, Eduroam has a linked hierarchy of RADIUS AS containing users' data (usernames and passwords) that securely forwards user credentials to the users' home institutions, where they are verified and validated. Eduroam security is based on three trust relationships:

1) The direct trust relationship between end user and IdP, managed by the user's home organisation, established through mutual authentication;
2) The direct trust relationship between IdP and SP, namely the network operator at the visited location, established through the use of the proxy hierarchy of RADIUS servers (organizational, national, global);
3) The transitive trust relation that makes the SP trust the user in order to use its network resources.

The authentication procedure involves two authentication steps:

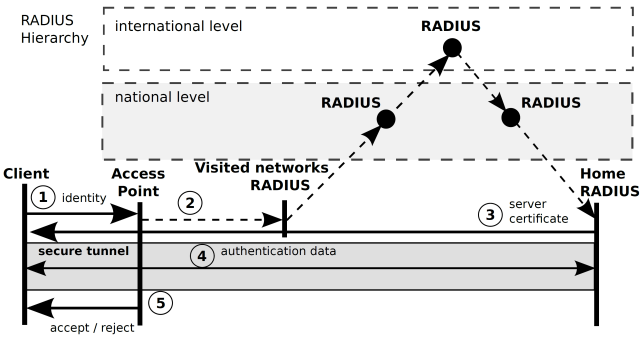

Fig. 1. Eduroam Authentication Process, figure taken from [1].

1) An external layer authentication (EAP-TTLS or PEAP) is performed to establish a secure communication tunnel between the user client device and the home AS;
2) Inside the established tunnel the supplicant runs an internal authentication algorithm (PAP or MS-CHAPv2), using the credentials provided by his home institution to verify his identity.

In the following of this section we will refer to Figure 1 that illustrates the authentication procedure executed when a user connects under roaming conditions.

External authentication: i) To access the network, the supplicant provides to the SP AP the user's identity "username@institution.tld" where institution.tld is the user realm and username is optional. ii) The SP AP forwards the identity to the local (visited) AS, which checks if it is responsible for that realm. Since it is not, it transfers the identity to the next RADIUS AS at the national or international level according to the realm part of the user's identity, until the user's home IdP AS is found. iii) After verifying the received identity, the user's home IdP AS sends back to the supplicant its certificate. iv) If the supplicant validates the certificate, the secure tunnel is established. The certificate of the IdP AS plays a crucial role in the authentication phase: failure or false verification of the certificate would cause the user serious security problems.

Internal authentication: iv) The supplicant can now use the secure tunnel to authenticate the user to the user's AS: if this phase succeed, then v) the user's AS can transmit the result to the AP, which will then authorize or deny network access when credentials are wrong.

Authentication vulnerabilities: As mentioned above, the purpose of the external authentication phase is to set up a secure and authenticated tunnel between the supplicant and the remote AS. By reviewing the authentication phase, it can be pointed out that: i) if the user's anonymous identity is not used in the external authentication phase (i.e., username@realm is sent), the user's anonymity is not maintained, and the attacker can link the user's identity with the hardware identity (such as MAC address), thus he can violate the user's privacy (identity and location); ii) Even if the protocols used in the internal authentication phase are secure, they vulnerably rely on the fact that a secure tunnel for the exchange of authentication data has been established in advance, then if the user's client does not

validate the certificate provided by the authentication server, the attacker can learn the user's credentials and compromise the user's privacy.

III. Experiment

We describe here how we set up and carried out the experiment. In order to assess the current level of security awareness in a medium-sized university, an experiment was set up with 35 students in computer and electronic engineering and 2 ICT professors, all of the study participants were from the same institution/used an Eduroam configuration from the local institution. The experiment involves the setup of an evil twin attack scenario, and the submission of two anonymous pre- and post-attack questionnaires with multiple-choice and open-ended questions to the same group of 37 users. The goal of the questionnaires is to test and understand the degree of awareness of a relatively skilled set of end users before and after being victims of such attack.

Pre-attack questionnaire: The anonymous pre-attack questionnaire consists of 16 multiple-choice and open-ended questions aimed to analyze the network and security skills and threat awareness of a relatively significant sample before they have been under attack.

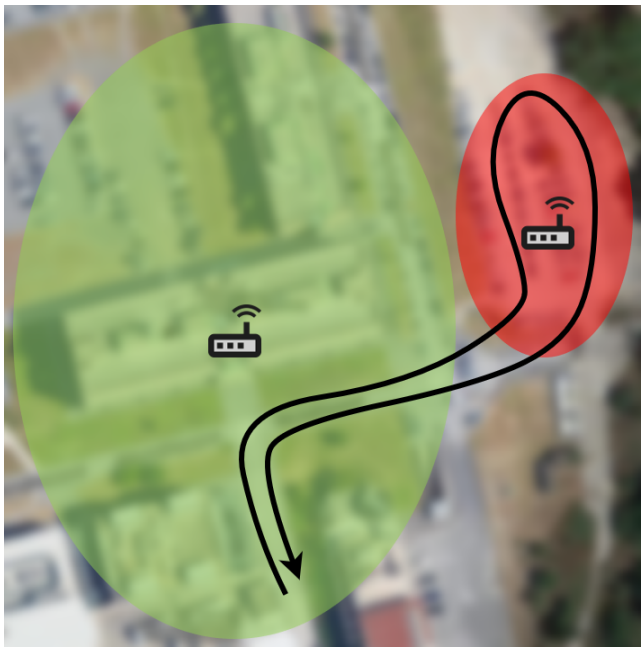

Fig. 2. Experiment area. Green: the area of legitimate Eduroam network. Red: the area of the rogue AP. Black arrow: the walking path.

Attack: The attack assumes that users have successfully connected to Eduroam previously. We did not ask users to make any changes to their configurations, assuming that they have configured the network automatically through the official Eduroam Configuration Assistant (Eduroam CAT) tool or manually by configuring their credentials (identity and password), authentication protocol and certificate verification fields. After completing the first questionnaire, the experiment takes place in which the users were simply asked to participate in a security test and follow the path shown in the Figure 2, without making them aware that they would be attacked. Malicious AP convinces the users' devices to connect to it, exploiting the fact that they will try to connect to the Wi-Fi AP with stronger signal. Since the user has previously connected to a legitimate Eduroam network, we expect that when the user is within range of a malicious AP, it will automatically try to connect without any user intervention, in a passive manner. The Eduroam rogue AP is implemented via a laptop, in which we have properly configured the Hostapd and Freeradius software suites. In addition, an Internet connection is provided to minimize the visibility of attacks.

Post-attack questionnaire: After being attacked, samples of students and professors are asked to answer a second anonymous questionnaire with 14 multiple-choice and open-ended questions. The goal here is to understand whether they have realized that they were under attack, how they realized that, and how much the awareness of wireless network security threats has increased after realizing they have been attacked. An anonymous id was used to link responses from the two questionnaires.

IV. Results

In the following section we analyze the behaviour of the tested devices and try to understand the dependency of the operating system and of the user unawareness.

A. Impact of devices

We report in table I the 33 unique mobile devices we tested of the 37 users: some participants had the same phone. After analyzing the behaviour of the smartphones during the experiment we concluded the following.

Dependence on the OS: Of the 37 participants, 33 used a different smartphone brand/Operating System configuration, with 9 Apple iPhones running iOS, and the remaining running Android. It appears that all Apple iPhones are not vulnerable: they do not connect to the rogue Eduroam AP and do not provide user credentials. Unlike Android smartphones, Apple smartphones do not allow the user to configure the certificate control policy. When they connect to the Wi-Fi network they show the received certificate and ask the user to accept it or not. This behavior leads to the fact that during the connection with the malicious Eduroam AP, the device shows to the users the forged Eduroam certificate. This behavior allows users to understand what is going on, thereby making them aware of the attack and, in our case, impeding the completion of the attack as the user intervention was necessary - indeed we did not ask participants to interact with their smartphone so as to perform a purely passive attack. By analyzing the experimental results, it can be found that Android smartphones are vulnerable (even with the latest Android OS 11). This is because unlike iOS, Android OS allows users to configure the network in a very detailed way, specifying authentication protocols and certificate control rules. When investigating the certificate control policy configuration in Android smartphones, we

Brand	Model	OS
Apple	iPhone 11 Pro	iOS 14.5
	iPhone 11 Pro, 11, XS, 8, 7	iOS 14.4
	iPhone 8	iOS 13.3
	iPhone 8	iOS 13
Samsung	S20, S10, S10e, S9, Note 9	Android 10
	S8, A70	Android 9
	S7	Android 8
Xiaomi	Mi 10, Mi 9T Pro	Android 11
	Mi 10, Mi10T, Mi10 Lite, Mi 9, Mi 9T Pro, Poco X3, Redmi Note 8, Redmi Note 7	Android 10
OnePlus	8	Android 11
	6, 5T	Android 10
Huawei	P20 Pro	Android 10
	P10	Android 9
Honor	9	Android 9
Motorola	G8 Power	Android 10

TABLE I
USER DEVICE/OS TESTED DURING THE EXPERIMENT.

found that in several smartphones users may not choose any policy, and the default policy is to accept unverified network certificates, which makes smartphones really vulnerable to the attacks.

Dependence on the Android version: Since all vulnerable smartphones come with Android OS, we ran some additional experiments in a controlled lab in order to identify the reasons behind their vulnerable behavior. We analysed the different Wi-Fi configuration dialogs exhibited by Android OS from version 5.1 to 11. We found two substantial changes in Android Nougat 7.0 [13], [14] that respectively introduce: i) The display of a warning of potential risks if users do not provide a CA certificate in the EAP configuration. ii) The addition in the EAP configuration menu of the option to not specify an EAP CA certificate and a user certificate. Their main effect is to require users to make conscious choices about certificate control policy. This leads us to conclude that the vulnerability only exists in devices with an Android version below 7.0. While this is true in the majority of the tested devices, some others, which even come with more recent Android OS versions, do not display any warning and apply the default vulnerable policy, i.e., they do not check the validity of the received certificates. An example of such behaviour is the Xiaomi Mi 10 with Android 10/11. This suggests that the customisation of the Android OS performed by the manufacturer may also play a key role in the vulnerable behaviour of devices.

B. User (un)awareness

We report in Tables II and III respectively the questions in the questionnaires and the most significant results, indicating the percentage of non-numeric responses and the weighted average (W/A) of numeric responses, in this case not available (N/A) is indicated in the percentage field. We emphasize that what we report here are qualitative and quantitative indicators whose objectives are: i) to show whether a particular device and its OS makes the user aware of a vulnerable configuration of the Wi-Fi network; ii) to analyze the end users by showing their characteristics in the field of network security, highlighting the critical points; and iii) to analyze the result of the instructions provided by the organizations to the users of the Eduroam network configuration. Through the analysis of the experimental results, many important aspects were discovered, which describe the current Wi-Fi network security knowledge and vulnerability awareness.

Certificate-Based Authentication: As shown in Table II, the vast majority (66%) of the participants is not aware of the fact that the Eduroam network uses certificates in the authentication process. This is surprising as the set of users comprises mainly students in ICT disciplines, and suggests that students do not behave as ICT engineers during daily activities. Combining this with the fact that 77% of the sample of students manually configure the network, it is very likely that users have vulnerable configurations that do not check the validity of the certificate.

Authentication protocols: Table II also shows that students do not have a clear idea about the authentication protocols supported by the network: this exposes them to numerous vulnerabilities that could even lead them to reveal their IMSIs - International Mobile Subscriber Identity [2]. From the experiments, in fact, it turns out that users are not familiar with the Eduroam authentication protocols. During device configuration there are hence chances that they select EAP-SIM/AKA as EAP method [15], [16] and eventually reveal their IMSI to the attacker (and also to the legitimate Eduroam system). As the IMSI is a world-wide permanent identifier, an attacker can exploit its knowledge to carry out a series of attacks designed to locate and track a specific user.

C. Organization vulnerabilities

Organisations participating in the Eduroam project must provide access credentials to users. They must also provide a guide to manually configure access to the Eduroam network or provide a tool to do so automatically. Unfortunately, organisations - including the university where we executed all the experiments - often provide outdated and insecure guides to users, which expose them to various vulnerabilities. Since 77% of the users configure the network manually and given that our questionnaires reveal a limited (on average) understanding of Wi-Fi/802.1X security configurations, organisations play a key role in the security of Eduroam. Often the Eduroam

Question	Answers	Percentage %
Does Eduroam use certificates in the authentication process?	Yes	34
	No	26
	I don't know	40
How did you configure Eduroam?	Manually	77
	Automatically with Eduroam CAT tool	17
	I don't use Eduroam	6
Have you ever connected to Eduroam under mobility/roaming conditions?	Yes	31
	No	60
	I tried without success	3
	I don't use Eduroam	6
How much attention will you pay to configure Wi-Fi network from 1 to 10?	Weighted average: 5.24	N/A
Does the device when it detects Eduroam, automatically connect to it?	Yes	83
	No	11
	I don't use Eduroam	6
How much would you rate your knowledge of Wi-Fi security from 0 to 10?	Weighted average: 4.74	N/A
Regarding the configuration of the certificate, choose the answer that you think more suitable	I leave the certificate field as default	31
	I have manually/automatically configured the certificate	34
	I configured "do not validate certificate"	11
	Eduroam not use certificates	17
What security protocols does Eduroam support? (select all the answers you think are valid)	Generic Username/Password protocol	23
	EAP-TTLS/PAP	37
	EAP-TTLS/MSCHAPv2	11
	WPA2-Personal	23
	PEAP/MSCHAPv2	0
	I don't know	34

TABLE II
KEY QUESTIONS FROM THE PRE-ATTACK QUESTIONNAIRE.

credentials provided to professors by their employers are the same used in national authentication and authorization services based on institutional digital identity: they can be also used for accessing several federated services including GÈANT eduGAIN, the inter-federation framework of Authorisation, Authentication and Identity (AAI) services that provide users across the research and education community with single-sign-on to thousands of service providers worldwide. The exposure of professors' Eduroam credentials therefore represents a huge issue related to the privacy and security of their digital identity.

V. USER DEVICE BEHAVIOR ANALYSIS

We present in this section an in-depth behavioral preliminary analysis on four smartphones from different brands: Apple, Samsung, Xiaomi, and ZTE. We evaluate the feasibility of the attack over different versions of the OS, of the devices' network configuration, and of the type of certificate used in the malicious network (self-signed, expired and valid). In addition to describing the differences in behavior and highlighting the vulnerabilities, we also propose solutions to the discovered security problems.

A. Attack feasibility

We start by evaluating the influence of the chosen authentication protocol and the type of certificate used.

Authentication protocol: By analyzing the results shown in Table IV, it is possible to show that only one smartphone has an implementation of Android OS that allows an extremely high attack feasibility, because any configuration that allows access to the legitimate Eduroam network is vulnerable and

Question	Ans	%
You have connected to an Eduroam rogue AP, how serious do you consider this situation to be from 0 to 10?	7.09	N/A
Were there any abnormal behaviours or warnings that made you feel you were under attack? Did you realise you were under attack?	Yes	24
	No	76
How serious do you consider the leakage of credentials to be from 0 to 10?	8.85	N/A
Do you have any idea what vulnerability enabled the attack?	Yes	24
	No	76
Did you expect an Eduroam configuration that allows you to access the Internet to be insecure and allow credential leaks?	Yes	55
	No	45
After this experiment, how much attention will you pay to configure Wi-Fi network from 1 to 10?	6.94	N/A
What do you think is your level of awareness of Wi-Fi security from 0 to 10?	4.22	N/A
Do you think there is a need to raise awareness about Wi-Fi security?	Yes	97
	No	3

TABLE III
KEY QUESTIONS FROM THE POST-ATTACK QUESTIONNAIRE.

Device and OS	TTLS-PAP			TTLS/PEAP-MSCHAPv2		
	Self signed	Exp.	Valid	Self signed	Exp.	Valid
Apple iPhone XS iOS 14.4	A	A	A	N/A	N/A	N/A
Xiaomi Mi 10 Android 11	C	C	D	A	A	A
ZTE Axon 10 Pro Android 9	B	B	B	A	A	A
Samsung S8 Android 8	B	B	B	A	A	A

TABLE IV
ATTACK FEASIBILITY FOR DIFFERENT DEVICES UNDER DIFFERENT CONDITIONS: A : GOOD, B : NOT SO GOOD, C : NOT SO BAD, D : BAD.

allows attackers to obtain access credentials of the victim under almost all tested conditions. Evaluating table IV from the point of view of the feasibility of the attack, the letters shown have the following meanings:

- **A)** Indicates that the device does not connect to the rogue AP with any certificate verification policy configuration, consequently the feasibility of the attack is null.
- **B)** Means that the device connects to the rogue AP only with the "Do not validate" as certificate control policy.
- **C)** Indicates that the device connects to the malicious AP with both the "Do not validate" and "Please select" policies, while using the "Use system certificate" policy the phone does not connect to the rogue AP.
- **D)** Emphasises a vulnerable behaviour that makes the attack feasible also with the "Use system certificate" control policy.

In addition to the protocol shown in Table IV, the configuration using Eduroam CAT is also analyzed under which in all possible cases, the behavior belongs to the letter **A)**.

Certificate: Experiments show that the type of certificate used in the malicious network only affects one smartphone. Unlike other tested smartphones, if the rogue AP uses a valid certificate, it provides user credentials even if the user explicitly selects the "use system certificate" policy. This leads us to believe that there may be vulnerabilities in the Wi-Fi network configuration and connection software. In all cases where the user connects to the malicious network, the device provides plain text credentials to the attacker without user's awareness. The tested Eduroam Wi-Fi network uses the Wi-Fi Alliance WPA2 standard while the new WPA3 [17] standard is available. WPA3 Enterprise has improved security compared to WPA2. This is largely due to the inability to use "skip certificate verification" or "accept any certificate" to configure the supplicant, and if the supplicant cannot verify the server identity, then it will no longer be possible to automatically send user credential materials to AS; it requires that the user explicitly accepts the trust in the certificate provided by AS. This relatively straightforward constraint on allowed configuration and user participation reduces the chance of tricking a supplicant into leaking credentials. It is important to point out that the WPA3-Enterprise specification does not impose any timing or causality between a failed server identity verification and the user's decision, which may still be vulnerable.

B. Device misconfiguration protection

By evaluating the results shown in Table IV from the perspective of Wi-Fi network misconfiguration protection:

- **(A)** and **(B)** can be considered reasonable: in the case **(B)** the user can, in fact, misconfigure the phone but only via a deliberate action.
- **(C)** and **(D)** can be considered dangerous: we consider dangerous not only **(D)** (for obvious reasons), but also **(C)**, since in this case the default configuration is vulnerable, whereas the vulnerability is fixed only by an

explicit intervention of the end user which must set the "Use system certificate" policy.

Moreover, results show that, despite the security improvements introduced in Android 7.0 described in detail in section IV-A, one among the four in-depth tested smartphones did not implement these enhancements. For the sake of clarity, however, after the latest update released by the manufacturer at the beginning of 2022, the device no longer appears to be vulnerable. Finally, as mentioned earlier, Apple's policy of reducing as much as possible the configuration capabilities provided to end users appears to pay off in terms of security, as it was not possible for any user to misconfigure the device and expose it to the attacks tested in this paper. Furthermore, Apple smartphones always show the certificate to the user when connecting to the network and whenever a new one is provided, therefore raising the user level of awareness.

VI. Conclusion

The main contribution of this paper is an experimental investigation of the *practical* security of Eduroam, a network used by millions of users in the research and education sector in more than 100 countries worldwide. To this end, we implemented and ran a controlled evil twin passive attack in the university's premises, conducted over 37 relatively ICT-skilled volunteers and 33 different combinations of smartphone brand/Operating System from seven vendors, and aimed at assessing vulnerabilities in the users' configurations in order to steal their credentials. Moreover, an in-depth preliminary analysis was conducted on four specific smartphones, to better understand their behavior while varying the authentication protocols and the nature of the certificates employed (self-signed vs. expired vs. valid). Finally, the technical work was complemented by the proposal of two anonymous questionnaires (one before the attack, and one after it) to the volunteers, so as to gather insights on their security awareness. A technical lesson learned from our work is that Android, compared to iOS, offers a greater freedom of configuration to the user and therefore is more exposed to possible attacks - like the one implemented by us - that aim at exploiting wrong or incomplete configurations. Moreover, our results appear to show that the practical sanity of Eduroam is quite low. Indeed, with somewhat consolidated attack techniques, still today an attacker can steal long term credentials to a non marginal fraction of users (more than one-third in our tests). Note that the attack yields the malicious gathering of persistent credentials used for a multiplicity of critical single-sign-on educational services (e.g., access to university email, access/recording of exam grades, etc). This appears a very serious vulnerability considering the highly interconnected global environment in which the Eduroam network is embedded. The final takeaway is that we would have expected a greater security awareness in the set of volunteers involved in the experiments - university students in ICT-related programs - as well as in the organizations that are called to properly configure the network access. Despite the fact that Eduroam vulnerabilities have been documented in the literature, we found a substantial discrepancy with the practical security awareness level of either users as well as organizations - even if we conducted tests in our own institution, we are aware of many other institutions which suggest to their students and employees vulnerable configurations.

Possible countermeasures could be: - Android side, set as default behavior to request and check the certificate provided by the network, but also showing the user an alert if abnormal network behavior is detected (e.g., an AP without a certificate or with a different certificate); It would also be useful to add a link to a network configuration guide to educate the user on possible misconfigurations and their impacts - User side, to have a greater understanding of the authentication protocols and to pay more attention during the network configuration; - Organization side, keep updated the guides related to the network configuration and hold seminars to raise users' awareness of these issues. In future work, we plan to analyze and develop technologies that end users and organizations can use to detect possible attackers.

References

[1] S. Brenza, A. Pawlowski, and C. Pöpper. A practical investigation of identity theft vulnerabilities in eduroam. In *Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'15)*, 2015.

[2] T. Perković, A. Dagelić, M. Bugarić, and M. Cagalj. On wpa2-enterprise privacy in high education and science. *Security and Communication Networks*, 2020, Sept. 2020.

[3] B. Altinok. eduroam: Collect, track, hack. https://medium.com/@besimaltnok/eduroam-collect-track-hack-183e843f7efc, Last accessed on 2021/5/26.

[4] A. Bartoli, E. Medvet, and F. Onesti. Evil twins and wpa2 enterprise: A coming security disaster? *Computers and Security*, 74:1–11, 2018.

[5] A. Bartoli, E. Medvet, A. De Lorenzo, and F. Tarlao. (in) secure configuration practices of wpa2 enterprise supplicants. In *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES)*, 2018.

[6] V. Ramachandran. Cracking wpa/wpa2 personal and enterprise for fun and profit. In *Hacktivity Conference*, 2012.

[7] M. Ghering. Evil twin vulnerabilities in wi-fi networks. Bachelor's thesis, 2016.

[8] K. Wierenga, S. Winter, and T. Wolniewicz. The eduroam architecture for network roaming. RFC 7593, 2015.

[9] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible authentication protocol (eap). RFC 3748, 2004.

[10] D. Simon, B. Aboba, and R. Hurst. The eap-tls authentication protocol. RFC 5216, 2008.

[11] P. Funk and S. Blake-Wilson. Extensible authentication protocol tunneled transport layer security authenticated protocol version 0 (eap-ttlsv0). RFC 5281, 2008.

[12] Microsoft. MS-PEAP: Protected extensible authentication protocol (peap), 2018. https://msdn.microsoft.com/en-us/library/cc238354.aspx, Last accessed on 2021/5/26.

[13] S. Tan. Display warning if users does not provide ca cert in eap config, 2016. https://android.googlesource.com/platform/packages/apps/Settings/+/03a117b, Last accessed on 2021/5/26.

[14] S. Tan. Add menu options for not specifying a eap ca cert and user cert, 2016. https://android.googlesource.com/platform/packages/apps/Settings/+/f827c92, Last accessed on 2021/5/26.

[15] H. Haverinen and J. Salowey. Extensible authentication protocol method for global system for mobile communications (gsm) subscriber identity modules (eap-sim). RFC 4186, 2006.

[16] J. Arkko and H. Haverinen. Extensible authentication protocol method for 3rd generation authentication and key agreement (eap-aka). RFC 4187, 2006.

[17] Wi-Fi Alliance. Wpa3 specification 3.0. https://www.wi-fi.org/file/wpa3-specification, Last accessed on 2021/5/26.