

# Roaming, Accounting and Seamless Handover in EAP-TLS Authenticated Networks

Carolin Latze and Ulrich Ultes-Nitsche

University of Fribourg, DIUF

Fribourg, Switzerland

E-Mail: {carolin.latze | uun}@unifr.ch

**Abstract:** The emergence of mobile phones with integrated 802.11 chipsets lead to the idea of replacing GSM calls with VOIP calls. Mutual authentication using EAP-TLS based protocols allows to automatically authenticate embedded devices at public wireless hotspots, which is one of the prerequisites in order to have a comfortable GSM-like 802.11 based setup. This work proposes a possible accounting and roaming scheme and discusses seamless handovers in EAP-TLS authenticated networks. It shows that EAP-TLS authenticated VOIP setups provide even more comfort for the user than GSM networks since there is the possibility to have one identity for every different operator that controls the hotspots.

## 1. INTRODUCTION

The emergence and propagation of public 802.11 hotspots lead also to the emergence and propagation of WLAN enabled embedded devices like mobile phones. This development lead to the idea of replacing the Global System for Mobile Communications (GSM) calls with Voice over IP (VOIP) calls, but until today VOIP over public wireless hotspots does not really work for several reasons.

The first reason is that the first 802.11 standard that has been released in 1997 did not contain any authentication methods; it mainly covered data transmission aspects [1]. Therefore, many different authentication methods emerged, that are not really compatible to each other with many of them not being really secure. Many public hotspots use captive portals for authentication, which are not very secure since they are based on probably weak user passwords. Furthermore, as all the users have to be managed in a central database, they do not scale very well and are uncomfortable as all the users have to be known in advance. Besides deploying captive portals, some providers of public hotspots also deployed Extensible Authentication Protocol (EAP) based authentication methods, which have been specified in the 802.11i standard [2]. EAP-TLS [3] is one of the most secure EAP based authentication methods when used in mutual authentication mode, but it is rather uncomfortable for naïve users as it requires X.509 certificates also on the client side. Requesting a X.509 certificate is not easy for inexperienced users. Therefore, several EAP-TLS based authentication methods arose that tried to reduce the complexity on the user's side without neglecting the mutual authentication. Examples are EAP-TTLS [4], PEAP [5] and EAP-SIM [6]. The most secure versions rely on hardware

tokens like EAP-SIM. This protocol, which is based on the SIM card, is a very promising authentication protocol used at public wireless hotspots at least in Switzerland. But beside problems like supporting only single sessions, one disadvantage of EAP-SIM is that it uses the Subscriber Identity Module (SIM) for authentication, which means, that every device that wants to connect to an EAP-SIM secured hotspot has to be equipped with a SIM card, which makes it rather uncomfortable. The other EAP-TLS based protocols rely either on a simple password or a smart card. The latter method is uncomfortable, the first unsecure. In 2007, the authors of this work proposed to use the trusted platform module (TPM) within EAP-TLS in order to provide the user a comfortable and secure way to support mutual authentication [7]. Concluding, one may say that approaches like EAP-SIM and EAP-TLS with TPM support enable a secure, more or less comfortable and automated login procedure, which is the first step on the way of making VOIP over WLAN as comfortable as GSM.

Besides having a suitable authentication method, GSM also covers aspects like accounting, roaming and seamless handovers, which will be discussed in this paper. The discussion is based on the fact, that public wireless hotspots are also controlled by different operators. Of course, there are projects to allow free WLAN access everywhere like FON [8], but those will only cover certain regions.

Roaming and Accounting are only important for network and customer management, whereas seamless handovers are a technical issue.

The next sections described EAP-TLS based authentication protocols more detailed, followed by a discussion of accounting and roaming issues. Afterwards a discussion of seamless handover concepts is given, followed by a conclusion.

## 2. EAP-TLS BASED AUTHENTICAIION

As mentioned above, EAP-TLS based authentication protocols are the most secure 802.1X authentication methods if used mutually. The basic EAP-TLS [3] represents the integration of the transport layer security (TLS) protocol within EAP. EAP-TLS may be used only with server authentication or mutually. In the mutual authentication setup, both sides need X.509 certificates, which means that every user has to request its own X.509 certificates for instance at VeriSign [9]. Everybody who ever requested its

own certificate knows, that this is a rather complicated process including the identity proof using the requester's ID card. That is one reason, why EAP-TLS is not really used at public wireless hotspots and it is a very hard constraint. In order to make the user's life easier, several EAP-TLS based protocols have been introduced. In this work, we will concentrate on two of them: EAP-SIM and EAP-TLS with TPM support.

## 2.1 EAP-SIM

EAP-SIM [6] is based on the idea to use EAP-TLS to authenticate the server and establish an EAP-TLS secured tunnel within which user authentication takes place. As the user authentication should not use X.509 certificates and as passwords are usually unsecure, there arose the idea of using hardware tokens on the user's side. The SIM card is a hardware token that many users possess anyway, so it is quite obvious to use it also for authentication in non-GSM networks. In EAP-SIM, the user will be authenticated using its identity stored in the SIM card.

The main drawback of this approach is that the SIM card has never been build for computer networks. It has been designed for telecommunication networks, which have other needs than computer networks. One problem is for instance that the SIM card only supports single session, which means that a user cannot authenticate itself against an 802.11 hotspot and call somebody at the same time. Another problem is that GSM modules are much more expensive than wireless chipsets and they need much more power which is not desired in a mobile environment.

However, EAP-SIM is used for authentication purposes at public wireless hotspots at least in Switzerland.

## 2.2 EAP-TLS with TPM support

In 2007, the authors of this work proposed to use the trusted platform module (TPM) within EAP-TLS instead of using other hardware tokens [7]. Many modern computers and in the future also many embedded mobile devices are equipped with the new TPMs, which provide cryptographic functions and secure storage for keys and hashes. TPMs are able to request more than one identity automatically without much work on the user's side. The only thing, the user has to do is to confirm the identity request. When authenticating against a public wireless hotspot, the user has to select the identity he wants to use (from a CA, the hotspot's provider accepts), which makes him untraceable in case he uses different identities for different providers.

In 2008, the authors presented a very promising proof-of-concept implementation of the approach [10], which leads to the hope, that EAP-TLS with TPM support will be used frequently in the future.

## 3. ACCOUNTING AND ROAMING

As public wireless hotspots are usually controlled by an operator and not by private persons that allow free access, there is the strong need to think about accounting. Therefore, a link between an authenticated device and the owner is needed, which will be described in section 3.1. It is clear that there will be different operators that control different access points. In order for the user to provide connectivity everywhere – which means at every reachable access point – there has to be a roaming concept in order to provide a seamless experience for the user. Roaming considerations for EAP-TLS with TPM support are presented in section 3.2.

### 3.1 Accounting

Accounting in 802.11 based networks is most probably based on the time interval that a user is connected to a hotspot or on the data load he produces. But in order to charge somebody the costs, there has to be a mapping between the authenticated identity and a real person. In countries like Switzerland or Germany this is already solved for EAP-SIM. If somebody wants to buy a SIM card, he has to register himself at the operator that issues that card. Things are a bit different for EAP-TLS with TPM support.

In TPM supported EAP-TLS, the identities are requested at a special certificate authority (CA) - called privacy CA (PCA). This may be done before connecting to an EAP-TLS secured hotspot at any PCA the user likes (risking that the operator that manages the hotspot does not accept it) or during authentication as described in [11]. As described above, the TPM requests the identities itself, so there is no mapping between user and identity. A way to solve this problem is to register the user in a shop. He may either request a new identity in a shop (on a designated hotspot) or register an already requested identity later. If accounting is needed, such a registering has to take place even if it is a bit uncomfortable.

### 3.2 Roaming

Roaming describes the process of authenticating an user with an identity registered at operator A at a public wireless hotspot under the control of operator B. Roaming is only needed for accounting.

For EAP-SIM, roaming is handled as in every GSM network. As long as there are roaming contracts between operator A and B, the user may use both networks. If there is not any contract, the user has to buy a new SIM card.

EAP-TLS with TPM support is a bit more comfortable for roaming as it supports different identities. When an user uses TPM identities, he may request one identity for every network. That may be done in advance or on-the-fly as described in [11]. For the registration at the first operator, the user requests a certificate like described above. Later on, the

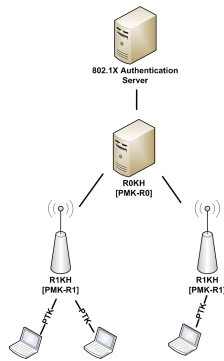


Figure 1 - Key Hierarchy in 802.11r

user may register easier online as he already has an identity that is mapped to a real person. In order to do so, the user may connect to a certain portal using the first identity and register a second identity as belonging to the same person. Using different identities for different operators may be cheaper than using always the same identity in roaming mode. Furthermore, if two operators have no contract, the user may request a new identity on-the-fly but has to register it as described in section 3.1.

#### 4. SEAMLESS HANDOVERS

After having discussed some management related problems, we will discuss now some technical problems. This section describes handover techniques for EAP secured networks.

Basically, the following actions have to be done:

- 1) Discovery of new access point.
- 2) Initiating EAP authentication.
- 3) Re-association with new access point.
- 4) Processing of authentication method.
- 5) EAPOL key exchange.

In the end, there might be a QoS renegotiation, but that is optional.

In general, there are network and mobile controlled handovers as well as network and mobile initiated handovers. This work concentrates on mobile controlled and initiated handovers.

The following subsections describe the detailed process for soft and hard handovers.

##### 4.1 Soft Handovers

Soft handover means that for a certain time a station may be connected somehow to more than base station. This means either directly through different network cards or indirectly. The latter one is also called semi-soft handover and describes a setup, where a station is associated with one access point and contacts a second one through the backbone. Soft handovers are usually smooth – which means they have

minimal packet loss – and fast – they produce minimal delay. Soft handovers are seamless. 802.11r is a new IEEE standard, which is still under development that describes semi-soft handovers for EAP secured networks [12].

The basic idea of 802.11r is to create a sharing scheme for the set of pair wise master keys (PMK), negotiated by an authentication server and a mobile station during EAP authentication. In 802.11r a mobile station has to go through the complete EAP authentication only for the first connect to an 802.11r enabled network. Later on, the authentication relies on the keys derived in that first authentication process.

Figure 1 shows the key hierarchy used in 802.11r. It represents the network of one operator in our case (such a scheme may also apply to subdomains of an operator's network). The entity on top of that scheme is the 802.1X authentication server handling all the authentication requests that come from an access point at level R1. Beneath the authentication server resides the R0 Key Holder (ROKH) holding the PMK-R0. Furthermore, ROKH is able to derive PMK-R1 out of its PMK-R0 and some other parameters like its address to bind the key to itself. The access points within that domain are called R1 Key Holder (R1-KH) and hold the PMK-R1. R1 Key Holders are able to derive the pair wise temporary keys (PTKs), which are the lowest level keys used between mobile station and R1KH. Keys are distributed in a top-down manner.

If a mobile station connects to such a network, for instance to an access point A, it uses the PTK generated out of PMK-R1<sub>A</sub> in order to associate with A. The ROKH does then distribute the PMK-R1 to every R1KH under its control. In case the mobile station starts moving, the access points are ready to authenticate the client faster, as they already know PMK-R1.

A domain shown in Figure 1 is defined as security domain (SD), which means there are one ROKH and several R1KH beneath it. Obviously, the possibility to roam only within one SD is not very useful. There is another concept called security mobility domain (SMD), which describes a set of SDs, where each R1KH may obtain PMK-R1 from every ROKH of the set. To put it short, a SMD describes a collection of domain within a mobile station may roam using 802.11r and which therefore supports seamless handovers.

In 2006, the authors of [13] did a performance analysis of the new and not yet released 802.11r standard. They have shown that 802.11r roaming produces delays less than 60ms, which is very promising for VOIP applications.

For our purposes, EAP-SIM and EAP-TLS with TPM support work directly within 802.11r. So, the problem of seamless handovers is already solved for both.

##### 4.2 Hard Handovers

Hard handovers are handovers, where a host has to disassociate from the old access point and associate to a new one afterwards. Figure 2 shows the time needed to

authenticate a mobile node using EAP-TLS with TPM support as example. It takes around seven seconds, which is quite long. That is why it is useful to make use of soft handovers whenever it is possible, especially if one has an active VOIP session. Seven seconds is far too long for VOIP. The results for EAP-SIM would be quite similar.

However, there are setups, when hard handovers are useful. First of all, they are needed, in case the mobile station moves to a network, which is not part of its former SMD. Furthermore, for EAP-TLS with TPM support, there is another use case for hard handovers. As mentioned above, working with TPM identities allows having different identities for different purposes. When thinking of operator controlled public wireless hotspots, this means, that a user may obtain an identity for every different operator. Of course, this means he has to register at every operator, but as mentioned in section 3.2 the user may save money during roaming. The authors of this work propose to use the following algorithm for handovers:

If a mobile station moves from a network controlled by operator A to a network controlled by operator B without having any open VOIP sessions, he changes his identity, which means, he does a hard handover. Either he has already an identity for operator B or he has to obtain a new one as described in [11]. If a mobile station moves from a network controlled by operator A to a network controlled by operator B while having an open VOIP session, hard handovers are not suitable. Therefore, in order not to lose the VOIP session, soft handover takes place. As soon as the VOIP session will be finished, the device will do a hard handover.

Hard handovers as described above are only useful for EAP-TLS with TPM support, as this authentication protocol supports different identities for the same person. EAP-SIM does only support one identity, so hard handovers are only used when roaming to a network that does not support 802.11r.

## 5. CONCLUSION

The presented work discussed aspects like accounting, roaming and seamless handovers in EAP-TLS authenticated networks. Accounting and roaming are more important from a manager's view on the network, whereas seamless handovers are a technical problem. The work has shown that seamless handovers are needed for VOIP but may be omitted for EAP authentication protocols providing more than one identity for the same user. Hard handovers provide more comfort for the user as they may save money, but cannot be used during open VOIP sessions.

The presented work also shows another advantage of TPM based EAP-TLS authentication compared to EAP-SIM. Besides the technical problems discussed in [7] like single session and the high energy requirements, EAP-SIM does only support one identity for each user. If he needs more than one, he has to buy a new SIM card, whereas the TPM itself is

able to request and store more than one identity (limited only by its memory). Having more than one identity allows combining soft and hard handovers in a clever way in order to save the user's money.

This work only discusses horizontal handovers, that means from one 802.11 cell to another one. Obviously, it might

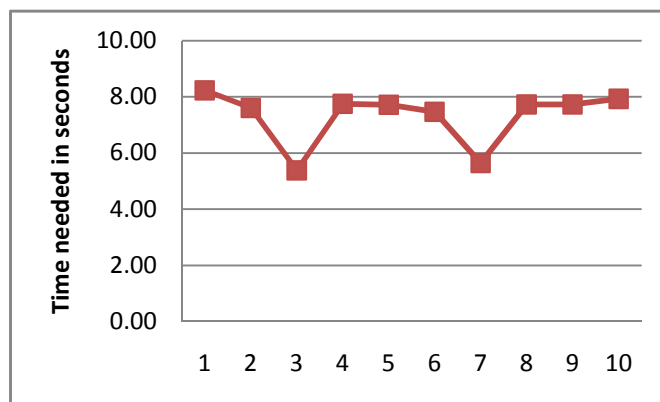


Figure 2 - Time Needed to Authenticate a Mobile Station Using EAP-TLS with TPM Support

happen that a user moves to an area with no 802.11 coverage at all. The standard that covers this so called vertical handover is called 802.21 [14]. Vertical handovers usually take place between 802.11 and GSM or 3G networks like UMTS and EDGE. In such a scenario, where the user is expected to do also vertical handovers, using EAP-SIM might be an advantage since that means, that the user has already a SIM card. Devices, that support only EAP-TLS with TPM support do not necessarily have a SIM card.

## REFERENCES

- [1] "IEEE 802.11 - The Working Group Setting the Standards for Wireless LANs", [Last Accessed] May 2008, [Online] <http://grouper.ieee.org/groups/802/11>
- [2] "IEEE 802.11i", [Last Accessed] May 2008, [Online] [http://www.ieee802.org/11/Report/tgi\\_update.htm](http://www.ieee802.org/11/Report/tgi_update.htm)
- [3] Dan Simon, Bernhard Aboba: "PPP EAP TLS Authentication Protocol", RFC 2716, 1999
- [4] Paul Funk, Simon Blake-Wilson: "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", Internet Draft, 2004
- [5] Ashwin Palekar, Dan Simon, Glen Zorn, Joseph Salowey, Hao Zhou, Simon Josefsson: "Protected EAP Protocol (PEAP) Version 2", Internet Draft, 2003

[6] Henry Haverinen, Joseph Salowey: "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, 2006

[7] Carolin Latze, Ulrich Ultes-Nitsche, Florian Baumgartner: "Strong Mutual Authentication in a User-Friendly Way in EAP-TLS", 15th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2007), Split - Dubrovnik, Croatia, September 2007

[8] "FON - Movimiento", [Last Accessed] May 2008, [Online] <http://www.fon.com>

[9] "Verisign Security", [Last Accessed] May 2008, [Online] <http://www.verisign.com>

[10] Carolin Latze, Ulrich Ultes-Nitsche: "A Proof-of-Concept Implementation of EAP-TLS with TPM support", 7th Annual ISSA Conference (ISSA 2008), Johannesburg, South-Africa, 2008

[11] Carolin Latze, Ulrich Ultes-Nitsche, Florian Baumgartner: "Towards a Zero Configuration Authentication Scheme for 802.11 Based Networks", 33rd IEEE Conference on Local Computer Networks (LCN 2008), Montreal, Canada, 2008

[12] "IEEE 802.11r", [Last Accessed] May 2008, [Online] [http://grouper.ieee.org/groups/802/11/Reports/tgr\\_update.htm](http://grouper.ieee.org/groups/802/11/Reports/tgr_update.htm)

[13] Sangeetha Bangolae, Carol Bell, Emily Qi: "Performance Study of Fast BSS Transition Using IEEE 802.11r", International Conference On Communications And Mobile Computing, Proceedings of the 2006 International Conference in Wireless Communications and Mobile Computing, New York, USA, 2006

[14] "IEEE 802.21", [Last Accessed] May 2008, [Online] <http://www.ieee802.org/21>