Enterprise Wi-Fi: we need devices that are secure by default

Alberto Bartoli, Eric Medvet, Andrea De Lorenzo, Fabiano Tarlao
University of Trieste, Italy

Abstract

Wireless networks have become an essential component of virtually every enterprise. The security technology for these networks (WPA2 Enterprise) has been designed for a world that is very different from today’s world. Basic assumptions for secure deployment of the technology are now violated systematically. As a result, Wi-Fi enabled personal devices are typically at risk of leaking single sign-on enterprise credentials everywhere and without any need of explicit action from their owners. It is necessary to emphasize this pervasive yet largely underestimated risk.

Introduction

Would you trust a security technology that makes it possible (i.e., quite likely) to steal the single sign-on enterprise credentials of any specific person in your enterprise by merely walking within 30 meters from that person? The attacker does not need to do any visible activity that might raise suspicions: a 50-euros device in a bag and a few seconds of physical proximity is all that is needed. Active cooperation of the target is not required and Internet connectivity is not required either. Thus, the attack may occur anywhere and the target would not notice anything. The attacker could steal the single sign on credentials of a large fraction of people of your enterprise that happen to pass within 30 meters from him. Perhaps at the canteen, or near the bus station, or anywhere outside of the enterprise.

Of course, you would not trust such a security technology. Interestingly, though, a technology of this kind is nearly ubiquitous and implicitly trusted by a lot of people and enterprises: it is WPA2 Enterprise, the suite of protocols for secure communication in enterprise wireless networks. It is necessary to emphasize the relevance of this important and pervasive yet largely underestimated risk. We need to raise the awareness on a fundamental security technology that is very often deployed by violating its requirements, which creates important risks to users.

Stealing enterprise credentials with evil twins

The attack scenario outlined above may succeed whenever people connect to enterprise wireless networks with devices that are not configured correctly. We recently showed in [1] that by just wandering around for a few hours in regions not covered by a wireless network we could have collected 200 enterprise credentials—roughly 25% of them in clear text and the remaining ones in hashed MS-CHAPv2 form, which can generally be decrypted easily [2]. We also showed that by remaining for a few seconds at less than 35 meters from a specific (voluntary) target whose Wi-Fi device is not configured correctly, there is a very good chance that you may steal his/her enterprise credentials; even when he/she is sitting in a car with closed windows.

The reason why these attacks work is quite simple. A Wi-Fi device (a supplicant in WPA2 Enterprise) may connect to an enterprise network only after executing an authentication protocol with the authentication server for that network. For the purpose of our discussion, this protocol may be summarized as follows: (i) the supplicant verifies the identity of the authorization server for the network it is attempting to connect to; (ii) the supplicant sends user credentials material to the
authorization server; (iii) the authorization server demonstrates knowledge of the user credentials to the supplicant. Execution of the first step relies on certain configuration information that must be stored on the supplicant before connecting. Such information includes the association between the name of the network and the name of the authorization server (e.g., in our university these are eduroam and raggio.units.it, respectively); it also includes the association between the name of the authorization server and a certified public key for that server.

Satisfying this configuration requirement is extremely important, because supplicants that are not configured correctly will execute the first step with any fraudulent wi-fi access point broadcasting the name of an enterprise network (evil twin) [2–5]. The authentication protocol will fail because the evil twin will not be able to prove knowledge of the user credentials. However, the supplicant will disconnect when it is too late, i.e., after having already sent credential material to the evil twin. The entire procedure takes just a few seconds and, most importantly, it does not require any engagement from the user, in particular when the user carries a smartphone with the Wi-Fi interface active.

Enterprise Wi-Fi today

Enterprise credential stealing through evil twins is not based on any vulnerability of WPA2 Enterprise: it is an obvious consequence of using this technology without satisfying one of its fundamental deployment requirements, that is, correct supplicant configuration [6]. The problem is, supplicants that connect to enterprise networks without being configured correctly are pervasive. All the analyses that we are aware of corroborate this claim unequivocally [7] and even network configuration guides prepared by organizations suggest insecure configuration practices very often [7]. Attacks based on an evil twin have thus a high probability of success.

What makes this risk important and pervasive is that WPA2 Enterprise was specified in 2004 but the world today is very different:

1. Virtually all enterprises have migrated to single sign-on architectures. Enterprise network credentials now usually unlock access to all enterprise services, including in particular all the services with a web interface. Network credentials are thus much more attractive and valuable to attackers than they used to be.
2. Everyone is now permanently carrying a Wi-Fi-enabled smartphone which often contains the user’s enterprise credentials and connect to Wi-Fi networks automatically. An evil twin may now be assembled with a few tens of euros and can be placed in a bag [1]. Attacks aimed at stealing network credentials may thus occur potentially anywhere and are virtually impossible to detect: they are executed automatically, in less than a second of proximity to an evil twin and without any need of involving the device owner in a working session.

One of the reasons for the prevalence of incorrectly configured supplicants is because defining an insecure configuration is much simpler and quicker than defining a secure one. A secure configuration requires the presence of certain configuration data on the supplicant, which must be preliminarily obtained through a connection link different from the enterprise network. Insecure configurations are much more straightforward to define as they do not require any prior connection and download: select the name of the enterprise network, insert enterprise credentials and then play with the network configuration until connecting, the most typical (insecure) options being “skip certificate validation” or “accept any certificate”. Users are not to blame for this behavior, as they cannot appreciate the resulting risks. Most importantly, they have no incentive in selecting a more cumbersome path toward their objective: connecting their device to the network [8].

One could require enterprises to deploy forms of “entrapments” for detecting supplicants that are not configured correctly and then notifying the corresponding users to contact the IT staff. On the other hand, it is a fact that many organizations not only tolerate but also suggest insecure configuration
practices [7], hence assuming the occurrence on a large scale of a spontaneous change that increases the technical and operational burden of IT staff seems to be excessively optimistic. Indeed, procedures of this kind may be implemented already but it is fair to say that they are actually deployed quite rarely.

Secure by default

We call on the technical community to disseminate the awareness that we are systematically deploying a widespread security technology by violating its key requirements, thereby creating important risks to users and organizations. WPA2 Enterprise devices will not disappear anytime soon, thus we must all be aware that we will have to cope with the pervasive risks of enterprise Wi-Fi for many years to come.

We also need to devise a transition plan that, in our opinion, necessarily requires a novel design for supplicants. The root cause of the problem is that users invariably attempt to connect their supplicants by providing only the name of the enterprise network, that is, without preliminarily obtaining the additional information required for a secure configuration. Consequently, we advocate a design that makes it impossible for those supplicants to connect. We believe this is the only realistic strategy for providing both users and enterprises with adequate incentives for installing the required information on supplicants.

Obviously, supplicant configuration should be sufficiently simple to make the new framework acceptable in practice and the likelihood of ending up in insecure configurations should be minimized. These generic recommendations can be made more useful and concrete based on secure by default design principles [9]: configuration should not require specific technical understanding and it should require only the insertion of a few short pieces of textual information (to prevent the need of non-obvious actions from the user such as downloading and installing a program or binary data with a device not yet connected to the network). Although these design principles do not prevent the possibility of insecure configurations, they are sufficiently specific to be actionable.

We have proposed a design based on this framework [1] but we believe that any secure by default approach needs strong incentives that cannot be purely technical [8]. Manufacturers are unlikely to place on the market supplicants whose configuration involves a user experience quite different from the established one. Support from a standards body in the form of certification requirements for supplicants could constitute a strong and probably decisive incentive for adopting a secure by default approach in the context of enterprise Wi-Fi.

There is an important opportunity in this respect, because the Wi-Fi Alliance has announced that new security protections will be specified soon as part of the new family of WPA3 protocols [10]. It is unclear whether the issue of supplicant configuration in enterprise Wi-Fi will be addressed and how: the limited information that is currently available is not very encouraging, as the focus is on new cryptographic protections but crucial issues of supplicant configuration are not mentioned at all [10]. It would be unfortunate if the new standard did not remove security assumptions that have proven to be unrealistic, as the society as a whole would have to cope with the resulting risks without any transition plan on the horizon. We can no longer afford devices that are secure only if configured correctly, but that may be used insecurely anyway and are typically used so.

References


