applied sciences

MDPI

Review

Understanding Server Authentication in WPA3 Enterprise

Alberto Bartoli

Dipartimento di Ingegneria e Architettura, University of Trieste, 34125 Trieste, Italy; bartoli.alberto@units.it

Received: 29 September 2020; Accepted: 4 November 2020; Published: 6 November 2020

Abstract: In December 2019, the Wi-Fi Alliance published version 2 of WPA3, the new certification program for Wi-Fi devices that updates WPA2. This new version of WPA3 addresses, amongst other things, one of the crucial weaknesses of WPA2: in many practical deployments of *enterprise* Wi-Fi networks—i.e., networks in which users have personalized credentials—a device may easily be attacked by fraudulent access points claiming to have the name of the targeted network (*evil twins*). In this work, we present the mechanisms that WPA3 version 2 has introduced for mitigating these risks, which have become more and more relevant in recent years. We discuss the defensive power and potential impact of the various options available. Understanding the resulting scenario is important because WPA3 will determine the behavior of such a fundamental and widespread technology as enterprise Wi-Fi for many years, yet WPA3 enterprise networks may still be configured in a way that could not provide much better defensive power than WPA2.

Keywords: network security; internet security; password; authentication

1. Introduction

In April 2018, the Wi-Fi Alliance published the technical details of the WPA3 certification program for Wi-Fi devices. WPA3 updates the WPA2 program, which had been specified more than 14 years earlier, and includes several capabilities aimed at enhancing the security properties of Wi-Fi networks. In December 2019, the Wi-Fi Alliance published version 2 of WPA3 [1]. This new version addresses, amongst other things, one of the crucial weaknesses of WPA2 that was not addressed in the first version of WPA3 and that affects *enterprise* Wi-Fi networks—i.e., networks in which each user has personalized credentials for all of his/her devices; in many practical deployments, a device may easily be attacked by fraudulent access points claiming to have the name of the targeted Wi-Fi network (*evil twins*) [2]. The impact of a successful attack of this kind depends on the specific attack scenario and may range from the evil twin acting as a man-in-the-middle for all the network traffic of the connected device to the evil twin collecting traffic sufficient for the offline guessing of the network credentials of the user that owns the device [3–7].

The weakness exploited in this class of attacks consists of a mismatch between the *assumptions* made in the WPA2 specification and the *reality* of its practical deployment. WPA2 assumes that each device needs be configured, before connecting, with certain identity information tailored to the specific enterprise network of interest, and that the device verifies at the connection time that the identity claimed by the network matches the identity specified in the configuration [1,8,9]. Devices that do not satisfy these requirements may be tricked into connecting to an evil twin that claims to have the identity of any enterprise network (as illustrated in more detail below) [10]. The problem is that insecure configurations of devices that connect to enterprise networks are quite commonplace. A recent survey with almost 1000 users of academic environments reports that more than 75% or respondents either do not know the name of the authorization server or do not even know that there is an authorization

server to be associated with the SSID of the enterprise network [11]. According to the same survey, only half of the respondents configured their devices correctly, by means of an automatic tool, and 40% of 311 configuration guides published by 69 academic institutions contain indications that lead or may lead to an insecure configuration. Other surveys on the topic of management of personal devices in enterprise Wi-Fi environments identified the same problem [12–15].

The risks introduced by evil twins have become more and more relevant since 2004, when WPA2 was specified, for three key reasons. First, network credentials have become very valuable to attackers, because virtually all enterprises have migrated to single sign-on architectures, and thus network credentials often unlock access to all enterprise services. Second, everyone is now permanently carrying a Wi-Fi-enabled smartphone, which often contains the user's enterprise credentials and connects to Wi-Fi networks *automatically*—e.g., while the user is walking with a smartphone in his/her pocket. Third, attacks aimed at stealing network credentials may occur potentially anywhere and are virtually impossible to detect; they are executed automatically, in less than a second of proximity to an evil twin (which may easily be hidden within a small bag, for example) and without any need to involve the device owner in a working session [10].

WPA3 version 2 thus addresses a long-awaited need for better defensive mechanisms in enterprise Wi-Fi networks [2]. In this work, we discuss the defensive power and potential impact of the various options available, along with the corresponding security maintenance cost tradeoffs. We are not aware of any similar analysis. Understanding the resulting scenario is important because WPA3 will determine the behavior of such a fundamental and widespread technology as enterprise Wi-Fi for many years, yet WPA3 enterprise networks may still be configured in a way that could not provide much better defensive power than WPA2.

The paper is organized as follows. In Section 2, the necessary background on the WPA2 Enterprise is provided, along with a description of the threat model, the relevance of the corresponding risks, and the existing literature on the subject. In Section 3, the new defensive mechanisms of WPA3 Enterprise are described. These mechanisms can be actually deployed in a variety of ways, with widely differing defensive power. In Section 4, the scenarios corresponding to the most common options are analyzed in detail. Section 5 provides a discussion of the defensive power of WPA3 Enterprise against attacks based on evil twins and attempts to provide a perspective on the likely future scenarios in this respect.

2. Background: Server Authentication in WPA2 Enterprise

In this section, we provide the necessary background on WPA2 Enterprise and focus on the configurations most commonly used. A Wi-Fi device (a *supplicant*) may connect to an enterprise network only after executing an authentication protocol with the *Authentication Server* (AS) for that network. For the purpose of our discussion, this protocol may be summarized as follows (we refer the reader to the abundant literature on the subject for full details—e.g., [9]):

- Phase 1: the supplicant verifies the identity of the AS for the network it is attempting to connect to.
- Phase 2:

    1. The supplicant sends user credential material to the AS.
    2. The AS demonstrates knowledge of the user credentials to the supplicant.

In Phase 1, the AS provides a certificate binding its name to a public key and the two parties establish a cryptographically secure TLS tunnel based on that public key (much like what happens at a higher level of the network software stack, when a browser connects to a web server with the HTTPS protocol). Phase 2 is executed within the TLS tunnel created at step 1.

Note that the certificate does *not* bind a public key to the name of the wireless network (i.e., to its SSID), only to the name of the AS. For example, in our university, the name of the network is eduroam, while the name of the AS is raggio.units.it. The correct execution of step 1 thus requires certain configuration information that must be stored on the supplicant before connecting—i.e., a *network*

profile. The network profile must include the association between the SSID of the network and the name of AS, where the AS name is provided in the form of a certificate.

WPA2 Enterprise left crucial security details regarding AS authentication unspecified. In particular, it was not specified how to make sure that: (i) the supplicant is indeed equipped with a network profile, (ii) the network profile is accurate, and (iii) the supplicant indeed uses the network profile as specified. WPA2 Enterprise merely assumed—i.e., took for granted—that these requirements are met by every supplicant at every organization. These details have far-reaching implications for the security of the network, its users, and the organization as a whole.

To clarify, consider a fraudulent wi-fi access point broadcasting the name of an enterprise network—i.e., an evil twin (ET) [3–7]. ET-based attacks can be classified as proposed in [7]: *replacement*, where a legitimate access point is switched off and replaced by the ET at the same location; *coexistence*, where the ET coexists with a legitimate access point at the same location; *remote clone*, where the ET is at a location where there is no legitimate access point. In this work, we are mainly interested in remote clone scenarios, in particular at locations that have nothing to do with the enterprise. We consider attacks aimed at eliciting credential material from the supplicant for later offline credential guessing [16–18]. The typical scenario for these attacks consists of users which carry supplicants configured for connecting to the wireless enterprise network automatically (e.g., smartphones) and that move outside of the enterprise. Attacks of this kind require a supplicant that remains in close proximity with an ET for a very short time and may occur potentially anywhere, often without any involvement of the user at the supplicant.

Consider a supplicant that happens to pass nearby an ET and whose configuration does not satisfy requirement (iii) above—e.g., a supplicant configured with such commonly available options as "skip certificate validation" or "accept any certificate". The supplicant will start interacting with ET, will complete Phase 1, and will begin the execution of Phase 2, often without any user action. Phase 2 will fail because the ET will not be able to prove knowledge of the user credentials, but the supplicant might disconnect when it is too late—i.e., after having already sent credential material to the ET. Similarly, consider a supplicant that does not satisfy either requirement (i) or (ii) —i.e., a supplicant that indeed checks the validity of received certificates but that does not know the name of the AS. In this case, the supplicant may start interact with ET as above, because the ET may legitimately own a certificate issued by a certification authority considered trusted by the supplicant. Even in this case, phase 2 will fail but the ET may have collected credential material.

In summary, supplicants which are not configured to use the correct Authentication Server name for a given enterprise network and to verify that the claimed identity of an Authentication Server indeed matches that name could be tricked into executing the authentication protocol with any ET claiming to have the SSID of that network [8]. The impact of attacks of this kind depends on the specific supplicant and may range from the evil twin acting as a man-in-the-middle to the evil twin obtaining either the user password or a hash of the user password [10]. In practice, supplicants that are not configured correctly are very common. Users often select the SSID of the enterprise network, insert their credentials, and then play with the network configuration until connecting, usually by selecting "skip certificate validation" or "accept any certificate". WPA2 Enterprise does not specify any means for *preventing* this behavior.

Organizations may adopt security policies that forbid insecure configurations or that mandate the usage on the enterprise network only by supplicants that have been approved (and hopefully correctly configured) by the IT staff. However, WPA2 Enterprise does not provide any technical means for detecting connection attempts from supplicants that are not compliant with the security policy. Furthermore, organizations often suggest insecure configuration practices—i.e., of the form "skip certificate validation" or "accept any certificate" [11]—which means that either network administrators are not aware of the corresponding risks or choose to ignore those risks, perhaps because the need to support users in configuring their devices would take away precious (and usually scarce) resources that may be devoted to other activities relevant to the overall security of the organization. The net result

is that WPA2 Enterprise is very often deployed by violating crucial security-relevant requirements, which creates significant security risks for users and for the organization as a whole.

A detailed and comprehensive survey of the defensive mechanisms that have been proposed for mitigating ET-based attacks to WPA2 Enterprise environments can be found in [7]. Most of the proposed defenses can mitigate attack scenarios where the ET either coexists with a legitimate access point or replaces one of those—in other words, those mechanisms are suitable for defending against attacks that occur at locations *within* the enterprise. According to this survey and to our knowledge, only three defense mechanisms capable of mitigating remote clone attacks—i.e., the attacks that may occur potentially anywhere and that are considered in the present work—have been proposed in the literature. Two of these mechanisms required significant changes to the authentication protocols used in WPA2 Enterprise and thus were not compatible with the existing infrastructure already deployed worldwide [19,20]. A third proposal for defending against remote clone attacks that did not require any change to WPA2 protocols can be found in [10]. The cited work was based on a significant change in the interface presented by supplicants to users; essentially, supplicants should distinguish between WPA2 Personal networks (those where a single password is shared by all supplicants and that are typically used in home environments) and WPA2 Enterprise networks, and users should identify networks in the latter category not only by their name (i.e., SSID) but also by the name of their Authentication Server. An advantage of this proposal was that it could be implemented fully on the supplicant side and that it could coexist with the existing WPA2 infrastructure.

Finally, we emphasize that the attacks of our interest are fully orthogonal to those made possible by vulnerabilities in cryptographic protocols, either in WPA2 [21] or in WPA3 [22]. The attacks in the cited works assume the ability to observe the encrypted traffic between the targeted supplicant and a legitimate access point. By exploiting certain vulnerabilities in cryptographic protocols, these attacks allow attackers to decrypt traffic (KRACK [21]) and to obtain supplicant credentials (DRAGONBLOOD [22]).

3. Server Authentication in WPA3 Enterprise

In this section, we provide a simplified description of the mechanisms provided by WPA3 Enterprise for reducing the risks associated with AS authentication. Our description does not cover all possible execution patterns and focuses instead on those that are most useful for understanding the defensive power of WPA3 Enterprise. We refer to the original document for full details [1].

First and foremost, WPA3 Enterprise forbids such supplicant configuration options as “skip certificate validation” or “accept any certificate”. WPA3 Enterprise dictates that if the supplicant fails to verify the server identity during Phase 1, the supplicant *cannot* enter Phase 2 automatically; the supplicant may enter Phase 2 only if the user *explicitly* accepts trust in the certificate provided by the AS—for example, by means of a dialog window. This interactive mechanism is called User Override of Server Certificate (UOSC).

The server identity in Phase 1 is considered verified if the AS has the name specified in the network profile or it has the same name as in the last successful connection. The two more common scenarios in which server identity validation fails and thus UOSC comes into play are:

- The supplicant is *not* configured with a network profile.
- The supplicant executes Phase 1 with an AS whose name is *different* from the name of the AS upon the last successful connection.

The fact that UOSC requires the *explicit* involvement of the user is a significant security improvement over WPA2 Enterprise; attack opportunities are limited only to when the user is actively interacting with the supplicant in order to connect to the enterprise network—e.g., the smartphone cannot enter Phase 2 with an ET automatically while the user is walking with a smartphone in his/her pocket.

Second, WPA3 Enterprise allows network administrators to constrain how supplicants may learn the name of the AS—i.e., how supplicants may obtain the certificate containing that name.

1. A supplicant may obtain the certificate from the AS itself, upon *every* connection.
2. A supplicant may obtain the certificate from the AS itself only upon the *first* connection; subsequent connections must use the same certificate of the first connection.
3. A supplicant can *never* obtain the certificate from the AS itself. The supplicant must be configured with a network profile—that is, it can only obtain the certificate by means of some out-of-band (secure) communication channel.

Option 1 is essentially equivalent to WPA2 Enterprise but with a crucial difference: when the supplicant observes that the name of the AS has changed, the requirement for explicit user involvement results in a much more secure setting, as observed above.

Option 2 is a form of Trust on First Use (TOFU). If the first connection is performed with the legitimate AS, then the supplicant will never enter Phase 2 with an ET. The user could explicitly accept trust in a certificate sent by an ET and enter Phase 2 (thereby leaking credential material to the attacker), but only if the supplicant has never connected to the enterprise network before. Server authentication based on forms of TOFU is widely used for secure remote access to network services with the Secure Shell (SSH) protocol [23] and was also proposed for enterprise Wi-Fi networks in a framework based on self-signed public keys without any need for certification authorities [19].

Option 3 is the most secure one: the supplicant will connect only to the AS that authenticates itself with a certificate identical to the one in the network profile already installed. With this option, an attacker may follow two tactics:

- Attack the communication channel that supplicants use for obtaining the network profile. The security properties of this channel will depend on the security policy of the organization and are orthogonal to WPA3 Enterprise.
- Attack supplicants that have never connected to the network and have not (yet) installed the network profile. In this case, the user could explicitly accept trust in a certificate sent by an ET and leak credential material. It follows that, even with the most secure option, WPA3 does not provide network administrators with a means to prevent connection attempts by supplicants that are supposed to install a network profile.

The three above options are implemented as follows. An enterprise network may be associated with a Trust Override Disable (TOD) policy that, when present, is contained in the certificate policy extension of the certificate presented by the AS. WPA3 Enterprise defines two such policies:

- TOD-STRICT, which means that UOSC must never be used for that network. That is, when server certificate validation fails, the user must not be asked to accept trust in the certificate received from the network and the connection attempt must be aborted without entering Phase 2. This TOD policy corresponds to option 3.
- TOD-TOFU, which means that UOSC may only be used upon the first connection attempt. The user may be asked to accept trust in the certificate received from the network only if the supplicant has never connected to the network, otherwise the connection attempt must be aborted without entering Phase 2. This TOD policy corresponds to option 2.

Finally, a certificate without any TOD policy corresponds to option 1.

In other words, network administrators may instruct supplicants of the rules for learning the name of the AS. However, these rules are encoded in the certificate of the (legitimate) AS of the network. As such, these rules *cannot* constrain the behavior of supplicants who attempt to connect *before* receiving such a certificate or installing the network profile.

4. Examples

For the purpose of our discussion, the behavior of a supplicant may be described in a state machine-like fashion by means of the following variables whose names and values are self-explanatory:

- Connected: a boolean.
- TOD-Policy: an enumerated value in none, TOD-TOFU, TOD-STRICT.
- AS-name: either none or a name for an Authorization Server.

Initially, for a given SSID, a supplicant is disconnected and both TOD-Policy and AS-name are set to none. Rather than analyzing all possible transitions from the initial state, we analyze the three key scenarios separately: first, we analyze the supplicant behavior in a network with no TOD policy, then in a network with a TOD-TOFU policy, and finally in a network with a TOD-STRICT policy. Furthermore, in order to simplify the description, we consider only a subset of the possible state transitions and outline other possible evolutions later.

Supplicant evolution in a network with no TOD policy is represented in Figure 1. We use a graphical notation in which a state is represented by a box containing the values for variables TOD-Policy and AS-name; the value of variable Connected is represented implicitly, with either a dashed box (disconnected supplicant) or a continuous box (connected supplicant). State transitions are represented by arrows. The text close to each arrow summarizes the event that provoked the transition. Such an event may be either an execution of Phase 1, or a disconnection, or a change in the supplicant configuration executed by means of an out-of-band procedure. Upon the first connection attempt (transition "a"), the user decides whether to trust the certificate received from the AS and, if so, further connections with that AS will occur automatically (transition "b"; the value last-AS for variable AS indicates the name of the AS in the last accepted certificate). If the AS identity declared in Phase 1 changes, the user will be involved again (transition "c").

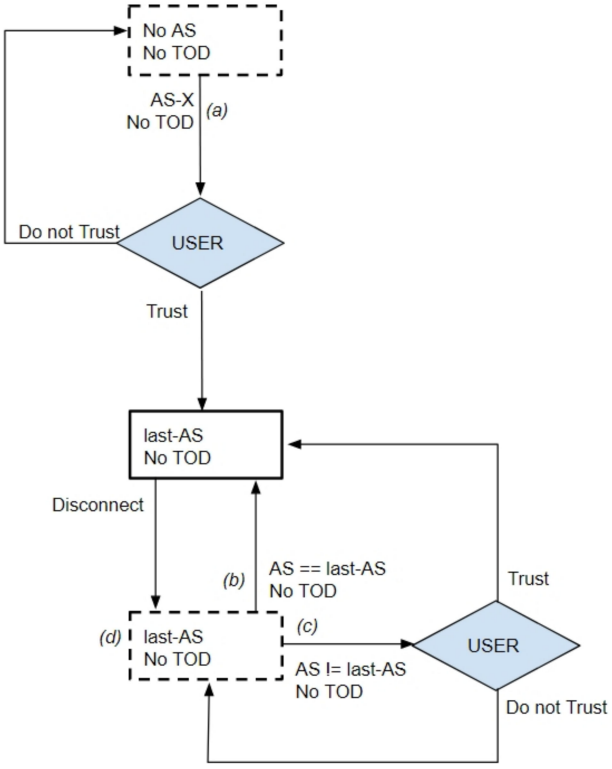

Figure 1. Supplicant evolution in a network with no TOD policy.

Supplicant evolution in a network with a TOD-TOFU policy is represented in Figure 2. In this case, the supplicant evolution is the same as in the previous case, with the important difference

that even if the AS identity declared in Phase 1 changes, the supplicant will stick to the AS identity learnt upon the first connection (transition "a"). While in this state, the only means for entering Phase 2 with a different AS requires changing the supplicant configuration with an out-of-band mechanism—e.g., by resetting the supplicant in its initial state. Such an event would correspond to a state transition not indicated in Figure 2.

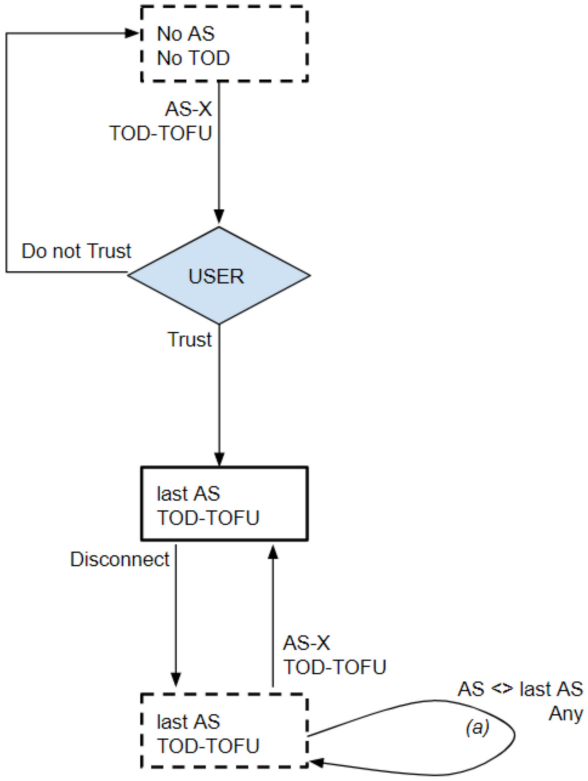

Figure 2. Supplicant evolution in a network with a TOD-TOFU policy.

Finally, evolution in a network with a TOD-STRICT policy is represented in Figure 3. In this case, the user is never involved and the supplicant will only connect to the AS whose identity has been configured out-of-band.

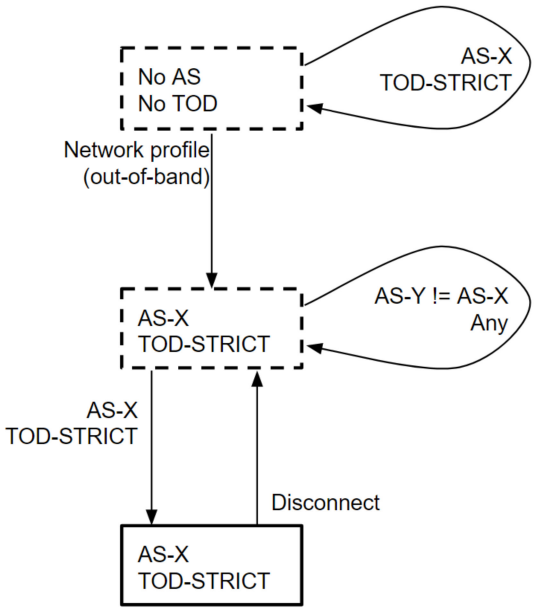

Figure 3. Supplicant evolution in a network with a TOD-STRICT policy.

In order to keep the presentation more focused, these diagrams illustrate only a subset of the supplicant evolutions allowed by the specification. Some of the evolutions not represented by the diagrams may result from the following facts.

- A supplicant could observe different values for the TOD-policy along its lifetime. For example, in Figure 1, when the supplicant is disconnected (state "d"), it could receive a certificate with a TOD policy set to either TOD-TOFU or TOD-STRICT and complete Phase 1 successfully. In these cases, the supplicant would update its variables accordingly, leading to states not shown in the figure. Similar considerations apply to Figure 2.
- The variables of a supplicant could be modified with out-of-band mechanisms. WPA3 Enterprise does not specify any requirements regarding how or when such modifications occur. For example, a supplicant could be reset in its initial state or its TOD policy could be modified, leading to states not shown.

An extremely important supplicant evolution not shown in the diagrams but allowed by the specification is that, in Figure 3, a supplicant in the initial state could change state even *without* installing the network profile required by the organization. For example, the supplicant could complete Phase 1 upon receiving a certificate with either TOD-TOFU or no TOD policy, leading to evolutions like those in Figures 1 and 2. In other words, even if an organization intended to prevent connections from supplicants that have not installed a network profile (i.e., enforce a TOD-STRICT policy), those supplicants could still connect to a fake AS if their user accepts trust in a certificate received before installing the network profile. The phenomenon of users that attempt to connect in a way that is not compliant with the security policy of the organization and thus is not eliminated by WPA3 Enterprise.

5. Discussion

Much of the improved security of WPA3 Enterprise over WPA2 is due to the impossibility of configuring a supplicant with "skip certificate validation" or "accept any certificate". In WPA2 Enterprise, the possession of a valid certificate may be sufficient to induce an incorrectly configured supplicant to enter Phase 2 automatically and without any user involvement, while this will no longer be possible with WPA3 Enterprise. The opportunities for tricking a supplicant into leaking

credential material to a fraudulent AS are thus greatly reduced by this relatively simple constraint on the allowed configurations.

It is important to point out that, actually, the WPA3 specification does not forbid those insecure configuration options clearly and explicitly. The specification requires that the identity of the server be verified in Phase 1 and that, if the verification fails, there must be a means for the user to possibly accept trust in the received certificate. On the other hand, the specification does not impose any temporal or causal relationships between a failed server identity verification and the decision of the user. In other words, a supplicant with a configuration option "accept any certificate" could collect the user intent once and for all, which would satisfy the literal meaning of the specification. The overall spirit of the specification, however, is such that the user intent should be collected explicitly whenever the server identity verification fails. In this work, we assume that the certification procedure for WPA3 supplicants, not publicly available at the time of this writing, will indeed guarantee that this is the case. Otherwise, much of the security improvements provided by WPA3 Enterprise could vanish.

WPA3 Enterprise provides several significantly different options and leaves important security-related decisions to network administrators (e.g., which TOD policy to apply, if any) and to users (e.g., whether to accept a certificate from the network and which ones). Leaving important security-sensitive decisions to people could lead, in practice, to decisions that are either short-sighted or not sufficiently informed, which may frequently result in a trade-off that is excessively biased toward lower costs, better functionality, and lower security. Indeed, it is fair to claim that the vast majority of security incidents today involve erroneous security-related choices made by users.

A crucial issue in this respect is that supplicants may still be allowed to connect without installing a network profile from a trusted out-of-band channel, and that in these cases it is up to the user to decide whether the information coming from the network is to be trusted. This is the root of the potential problems in server authentication. While WPA3 Enterprise has greatly reduced the attack opportunities in this respect, the root of the problem remains.

The WPA3 Enterprise specification includes a set of recommended warning messages to be presented to users. These messages are clear and informative, at least from the point of view of a technically savvy reader. On the other hand, it is difficult to assess whether they will be adequate for non-technically savvy users and, most importantly, what the behavior of those users when they need to connect will be. We are not aware of any specific study in this area, but studies on the behavior of users when faced with security-related browser warnings could provide interesting insights. In particular, it was recently ascertained that fostering adequate comprehension of warnings related to server identity over TLS is still a significant challenge, despite the many years of design iterations in this area [24].

Consider a user of an organization that has chosen to not enforce any TOD policy. Suppose the supplicant has not installed any network profile, as often occurs today. If the user actively attempts to connect while in range of an ET, the user will be presented with a warning (because the ET will present a certificate different from the one last used by the supplicant) and will have to take an important security-related decision. We will have to hope that users will take the correct decision—i.e., refuse to connect. This is almost identical to what happens today with WPA2 Enterprise (the only difference being that certain WPA2 Enterprise supplicants might connect automatically even without asking the user [10]).

This fact should be taken into account very carefully in roaming access services. The eduroam network, for example, allows the users of participating institutions (universities, research institutions, schools) to obtain Internet connectivity at any other participating institution by means of WPA2/WPA3 Enterprise technology. Essentially, eduroam provides a secure infrastructure for enabling supplicants to execute the authentication protocol with the AS of their home institution, irrespective of where they happen to be located [8]. The crucial point is that eduroam-enabled hot spots are available at tens of thousands of out of campus locations distributed across more than 100 countries: city centers, commercial malls, airports, railway stations, restaurants, touristic locations, and so on. Ensuring that an access point broadcasting the "eduroam" SSID is actually a legitimate access point is therefore

made very difficult exactly by the widespread diffusion of eduroam. Users with supplicants without a network profile installed and coming from organizations without any TOD policy, thus, will be required to take important security-related decisions whenever they need to connect and happen to be in range of an access point claiming to be eduroam. We believe that this fact may be critical. Similar considerations apply to govroam, a roaming access service for the public sector in the UK that is based on the same technology as eduroam and is available at more than 4000 hot-spots [25].

Based on the above considerations, roaming access services such as eduroam should leverage the policy tools at their disposal to enforce the adoption of a TOD policy by participating institutions. A normative enforcement of this kind is essential, because the default option (no TOD policy) does not require any change in the AS certificate management and is the one that requires minimum effort for administrators. The fact that many academic institutions promote supplicant configurations that are insecure but easier to describe and maintain is another important factor to consider in this respect [11].

The benefits of adopting a TOD policy are clear: they greatly reduce the opportunities for attacks aimed at impersonating AS. The corresponding costs, from the point of view of network administrators, are as follows:

- At deployment time, TOD-STRICT has a high cost: the organization must be prepared to support users that may not be able to install the correct network profile autonomously, or that do not even know what a network profile is. TOD-TOFU has a cost probably negligible: it is reasonable to expect that most users will be able to connect their supplicants autonomously, as they merely need to accept the received certificate explicitly. Of course, users must be warned that the first connection must be performed at a certainly safe location.
- When the AS certificate has to be renewed or revoked, TOD-STRICT has a negligible cost, as long as the network profile consists of the root certificate and the name of the AS. TOD-TOFU may instead have a significant cost, because all the supplicants that have accepted the previous AS certificate would be unable to connect to the enterprise network. The network configuration of *all* those supplicants would have to be reset or updated, which would only be possible with an out-of-band mechanism. Indeed, the management of key replacement in frameworks based on TOFU is an issue that is very difficult to address in a practical and scalable manner [19].

Certificate renewal may far away in the future, but such an event will have to be handled sooner or later. Furthermore, certificate revocation might become necessary almost unpredictably, either because of cryptographic advances or because of attacks that force an organization to reset its complete IT infrastructure.

These costs may be particularly significant for organizations with hundreds or thousands of users whose devices cannot be configured remotely and automatically by network administrators. Those organizations could thus find the default no TOD policy option even more attractive.

6. Conclusions

WPA3 Enterprise version 2 is certainly an improvement over WPA2 Enterprise, but the root of the server authentication problem remains: users may still be required to decide whether a claimed identity received from the network is to be trusted. The new mechanisms allow minimizing the potential exposure of users to those scenarios by providing network administrators with different security–cost trade-offs. The default option has minimal administrative cost but does not provide a strong defensive power, in particular for roaming users. The more secure options have a cost-benefit balance that could not facilitate their widespread, spontaneous adoption and should thus be accompanied by policy tools orthogonal to WPA3.

It seems fair to claim that a seemingly basic functionality such as connecting securely to an enterprise Wi-Fi network will still remain unavailable out-of-the-box for a long time. Careful device configuration, user education, and normative tools will still be required even after a full transition to WPA3 version 2. Furthermore, such a transition will be quite slow, as certification for this version

is optional at the time of this writing and WPA3 devices will have to coexist with WPA2 ones for a long time.

Funding: This research received no external funding.

Acknowledgments: The author is grateful to Eric Medvet and Andrea De Lorenzo for their useful comments on this work.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Wi-Fi Alliance, WPA3 Specification—Version 2.0. December 2019. Available online: https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v2.0.pdf (accessed on 5 November 2020).
2. Bartoli, A.; Medvet, E.; de Lorenzo, A.; Tarlao, F. Enterprise wi-fi: We need devices that are secure by default. *Commun. ACM* **2019**, *62*, 33–35. [CrossRef]
3. *Weaknesses in MS-CHAPv2 Authentication*. Microsoft Security Response Center: 20 August 2012. Available online: https://msrc-blog.microsoft.com/2012/08/20/weaknesses-in-ms-chapv2-authentication/ (accessed on 5 November 2020).
4. Brenza, S.; Pawlowski, A.; Pöpper, C. 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, 22 July 2015; pp. 14:1–14:11.
5. Cassola, A.; Robertson, W.; Kirda, E.; Noubir, G. A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication, in NDSS—Network and Distributed Security Symposium. 2013. Available online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.303.4335 (accessed on 3 April 2018).
6. Snoodgrass, H.; Hoover, J. BYO-Disaster and Why Corporate Wireless Security Still Sucks, in DEFCON 21. Available online: https://www.defcon.org/images/defcon-21/dc-21-presentations/djwishbone-PuNk1nPo0p/DEFCON-21-djwishbone-PuNk1nPo0p-BYO-Disaster-Updated.pdf (accessed on 5 November 2020).
7. Lanze, F.; Panchenko, A.; Ponce-Alcaide, I.; Engel, T. Undesired Relatives: Protection Mechanisms against the Evil Twin Attack in IEEE 802.11. In Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Montreal, QC, Canada, 21–22 September 2014; pp. 87–94.
8. Wierenga, K.; Winter, S.; Wolniewicz, T. The Eduroam Architecture for Network Roaming, RFC 7593. 2015. Available online: https://tools.ietf.org/html/rfc7593 (accessed on 5 November 2020).
9. Frankel, S.; Eydt, B.; Owens, L.; Scarfone, K. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, NIST, SP-800-97. February 2007. Available online: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-97.pdf (accessed on 5 November 2020).
10. Bartoli, A.; Medvet, E.; Onesti, F. Evil twins and WPA2 Enterprise: A coming security disaster? *Comput. Secur.* **2018**, *74*, 1–11. [CrossRef]
11. Bartoli, A.; Medvet, E.; de Lorenzo, A.; Tarlao, F. (In)Secure Configuration Practices of WPA2 Enterprise Supplicants. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018. [CrossRef]
12. *BYOD and Mobile Security Report*. Crowd Research Partners: 2016. Available online: https://crowdresearchpartners.com/portfolio/byod-mobile-security-report/ (accessed on 5 November 2020).
13. Yanson, K. Results of implementing WPA2-enterprise in educational institution. In Proceedings of the IEEE 10th International Conference on Application of Information and Communication Technologies, Baku, Azerbaijan, 12–14 October 2016.
14. Bassett, B.; Lund, D. 2016 Enterprise Mobility Survey Results: Strategic Imperatives. Available online: http://docplayer.net/52750420-2016-enterprise-mobility-survey-results-strategic-imperatives.html (accessed on 5 November 2020).
15. *Syntonic 2016 Employee: BYOD Habits and Attitudes*; Syntonic: Seattle, WA, USA, 2016.
16. Bonneau, J. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–23 May 2012; pp. 538–552. [CrossRef]

17. Wang, D.; Zhang, Z.; Wang, P.; Yan, J.; Huang, X. Targeted online password guessing: An underestimated threat. In Proceedings of the 2016 ACM SIGSAC conference on Computer and Communications Security, Vienna, Austria, 24–26 October 2016; pp. 1242–1254.
18. Ji, S.; Yang, S.; Hu, X.; Han, W.; Li, Z.; Beyah, R. Zero-Sum Password Cracking Game: A Large-Scale Empirical Study on the Crackability, Correlation, and Security of Passwords. *IEEE Trans. Dependable Secur. Comput.* **2017**, *14*, 550–564. [CrossRef]
19. Gonzales, H.; Bauer, K.; Lindqvist, J.; McCoy, D.; Sicker, D. Practical Defenses for Evil Twin Attacks in 802.11. In Proceedings of the IEEE Globecom Communications and Information Security Symposium, Miami, FL, USA, 6–10 December 2010.
20. Byrd, C.; Cross, T.; Takahashi, T. *Secure Open Wireless Networking*; Black Hat: Las Vegas, NV, USA, 2011.
21. Vanhoef, M.; Ronen, E. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1313–1328.
22. Vanhoef, M.; Ronen, E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. Available online: https://eprint.iacr.org/2019/383 (accessed on 5 November 2020).
23. Ylonen, T.; Lonvick, C. The Secure Shell (SSH) Authentication Protocol, RFC 4252. 2016. Available online: https://tools.ietf.org/html/rfc4252 (accessed on 5 November 2020).
24. Reeder, R.W.; Felt, A.P.; Consolvo, S.; Malkin, N.; Thompson, C.; Egelman, S. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems—CHI '18, Montreal, QC, Canada, 21–26 April 2018; pp. 1–13.
25. Govroam Service Definition, Jisc Services Ltd. May 2019. Available online: http://repository.jisc.ac.uk/6907/1/govroam-service-definition.pdf (accessed on 5 November 2020).