Hindawi
Security and Communication Networks
Volume 2020, Article ID 3731529, 11 pages
https://doi.org/10.1155/2020/3731529

Research Article

On WPA2-Enterprise Privacy in High Education and Science

T. Perković, A. Dagelić, M. Bugarić, and M. Čagalj

Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, University of Split, Split, Croatia

Correspondence should be addressed to T. Perković; toperkov@unist.hr

Received 29 January 2020; Revised 24 July 2020; Accepted 24 August 2020; Published 7 September 2020

Academic Editor: Savio Sciancalepore

A plethora of organizations, companies, and foremost universities and educational institutions are using WPA2-Enterprise protocol to allow their end-users to connect to provided Wi-Fi networks. When both the provider's and the end-user's devices are configured properly, it is considered one of the safest Wi-Fi connection protocols with the added benefits of having a unique password for every Wi-Fi user. However, a known evil twin attack can be performed to steal users' Wi-Fi login credentials, if the devices are not configured correctly. Considering the widespread use of Wi-Fi-enabled smartphones and rising concerns regarding users' privacy, we focus on the privacy aspects of WPA2-Enterprise vulnerabilities mainly on the widespread Eduroam network. We show that device deanonymization is a concerning liability of many Eduroam networks. More than 87% of 1650 devices collected during a two-month test on our university are vulnerable to MAC address deanonymization attack. Furthermore, by analyzing the Eduroam Configuration Assistant Tool of 1066 different institutions around the world, 67% of exported Eduroam profiles having the Wi-Fi device reveal the user's identity in the clear, thus linking the users with the device's MAC address. Indeed, the analysis of the configuration profiles has been confirmed by performing the deanonymization attack on a large-scale international music festival in our country, where 70% of the devices have been vulnerable. Additionally, we showcase the psychological aspects of secure Eduroam users, where some are willing to modify secure configuration profiles to gain aspects to certain blocked features. As a result, the attacker is granted with user credentials and IMSI number and provided with access to all Eduroam-related services.

1. Introduction

Nowadays, a large number of protocols are used to establish an Internet connection via a Wi-Fi network. These protocols range from open Wi-Fi networks-hotspots to WPA or WPA2 protocols with keys shared between the device and the access point (AP). Numerous companies, institutions, universities, and education centers utilize WPA2-Enterprise networks, where wireless devices establish a secure connection to a Wi-Fi network following the IEEE 802.1X standard based on port-isolation functionality. In the era of smartphone devices, user privacy has become increasingly important, and many papers discuss this problem within the context of Wi-Fi-enabled devices [1–4]. With the spread of recent COVID-19, it is especially essential to minimize any privacy and security risks for individuals, protecting their civil liberties [5, 6].

The problem of user privacy is not limited to stealing user's login credentials and can be divided into categories [7]: identity privacy, location privacy, financial privacy, social privacy, and personal privacy. Device deanonymization, in which an adversary recognizes the device and simultaneously links it to the owner, can have some serious privacy implications [1]. In this paper, an attack is presented, where the adversary exploits the vulnerability of the most widely used WPA2-Enterprise network today, *Eduroam*, to compromise the user's personal, location, and identity privacy.

It is well known that WPA2-Enterprise networks, such as Eduroam, suffer from security weaknesses and several recent publications were trying to emphasize the problem of securing these systems [8–11]. However, these papers were primarily focused on security analysis from the aspect of stealing user credentials. The problem of device deanonymization, such as linking the device (MAC address) with its owner, was not covered in detail within current research, to the best of our knowledge.

Eduroam became popular as it provides Internet connectivity to students, researchers, and staff not only within their university campus and research centers but also during their visits to other participating institutions. In the Eduroam Architecture for Network Roaming [12], it is stated that *the system should be designed to preserve user anonymity, which indicates hiding user identity from the third parties*. Unfortunately, this paper shows that the erroneous configuration of supplicant devices for Eduroam network may lead to anonymity violation, even if such configuration allows successful connection to the Internet over legitimate Eduroam access point.

To preserve user anonymity, during WPA2-Enterprise authentication, devices send anonymous identity that holds the realm (institution) belonging to the user's profile (e.g., `anonymous@realm`). Since this message is sent in the clear, a passive adversary that observes all phases of WPA2-Enterprise protocol communication can easily capture this information [13]. As shown in this paper, the erroneous configuration of supplicant devices will leak private identities in the clear (e.g., by sending `username@realm`) in a large percentage of cases. To our surprise, the official Eduroam configuration profiles for a large number of universities indeed force devices to leak private user identities. Having gained such information greatly increases the severity of (identity and location) privacy attacks, as the adversary is no longer tracking the device (mainly the smartphone) but the actual individual. Linking the person with a device (MAC address) can lead to serious privacy threats, such as tracking people and knowing where they are (such as on music festivals or even demonstrations), as well as the direct contacts they were in touch with. Police can use such a technology to track suspects either by using some form of real-time attack to disclose the current location or by using some historical location data to prove somebody's previous whereabouts. Journalists/paparazzi could use such technology to find out celebrities' favorite restaurant/museum or to be notified when they arrive at a particular location. As more and more data are being monitored and stored, such information can be used in different big-data researches like user categorization, marketing purposes, behavior analysis, or location-targeted marketing (based on social network profiles). It can be used to influence political campaigns or decision-making of potential product buyers. All of this can be done without any real knowledge of the user being tracked. It can be simultaneously applied to large groups of people (shopping malls, events, popular tourist destinations, etc.).

This paper also demonstrates an evil twin attack on Eduroam network. Supplicant devices in their Eduroam configuration profiles in many cases do not validate the certificate sent by Authentication server. Certificate validation of the authentication server is not mandatory (e.g., in the Wi-Fi configuration profile on Android devices). This can be exploited by an adversary with an evil twin AP (AP with the same Service Set Identifier (SSID) as the legitimate AP-Eduroam) to steal credentials from users who try to connect to it. This kind of attack is even more severe considering it provides the attacker with the access to various services accessible with Eduroam credentials, which further violates the privacy of users. One of these examples is the e-citizens service in our country, which allows users with Eduroam credentials to download marriage or birth certificates and enables them to change their residential address, check medical appointments and employment status, etc.

In this paper, the following contributions are made:

- Vulnerabilities of Eduroam networks on 1066 university and institution configuration profiles were surveyed, and more than 67% of surveyed institutions are issuing faulty Eduroam configuration profiles vulnerable to passive device deanonymization attack
- A two-month experimental setup was mounted on our university showing that the combination of an active attack and a passive attack can get up to 87% success rate for device deanonymization attack
- The results of three-day experimental setup mounted on a music festival that attracts 150 000 people every year from more than 140 countries confirm that Eduroam privacy is not limited to our university
- An interesting social aspect during the active attack was observed showing that users tend to modify Eduroam configuration profiles to gain access to the Internet, thus potentially revealing additional private information (Eduroam login credentials)
- We surveyed a wide range of services in our country and discovered that they are using Eduroam credentials for authorization, including platforms of e-citizen, which additionally may reflect on disrupting user privacy

The rest of the paper is organized as follows: Section 2 defines prerequisites and the attacker model, along with the experimental setup. The following two sections describe two different attacks (with results and other observations): in Section 3, we present the passive deanonymization attack, while in Section 4, we introduce the evil twin attack. Countermeasures are introduced in Section 5, and conclusions are provided in Section 6.

2. Prerequisites and Attacker Model

In WPA2-Enterprise networks, three parties can be differentiated as shown in Figure 1: supplicant, authenticator, and authentication server, which are employed by a Wireless Device, access point (AP), and authentication server (AS), respectively. During IEEE 802.1X authentication, the communication between a supplicant, AP, and AS is carried out with Extensible Authentication Protocol (EAP) [14]. EAP utilizes a number of authentication protocols, such as EAP-TLS [15], EAP-TTLS [16], and PEAP [17], which provide mutual authentication of the client (supplicant) and server (AS). EAP-TLS, based on mutual authentication via X.509 client and server certificates, is a protocol that is rarely deployed in WPA2-Enterprise networks.

This paper focuses on privacy breaches of mutual authentication protocols based on tunneled authentication, which are utilized by EAP-TTLS and PEAP protocols. As

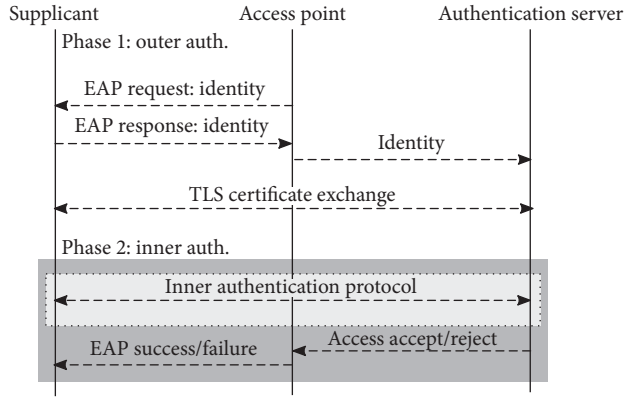

Figure 1: Simplified EAP-TTLS or PEAP authentication protocol.

shown in Figure 1, tunneled authentication is comprised of two phases: in *Phase* 1, denoted as *Outer Authentication*, the supplicant sends its identity as a response to a challenge message received from the AP. The AP forwards a received identity to the AS. Upon successful identity validation, the AS responds with a server certificate. The supplicant (optionally) validates the server certificate and creates a secure tunnel with AS. In *Phase* 2, denoted as *Inner Authentication*, AS validates the supplicant credentials that are transmitted through a tunnel from supplicant to AS. Upon successful validation, AP grants the supplicant the access to a network. EAP-TTLS supports two inner authentication protocols, PAP and MSCHAPv2, while PEAP supports MSCHAPv2 inner authentication protocol. Although both PAP and MSCHAPv2 protocols are insecure, they are used due to the fact that the authentication information is sent within a tunnel previously established between the supplicant and authentication server.

Inaccurate configuration of WPA2-Enterprise networks at the supplicant side can have serious privacy implications:

(a) If in Phase 1 of the protocol an anonymous user identity is not used (i.e., `username@realm` is sent), the adversary will be able to link outer identity with the hardware identity (e.g., MAC address), thus performing device deanonymization and violating user's (identity and location) privacy.

(b) If in Phase 2 of the protocol certificate verification is not used, the adversary will learn the client credentials of WPA2-Enterprise networks which can be further used for compromising user's (identity, location, and personal) privacy.

In this paper, we assume that the victim's device successfully connected to WPA2-Enterprise network in the past, which indicates that users either installed configuration profile on their device or manually configured Wi-Fi profiles for the WPA2-Enterprise network. This requires setting up user credentials, anonymous identity field, and authentication methods and selecting appropriate protocols (EAP-TTLS/PAP, EAP-TTLS/MSCHAPv2, or PEAP/MSCHAPv2). Also, once the device gets within the radio range of the AP, it is assumed that the device will automatically initiate the connection to it.

2.1. Attacker Model. In this paper, the following attacker types are considered:

Passive attacker: the adversary eavesdrops the communication between the supplicant and the target access point. In the passive attack example, the adversary is equipped with hardware and software tools that can intercept the communication between legitimate devices. The assumption is that the attacker can record the WPA2-Enterprise login procedure and learn the MAC address of the victim device and capture user identity, thereby linking the user with MAC address and deanonymizing the victim.

Active attacker: here the adversary mounts an evil twin attack that lures the victims to connect to it. The assumption is that such attack type is automated in the sense that the connection is made automatically when the client device finds itself within the radio range of the fake AP. The assumption is that the victim successfully configured the WPA2-enterprise profile on a supplicant device and established a connection to a legitimate network in the past. The goal of an active attack is to collect user's identity or even full credentials used for WPA2-Enterprise systems, that is, victim username and password, which can be further used to violate user privacy. In another type of active attack, we assume that the victim is not given the access to the Internet although all phases of the EAP authentication protocol were successful. The goal here is to lure victims into modifying their existing configuration profiles that would end up revealing private information in the clear (e.g., IMSI numbers, usernames, passwords, etc.).

2.2. Experimental Setup. Both passive and active attacks were implemented on Raspberry Pi 3 (RPi) running Kali Linux operating system with an external USB adapter wireless card (that supports monitoring mode), as shown in Figure 2. A built-in Kali package *hostapd-wpe* (https://tools.kali.org/wireless-attacks/hostapd-wpe) was used for the execution of the active attack that implements the functionalities of 802.1X authenticator and authentication server. By impersonating a legitimate Eduroam WPA2-Enterprise network, supplicant credentials could easily be captured and logged along with the complete connection procedure, including the used methods and protocols to establish a WPA2-Enterprise connection.

An active attack was carried out in four locations within the grounds of our University during the period of two months (from May to July), precisely at those places where the majority of students, teachers, and personnel were located during the lectures or breaks between lectures: a popular cafe bar, two lecture halls, and the entrance to the campus facility. The Raspberry Pi device was placed in a controlled environment, and only the authors of this paper had access to it.

An additional USB adapter wireless card was employed (Figure 2) to passively capture all link-layer traffic between a supplicant device and WPA2-Enterprise network. By placing a Wi-Fi adapter in monitor mode and using *tshark* network protocol tool, it is possible to capture and analyze network

Figure 2: Implementation setup of our passive and active attacker based on Raspberry Pi device and two external antennas.

traffic at the link layer, including all EAP protocol phases. This is especially interesting for capturing packets in Phase 1 of the EAP protocol, where outer identity may result in device deanonymization.

2.3. Collecting the Data and Preserving Privacy. To ensure the privacy of the collected data and to preserve the anonymity of users, all the collected data on the Raspberry Pi device was encrypted, as suggested in [18]. More precisely, the encrypted data d_i contained username, institution, MAC address of the device, flag with information on whether the username was sent as a part of EAP client response message, the flag of used authentication protocol (TTLS, PAP, and MSCHAPv2), and flag holding the information on whether the authentication was terminated due to the certificate validation. For an encryption algorithm, Advanced Encryption Standard (AES) was selected with Cipher Block Chaining (CBC) block cipher. The key k_i used to encrypt the data was obtained from the hash chain, with the master key K as the head of the chain key. The master key was only known to the authors of this paper and was stored on a local computer for the sake of decryption and computing statistics. Initially, RPi device stored the first key k_i as a result of calculated cryptographic one-way function of master key K (calculated SHA-256 hash function $k_1 = h(K)$). With every new data entry, a new key was generated, while the previous key was erased as follows: $k_i = h(k_{i-1})$, while the collected data d_i was encrypted with freshly generated key $E_{k_i}(d_i)$. In this way, malicious users cannot link the same encrypted data multiple times with different keys without knowing the master key K. Since previous keys have been erased, if RPi falls into the wrong hands (e.g., someone steals it), only the last encrypted data will be recovered.

The collected data was stored on a flash memory card of Raspberry Pi device, collected daily, and kept encrypted on a computer for further analysis. After collecting the data, the flashcards were erased and destroyed.

The University of Split does not have an established policy on user privacy research, but the approval from the Chair of the Ethics Committee was secured. All possible measures, as depicted above, were taken into consideration to make sure that all legal and ethical issues were handled properly.

3. Privacy Leaks of Phase 1 of EAP Authentication

In this section, device deanonymization attack is depicted, whereby the user's privacy can be compromised via passive attack. Recall that, in Phase 1 of EAP authentication protocol, if supplicant devices are not properly configured, user identities are sent in the clear, thereby deanonymizing the user's device. A simple passive attacker placed in front of two legitimate devices (supplicant and Eduroam AP) can easily collect usernames. Linking a username (hence a user, his/her face) with a unique MAC address can violate (identity and location) privacy of the device owner. For the sake of simplicity of our attack, an evil twin Eduroam network was mounted on our university for two months with the aim of collecting outer identity in Phase 1 of EAP authentication protocol, but the same could be achieved via passive attack. Furthermore, the same attack was mounted at the three-day music festival aimed at collecting outer identities. The results are summarized in the remainder of this section.

To establish a connection to the WPA2-Enterprise system, such as Eduroam network, users can either install configuration profiles on their devices from the official Eduroam Configuration Assistant Tool (Eduroam CAT) or manually configure their connection to WPA2-Enterprise network using supplicant's Wi-Fi settings. From the user's perspective, Eduroam CAT is a simple configuration file downloaded and installed on a device from the official Eduroam website. It automatically configures the fields responsible for EAP protocols and built-in authentication methods (e.g., EAP-TTLS, PAP/MSCHAPv2, and/or certificate verification, anonymous identity), simplifying the configuration procedure for an unaided user.

In the Eduroam architecture for network roaming [12], it is stated that the system should be designed to preserve user anonymity, which indicates hiding the user identity from third parties. For this reason, anonymous outer identities are exchanged in Phase 1 (Figure 1) of the protocol, while the exchange of credentials is protected with tunneled authentication before the certificate verification. Anonymity is preserved simply by sending outer identity containing the message `anonymous@realm`, where the realm indicates authentication server based on the company/institution name. Unfortunately, an erroneous configuration of supplicant devices results in device deanonymization, which is accomplished by sending outer identity `username@realm` in the clear containing the username of the device owner.

3.1. Results-Captured Usernames at University Campus. A total number of 631 devices attempted to establish connection to Eduroam Wi-Fi network with certificate validation enabled in supplicant devices. More than 67% of these devices (429) exchanged their `username@realm` in the clear as a part of the EAP client response message (Phase 1), leading to device deanonymization. Table 1 summarizes EAP authentication protocols for devices that leaked usernames in the clear, which implemented certificate verification. Figure 3 shows the distribution of these devices/vendors, with Apple devices being on top. Even though all Apple devices had a certificate verification enabled, it should be noted that all Apple devices revealed the identity of the device owner by sending username in the clear. By default,

Table 1: Summary of EAP authentication protocols configured on devices with enabled certificate verification captured during the two-month period at our university.

	EAP-TLS	EAP-TTLS	PEAP	Total
Our institution	0	247	11	258
Other institutions in univ.	0	126	2	128
Other universities	2	5	0	7
Usern. without institution	0	14	22	36

iOS-based (Apple) devices do not use anonymous identity [19], which also has been confirmed by our analysis. To send the anonymous identity, an explicit `outer identity` field has to be specified in CAT profile for Apple devices, which in the case of our institution was left out.

3.2. Results-Analysis of CAT Profiles. After the latter revelations, further analysis of CAT configuration profiles was conducted for other institutions and universities. Interestingly, a large number of institutions and universities from many countries also provide CAT profiles that leak private usernames as a part of the EAP client response message sent to the authentication server. From the official Eduroam website, CAT profiles were downloaded and analyzed for 1066 institutions from 18 countries. The results are summarized in Table 2. As can be seen, more than 67 *percent!* of institutions do not use anonymous identity (outer identity) field to identify the authentication server but, instead, send username with institution name in the clear during Phase 1 of EAP authentication. Although CAT profiles were analyzed for Apple and Linux-based operating systems, a brief analysis of CAT configuration profiles for all other operating systems indicates that in most cases outer identity or anonymous identity fields are not implemented.

3.3. Results-Captured Usernames at Music Festival. In 2019, an evil twin attack on Eduroam network was mounted during a three-day music festival that attracts nearly 150,000 people from more than 140 countries. In total, 1369 supplicant devices attempted connection to our Eduroam network by sending outer identity. From the analysis of realm (institution) captured in Phase 1 of the protocol, the majority of attendees arrived from Spain, the United Kingdom, Norway, Australia, Germany, Sweden, Austria, USA, Canada, Netherlands, and Croatia (https://www.total-croatia-news.com/lifestyle/37563-ultra-europe) (as summarized in Table 3). More interestingly, 967 supplicant devices out of 1369 (70 percent) sent usernames in the clear, resulting in device deanonymization. This result only confirms how insecure CAT configuration profiles for a large number of universities contribute to device deanonymization in practice.

3.4. Implications and Other Observations. As shown in Section 3.1, an insecure configuration of devices can easily lead to collecting Eduroam usernames. What is even more important, official configurations issued by institution

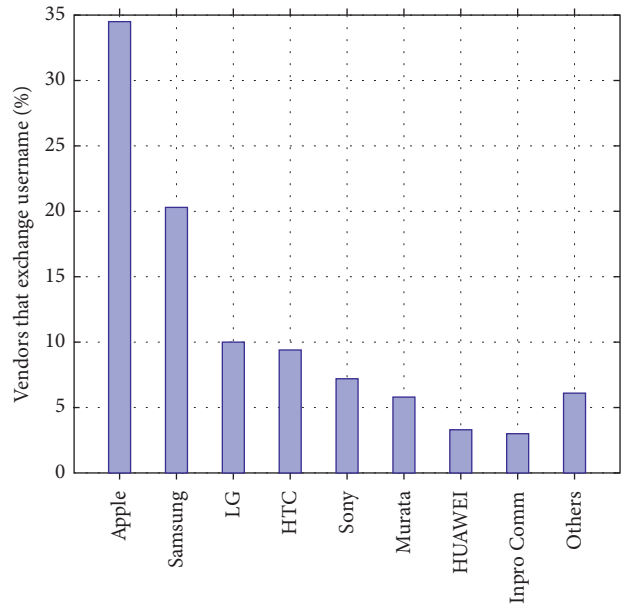

Figure 3: Distribution of vendors equipped with Eduroam configuration profile and certificate verification of authentication server which attempted to establish a connection to our fake WPA2-Enterprise network.

representatives send usernames in the clear over the air during the authentication phase.

Linking username with unique device identifiers such as MAC address may lead to serious (identity and location) privacy concerns. The problem of leaking usernames as a part of the EAP authentication protocol (Phase 1 in Figure 1) was denoted in Defcon 21 conference [13], but their talk was focused on stealing complete user credentials rather than usernames only. Although capturing usernames will not provide the users with the access to enterprise systems or emails of a victim, the basic problem of linking username (thus a user) with a unique device identity (MAC address) arises a completely new set of privacy issues that have to be considered very seriously. This allows the attacker to learn more about the user from the unencrypted network traffic collected, while the user is connected, for example, to an open AP or fake AP or within the presence of Man-in-the-Middle (MITM) attack [20, 21].

Extracting usernames may lead to revealing the real name or real face of the person standing behind a device with a unique identification, such as MAC address, which results in device deanonymization. To show how easily this can be accomplished, as a proof of concept, a private web page was created which outputs captured Eduroam username, MAC address of the device, and user Common Name (resulting from a username query to LDAP university server), as well as a public user picture taken from the university website. Figure 4 shows a snapshot of the web page with dummy data.

It is well known that many devices send in the clear a list of access points they connected to in the past (i.e., a Preferred Network List (PNL)). PNLs represent an interesting source of information, as they hold a list of hotspots (e.g., names of restaurants, coffee bars, airports, etc.) as a source of

Table 2: Summary of analyzed Eduroam CAT profiles of 1066 institutions from 18 countries.

	Australia	Austria	Belgium	Czech Republic	Denmark	Finland	France	Netherlands	Hungary
Not using anonymous identity	12	21	13	59	20	27	80	34	12
Using anonymous identity	2	5	1	2	4	17	113	15	9
Overall number of institutions	14	26	14	61	24	44	193	49	21
	Italy	Norway	Poland	Portugal	Slovakia	Spain	Sweden	Switzerland	UK
Not using anonymous identity	71	54	43	40	9	35	21	24	149
Using anonymous identity	11	0	19	3	3	62	5	25	46
Overall number of institutions	82	54	62	43	12	97	26	49	195

Table 3: Summary of top 10 countries with Eduroam identities collected at the music festival.

	Croatia	UK	Spain	Norway	Netherlands	Australia	Germany	Sweden	Slovenia	Switzerland
Number of identities	262	138	91	86	63	49	47	35	30	24

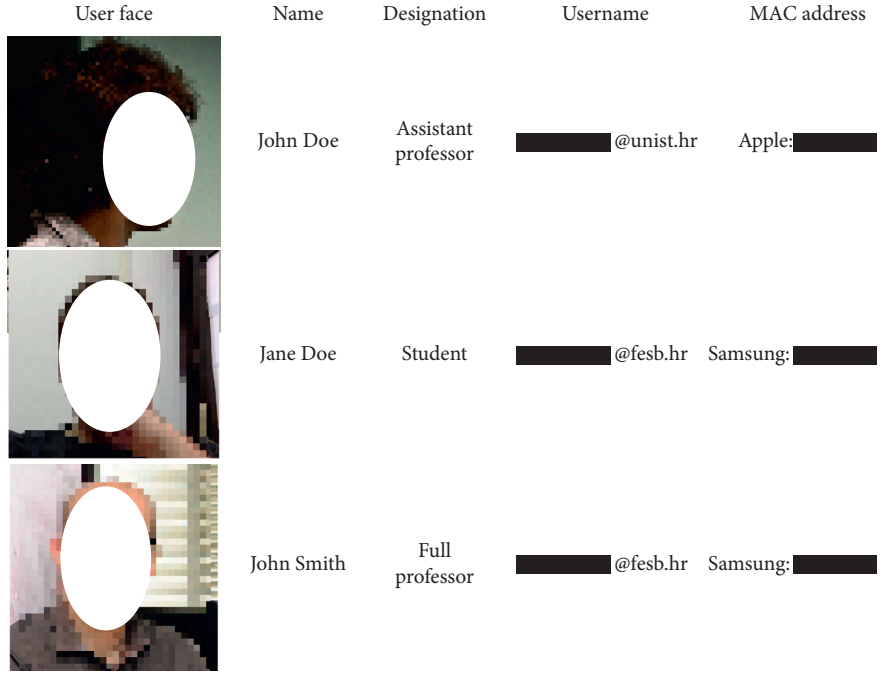

Figure 4: Web page created to link user device (MAC address) with the user-his/her face.

private location information. This indicates that linking username, hence a person, with MAC address can further help adversary in disclosing user whereabouts [22, 23]. A large number of research papers highlight the risk of privacy violation by analyzing Wi-Fi probes and MAC address along with encrypted and unencrypted traffic [4, 23–29]. Recently, vendor manufacturers started to use MAC randomization to prevent such privacy leaks. However, it seems that it is quite challenging to preserve the privacy using MAC randomization [30, 31] through the use of sequence numbers while sending probe requests or by sending the complete PNL list with randomized MAC address, which separates users from the unique fingerprint determined by continuously repeated PLN list of SSIDs.

The attacker could install a set of passive Wi-Fi sniffers, for example, around the university campus, at music festivals, or even at demonstrations that act as MAC address catchers. These sensors could be used for tracking people [22]. For instance, people could be tracked when visiting clinics or political campaigns. Generally, geolocating the device and linking its identity with a real person pose a serious privacy threat.

4. Privacy Leaks of Phase 2 of EAP Authentication

The nature of devices to automatically attempt to establish a Wi-Fi connection once the device gets within range, without any user involvement, allows adversaries to easily perform active attacks using an evil twin Wi-Fi network. In this section, the results of an evil twin attack on Eduroam network are presented from the data collected during two months at our university. The goal of such an attack is to collect user identity or user credentials in Phase 2 of

EAP authentication protocol, denoted as tunneled authentication.

4.1. Results-Captured Usernames at University Campus. A total number of 1650 unique devices attempted connection to evil twin Eduroam network over the course of two months. Table 4 summarizes the protocols employed by devices in their configuration profiles for Eduroam network. Out of all devices, 1019 (61%) did not employ certificate validation, which resulted in direct device deanonymization by sending username in Phase 2 of EAP authentication protocol. From other interesting observations, 392 user identities had PAP inner authentication protocol, where user credentials were sent in the clear to the authentication server. The other 606 users enabled MSCAHPv2 protocol, where challenges and responses were captured and stored (in a form of hash value). Since MSCHAPv2 protocol is also insecure [32], passwords can still be extracted by utilizing offline or online brute-force attack or dictionary attack on the collected challenge/response messages using tools such as ASLEAP (https://tools.kali.org/wireless-attacks/asleap) or John the Ripper (https://tools.kali.org/password-attacks/john). Two devices used MSCHAP protocol, while 19 devices used PEAP. Recent works [8–10] also noticed that a large portion of users (in similar percentages to those in our university/faculty) use an insecure configuration to connect to Eduroam network, which confirms our findings.

4.2. Implications and Other Observations. In this section, other interesting observations are outlined for the evil twin attack on Eduroam network during the period of two months.

4.2.1. IMSI Catcher. Recall that, in this paper, we focused on device deanonymization by revealing client usernames and linking them to the device MAC address, as well as stealing user credentials (usernames and passwords) through automatic connection attempts to evil twin WPA2-Enterprise AP. However, in the implementation of evil twin attack, users were not granted access to the Internet, although all phases of the authentication protocol were completed and users were connected to the fake Eduroam network.

The majority of captured usernames and user credentials (along with MSCHAPv2 challenges and responses) result from supplicants automatically initiating a connection to the Eduroam network once they move in a range of fake Eduroam AP. However, some devices tried to establish a connection to Eduroam network using different EAP authentication protocols (different from ones supported by Eduroam). This indicates that users, within a range of Eduroam network, tried to establish a connection to the Eduroam network by testing various EAP protocols provided by the supplicant. Since users are generally unfamiliar with authentication protocols provided by Eduroam network [9], devices equipped with, for example, Android OS, give users the possibility to manually select from one of the EAP protocols during the configuration of their supplicant.

Table 4: Summary of captured Eduroam credentials.

	PAP	MSCHAP	MSCHAPv2	PEAP	Total
Our institution	238	0	295	7	540
Other inst. in university	63	1	132	2	198
Other universities	2	0	6	3	11
Usern. without institution	89	1	173	7	270
Total	392	2	606	19	1019

One of these protocols is EAP-SIM/AKA protocol [33, 34], whose security was analyzed in [35]. During the authentication phase, an authenticator (in our case RPi device) sends an EAP Request/Identity message to the supplicant device. If supplicant utilizes EAP-SIM/AKA protocol, it replies with EAP-Response/Identity message sent in the clear, which is IMSI number. This number is a global unique identifier and must be kept secret at all times. By selecting EAP-SIM/AKA authentication protocol, at least seven IMSI numbers from the data were captured via *tshark* network analyzer tool.

4.2.2. Modifying Configuration Profiles. From the analyzed EAP response messages, at least 78 users modified their configuration profiles (anonymous field) once, while 20 users revealed their username by replacing the anonymous identity in anonymous field with their exact username. At least 7 users inserted their password in anonymous field of their configuration profile. Interestingly, on some devices, multiple usernames were collected, indicating that users gave their devices to colleagues for them to test whether their configuration profile could grant them access to the evil twin Eduroam AP.

Also, 17 users switched from EAP-TTLS MASCHAPv2 to a less secure PAP, giving the password to the attacker in the clear. At least 27 users tested different EAP-TTLS MSCHAPv2 configuration profiles from collecting/observing usernames in MSCHAPv2 inner authentication protocols. Note that challenges and responses were not logged in MSCHAPv2 inner authentication, while no additional brute-force attack was performed, so we cannot say whether the users tested different passwords during the login procedure by not modifying the username. Also, 9 users tested different passwords with PAP inner authentication protocol; note that, with PAP, both username and password are sent in the clear.

From the collected usernames in the EAP-Response/Identity field, 113 users were equipped with at least two devices. By not granting the users access to the Internet over fake Eduroam network, 36 users/devices switched off certificate verification, allowing the attacker to steal their credentials.

As stated in many research papers, people are focused on getting their work done, as they do not have the time to continuously search for privacy and security threats. In the case of Eduroam network, where users modify their supplicant profiles for the WPA2-Enterprise network, it is clear that users aim at switching off security features such as

certificate validation to get access to the network. In combination with visibility problems, which are characteristic in human-computer interaction, users became disconnected between their actions, as their configuration profiles, once successfully giving them access to the Eduroam network, now fail them at getting the work done [36, 37], establishing an Internet connection. Other than that, not knowing the meaning of certificate validation, anonymous identity field, and all other protocols and simultaneously allowing the users control over their actions (modifying configuration fields) can easily lead to security and privacy threats. Furthermore, giving users an option to manually select from various protocols, especially if users are not given service such as access to the Internet, motivates them to modify the existing configuration profiles, which can lead to serious security and privacy problems in the end. Indeed, as shown in [9], 35.3% of users "have played with configuration options until it worked." This indicates that the attack in which users were not granted access to the network is quite dangerous and might lead to an insecure configuration that would reveal username to the attacker, bearing in mind that at the same time they do have control over their supplicant configuration profiles. This only raises a general fact that users want to use a free service provided to them by Eduroam network. If this service is given to them (e.g., by seeing an Eduroam network in the supplicant menu), some users will test the majority of possible combinations given to them via a supplicant menu just to establish an Internet connection. As the results of conducted evil twin attack suggest, not giving users the access to the Internet motivated users to switch off the certificate verification. Other users switched from MSCHAPv2 to less secure PAP inner authentication protocol, some even used EAP-AKA/SIM protocol and sent IMSI numbers, and others revealed their username, while at the end some inserted password into anonymous identity field.

4.2.3. Implications of Collecting Eduroam Credentials. In our country, Eduroam credentials are linked with authentication and authorization infrastructure of science and higher education (`AAI@EduHr`), with 900,000 e-identities available within the system [38]. With captured credentials, users can access many services, thus compromising user (identity and personal) privacy. For example, students and faculty employees from all universities in the country have access to service e-Citizens, a project of the Croatian Government, where "citizens can request electronic copies of birth certificates, marriage or life partnership certificate, ask for electronic records of residence or owned vehicles and many other documents" [38], without using two-factor authentication (only username and password, same as the ones used for Eduroam). Clearly, by capturing user credentials, a large portion of private user information is given to the attacker.

With Eduroam credentials, students have access to the grading system and to course materials, and they can vote for a course they would like to attend next year. The course with the majority of votes will be offered to the students for enrollment over the course of the following academic year. With Eduroam credentials, students and employees of the faculty/university have access to the MSDN Academic Alliance system for personal download of Microsoft software. An adversary, therefore, has access to a list of personal software licenses.

Moreover, scientists in our country can use `AAI@EduHr` credentials (same as those used for Eduroam) to access their ResearcherID (https://www.researcherid.com), ORCID (https://orcid.org/my-orcid), and CROSBI (Croatian research database) profiles ([https://www.bib.irb.hr]). For example, Clarivate Analytics (formerly Thomson Reuters) assigns the ResearcherID profile to every author on demand. Using ResearcherID, the authors link their published work facilitating the process of following their scientific production. As denoted on the ResearcherID web page, "...ResearcherID, Web of Science, and EndNote (all offerings from Clarivate Analytics) share login credentials," which indicates that `AAI@EduHr` credentials can be used to access all these services as well. Since the majority of universities around the globe base their rankings on publications in Web of Science databases, universities advise their employees to regularly update their profiles according to these databases. Within the university, departments also rank themselves according to these publications. Since all profiles, ResearcherID, ORCID, and CROSBI, can be linked with Eduroam credentials, stealing credentials can motivate adversary into modifying/deleting user profiles in these databases.

Implications of stealing/learning Eduroam user credentials have been analyzed for only one institution and one university. We believe that universities around the world also utilize Eduroam credentials for similar and many other services, which only indicates how inappropriate configuration of WPA2-Enterprise supplicant opens a backdoor to other serious privacy concerns. Whether users reuse Eduroam credentials (usernames and/or passwords) on other services (e.g., Instagram, Facebook, etc.) remains an open problem, which is out of the scope of this paper. For future work, we plan to expand our analysis to cover other universities as well.

5. Countermeasures

From the analysis performed in this paper, it can be seen that, by collecting WPA2-Enterprise usernames, along with complete user credentials (usernames with passwords), systems can have serious implications on user anonymity. The results of the above analysis, as well as a study conducted in previous research papers [8–10], indicate that preserving user's privacy is not well recognized, and a large focus is placed on stealing user credentials in WPA2-Enterprise systems rather than on user deanonymization-collecting usernames and linking them (i.e., a user-his/her face) with device MAC address. A two-month study of the WPA2-Enterprise Eduroam network showed that usernames are indeed sent in the clear over the air, mostly because configuration profiles used for Eduroam network (downloaded from official Eduroam CAT) in a large number of

universities do not explicitly set up anonymous identity (outer identity) field. A more detailed analysis of 1066 institutions from 18 countries showed that 67% do not use anonymous identity in their configuration setup (Table 2).

Preventing Device Deanonymization in Phase 1: What Can Be Done? By default, a tool called Eduroam Identity Provider administrator from GEANT allows university and research institution administrators to generate customized Eduroam installers for various platforms (https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+IdP+administrators). Currently, in their settings, it is stated that administrators can decide whether they want the generated installers to be configured with an anonymous outer identity, and, by default, this feature is not enabled. Hence, the first step to secure the users from passively stealing usernames would require Eduroam administrators to preconfigure Eduroam installers (configuration profiles) found on Eduroam CAT web page to include anonymous outer identity. A further step would require GEANT to at least enable anonymous outer identity field by default or make it enabled by default without giving administrators an option to disable it, which would be a more rigorous approach. Unfortunately, this still does not prevent users from modifying installed configurations for Eduroam network on supplicant devices or even configuring connection settings on their own from scratch.

Preventing Security and Privacy Leaks in Phase 2: What Can Be Done? Our findings as well as the analysis in other research papers [8, 10] indicate that stealing the user credentials with evil twin attack is based on the fact that the user's supplicant devices skip certificate validation during the procedure of WPA2-Enterprise connection. To prevent these types of attacks, university and research institution administrators should generate CAT installers that skip certificate validation. Similarly, as above, users can still modify configurations on supplicant devices, but it is believed that appropriate configuration from administrators will reduce username and credential leak in both phases of the EAP authentication protocol.

Some papers discuss other attempts to prevent modifications on the supplicant side. In the recent paper, an approach is presented, where certificate validation can never be skipped [8]. Indeed, in recently proposed WPA3-Enterprise standard, to prevent against certain types of attacks, certificate validation is mandatory on the client side when WPA3-Enterprise is used [39]. Also, the recently proposed standard from Wi-Fi Alliance uses secure, cellular roaming for WPA2-Enterprise-based networks [40]. The protocol proposes many hotspots deployed around the world, which allow users to authenticate using SIM card, certificate or username, and password. It seems that recent discoveries on the problem of certificate validation resulted in importing new security features in recent standards. It yet remains to be seen how the problem of sending usernames in the clear will be affected by the proposed solutions, even within the presence of certificate verification. Even if certificate validation is mandatory by new protocols and standards, it also remains to be seen how users would react within the presence of an evil twin AP that does not establish a connection with a supplicant. This is especially interesting given that users can control all fields, which in the presence of arisen frustration (not being connected to the Internet) may force users to enter usernames and passwords in all available fields and/or select from the range of available protocols, which may result in disclosing usernames, credentials, or IMSI numbers.

6. Conclusion

In this paper, a new approach to device deanonymization and information theft is presented, which exploits WPA2-Enterprise vulnerabilities within the Eduroam network. When configured improperly, devices connecting to Eduroam network allow the attacker to passively monitor Wi-Fi traffic and read the username sent by the victims device during Phase 1 of EAP authentication. A two-month experimental attack mounted on our university showed that, out of 1650 different devices, 67% are subject to device deanonymization attack. Further analysis of the Configuration Assistant Tools of 1066 institutions from all over the world shows that 67% of Eduroam profiles reveal the user's identity in the clear, thus linking all the Wi-Fi traces done by that device to its owner. In line with the findings based on the Configuration Assistant Tools analysis, another experimental attack has been performed at a large-scale international music festival, where we found that 70% of the observed devices are vulnerable to the same passive attack.

Mounting an evil twin Eduroam network will prompt the nearby devices to automatically establish a connection enabling the attacker to perform an active attack, where device deanonymization as well as user credentials theft can be achieved at Phase 2 of EAP authentication. During the two-month experiment at our university, 61% of the devices did not employ certificate validation, allowing us access to their Eduroam credentials and even linked services such as e-Citizens, where one can download electronic copies of birth certificates, marriage certificates, or life partnership certificates. Even though a portion of the users had safely configured devices, they opted to tamper with the Wi-Fi configuration profiles after having been denied Internet access, ultimately making them susceptible to the attack or even leaking device's IMSI number.

As a countermeasure, network administrators are advised to properly create configuration profiles that will prevent information leaks (usernames and credentials) in Phase 1 and Phase 2 of EAP authentication. Although users can still tamper with the Wi-Fi configuration profile, thus making them vulnerable to the deanonymization attack, we believe that the appropriate configuration will greatly reduce the attack's success rate.

Data Availability

To preserve privacy of users, the data were logged and are only available to the authors of the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Cunche, "I know your MAC Address: targeted tracking of individual using Wi-Fi," in *Proceedings of the International Symposium On Research In Grey-Hat Hacking-GreHack*, Grenoble, France, November 2013.

[2] D. Shaoyong, H. Jingyu, G. Yue, and Z. Sheng, "Ev-linker: mapping eavesdropped wi-fi packets to individuals via electronic and visual signal matching," *Journal of Computer and System Sciences*, vol. 82, no. 1, pp. 156–172, 2016.

[3] C. Matte, J. P. Achara, and M. Cunche, "Device-to-identity linking attack using targeted wi-fi geolocation spoofing," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, New York, NY, USA, June 2015.

[4] M. Cunche, M. A. Kâafar, and R. Boreli, "I know who you will meet this evening! Linking wireless devices using Wi-Fi probe requests," in *Proceedings of the 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, San Francisco, CA, USA, June 2012.

[5] C. Troncoso, M. Payer, J.-P. Hubaux et al., "Decentralized privacy-preserving proximity tracing," 2020, http://arxiv.org/abs/2005.12273.

[6] J. Chan, D. Foster, S. Gollakota et al., "Privacy sensitive protocols and mechanisms for mobile contact tracing," 2020, http://arxiv.org/abs/2004.03544.

[7] N. Cheng, X. Wang, W. Cheng, P. Mohapatra, and A. Seneviratne, "Characterizing privacy leakage of public WiFi networks for users on travel," in *Proceedings of the IEEE INFOCOM*, Turin, Italy, April 2013.

[8] A. Bartoli, E. Medvet, and F. Onesti, "Evil twins and WPA2 Enterprise: a coming security disaster?" *Computers & Security*, vol. 74, pp. 1–11, 2018.

[9] A. Bartoli, E. Medvet, A. D. 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*, Hamburg, Germany, August 2018.

[10] 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 & Privacy in Wireless and Mobile Networks*, New York, NY, USA, June 2015.

[11] V. Ramachandran, "Cracking WPA/WPA2 Personal And Enterprise for Fun and Profit," Hacktivity, Budapest, Hungary, 2012.

[12] K. Wierenga, S. Winter, and T. Wolniewicz, "The eduroam architecture for network roaming," 2015, https://www.tools.ietf.org/html/rfc7593/.

[13] J. Snoodgrass and J. Hoover, "BYO-Disaster and why corporate security still sucks," *DEFCON*, vol. 21, 2013.

[14] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP), RFC 3748 (proposed standard), Internet engineering task force," 2004, http://www.ietf.org/rfcrfc3748.txt.

[15] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS authentication protocol, RFC 5216 (proposed standard), internet engineering task force," 2008, http://www.ietf.org/rfc/rfc5216.txt.

[16] P. Funk and S. Blake-Wilson, "Extensible authentication protocol tunneled transport layer security authenticated protocol version 0 (EAP-TTLSv0), RFC 5281 (informational), internet engineering task force," 2008, http://www.ietf.org/rfc/rfc5281.txt.

[17] Microsoft, "MS-PEAP protected extensible authentication protocol (PEAP)," 2018, https://msdn.microsoft.com/en-us/library/cc238354.aspx.

[18] L. Demir, M. Cunche, and C. Lauradoux, "Analysing the privacy policies of Wi-Fi trackers," in *Proceedings of the 2014 Workshop on Physical Analytics*, Bretton Woods, Carroll, NH, USA, June 2014.

[19] M. Ghering, "Evil twin vulnerabilities in Wi-Fi networks," Bachelor thesis, Radboud University, Nijmegen, Netherlands, 2016.

[20] F. Fund, "Run a man-in-the-middle attack on a WiFi hotspot," 2019, https://witestlab.poly.edu/blog/conduct-a-simple-man-in-the-middle-attack-on-a-wifi-hotspot/.

[21] N. Sidiropoulos, M. Mioduszewski, P. Oljasz, and E. Schaap, "Open WiFi SSID broadcast vulnerability," *SSN Project Assessment*, vol. 24, 2012.

[22] B. Bonne, A. Barzan, P. Quax, and W. Lamotte, "WiFiPi: involuntary tracking of visitors at mass events," in *Proceedings of the World Of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Madrid, Spain, June 2013.

[23] M. Cunche, "I know your MAC address: targeted tracking of individual using Wi-Fi," *Journal of Computer Virology and Hacking Techniques*, vol. 10, no. 4, pp. 219–227, 2014.

[24] A. Dagelić, M. čagalj, G. Perković, and M. Biloš, "Towards linking social media profiles with user's wifi preferred network list," *Ad Hoc Networks*, vol. 107, no. 1, p. 102244, 2020.

[25] A. Dagelic, T. Perkovic, B. Vujatovic, and M. Cagalj, "SSID oracle attack on undisclosed Wi-Fi preferred network lists," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 5153265, 15 pages, 2018.

[26] J. Atkinson, "Your WiFi is leaking: inferring private user information despite encryption," Thesis (Doctoral), 2015.

[27] N. Cheng, X. Oscar Wang, W. Cheng, P. Mohapatra, and A. Seneviratne, "Characterizing privacy leakage of public WiFi networks for users on travel," in *2013 Proceedings IEEE INFOCOM*, Turin, Italy, April 2013.

[28] P. Falcone, F. Colone, A. Macera, and P. Lombardo, "Localization and tracking of moving targets with WiFi-based passive radar," in *Proceedings of the 2012 IEEE Radar Conference*, Atlanta, GA, USA, May 2012.

[29] J. Freudiger, "How talkative is your mobile device?: an experimental study of Wi-Fi probe requests," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, New York, NY, USA, June 2015.

[30] M. Vanhoef, C. Matte, M. Cunche, L. S. Cardoso, and F. Piessens, "Why MAC address randomization is not enough: an analysis of Wi-Fi network discovery mechanisms," in *Proceedings of the 11th ACM on asia Conference on Computer and Communications Security*, Xi'an, China, June 2016.

[31] C. Matte, M. Cunche, F. Rousseau, and M. Vanhoef, "Defeating MAC address randomization through timing attacks," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, Darmstadt, Germany, July 2016.

[32] B. Schneier, Mudge, and D. Wagner, "Cryptanalysis of microsoft's PPTP authentication extensions (MS-CHAPv2)," in *Proceedings of the International Exhibition and Congress on Secure Networking-CQRE (Secure) '99*, Düsseldorf, Germany, December 1999.

[33] H. Haverinen and J. Salowey, "Extensible authentication protocol method for global system for mobile communications (GSM) subscriber identity modules (EAP-SIM), RFC 4186 (informational), internet engineering task force," 2006, http://www.ietf.org/rfc/rfc4186.txt.

[34] J. Arkko and H. Haverinen, "Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA), RFC 4187 (informational), internet engineering task force," 2006, http://www.ietf.org/rfc/rfc4187.txt.

[35] P. O'hanlon, R. Borgaonkar, and L. Hirshi, "Mobile subscriber WiFi Privacy," in *Proceedings of the IEEE Symposium On Security And Privacy 2017 Workshop on Mobile Security Technologies*, San Jose, CA, USA, February 2017.

[36] P. Dourish, R. E. Grinter, J. Delgado de la Flor, and M. Joseph, "Security in the wild: user strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 391–401, 2004.

[37] P. Dourish and D. Redmiles, "An approach to usable security based on event monitoring and visualization," in *Proceedings Of the 2002 Workshop on New Security Paradigms*, pp. 75–81, Las Vegas, NV, USA, May 2002.

[38] M. Bozac, "e-Gradani i e-usluge su u razvoju, ali broj korisnika još je uvijek nizak," 2017, https://markobozac.com/dirty-hands/2017/05/e-gradanin-e-usluga-broj-korisnika/.

[39] Teldat, "WPA3: improved Wi-Fi Security," 2018, https://www.teldat.com/blog/en/wpa3-wi-fi-network-security-wpa3-personal-wpa3-enterprise/.

[40] Wi-Fi Alliance, "Wi-Fi CERTIFIED™ passpoint (Release 2) deployment guidelines rev 1.1," 2016, https://www.wi-fi.org/downloads-public/Passpoint\text{_}R2\text{_}Deployment\text{_}Guidelines-v1.1.pdf/13481/.