EAP-TPM: A New Authentication Protocol for IEEE 802.11 Based Network

Carolin Latze
University of Fribourg
Department of Informatics
Bd. de Prolles 90
1700 Fribourg
Switzerland
Email: carolin.latze@unifr.ch

Ulrich Ultes-Nitsche
University of Fribourg
Department of Informatics
Bd. de Prolles 90
1700 Fribourg
Switzerland
Email: uun@unifr.ch

Josua Hiller
Swisscom Schweiz AG
Waldeggstrasse 51
3097 Liebefeld
Switzerland
Email: josua.hiller@swisscom.com

***Abstract*—Nowadays authentication at public wireless hotspots is still not very comfortable for normal users. Most of the hotspots provide a captive portal asking the user for credentials or his phone number to send him an one-time password (OTP). This is uncomfortable especially on embedded devices like mobile phones due to the small screen. Therefore the PWLAN hotspots of Swisscom provide another more comfortable authentication method called EAP-SIM, which allows for an automated hotspot login using SIM credentials. This requires a SIM slot in the users notebook and an additional data SIM card, which again renders it uncomfortable for the users and restricts its usage to devices with SIM slots. EAP-TPM instead makes use of the Trusted Platform Modules (TPMs) shipped with almost every new computer (and also with mobile phones from 2010 on). Peers in EAP-TPM are authenticated using the TPM identities that can be obtained much more easier than X.509 certificates in EAP-TLS. Therefore, EAP-TPM is a promising protocol for future PWLAN authentication on notebooks and embedded devices like mobile phones and mobile game consoles. The demonstrator shows the first real world implementation of EAP-TPM, its potential and how easy EAP-TPM can be integrated into the existing PWLAN infrastructure. Furthermore, we will demonstrate the identity retrieval and the login process.**

I. Introduction

EAP-TPM [1] is a new authentication protocol for wireless LANs. It has been first published in 2007 [2] as extension to EAP-TLS and was later extended with an auto-provisioning feature [3]. The authors of [2] identified EAP-TLS [4] as one of the most secure authentication schemes when used in mutual mode. But the requirement for X.509 client certificates makes EAP-TLS very uncomfortable and therefore unusable in the real world. Trusted Platform Modules (TPMs) as specified in [5] provide so called TPM identities that can be obtained automatically and have been identified as suitable for network identification [6]. EAP-TPM is based on EAP-TLS which makes it a very secure authentication protocol. Furthermore the possibility to request new identities automatically makes it a very user-friendly protocol. As the TPM will be an ubiquitous device in the near future, users do not need to extend their hardware anymore if they want to have a comfortable PWLAN login (for instance with PCMCIA SIM adapters as it is the case with EAP-SIM). The auto-provisioning scheme proposed in [3] even allows users to connect to new networks in an ad-hoc manner without obtaining an identity before.

II. Common PWLAN Authentication Methods

Nowadays, there is mainly one authentication method used in public wireless LANs, which is the captive portal. Captive portals use the web-browser as authentication device and block every traffic until the user connects to the portal giving his credentials. This can be either a username and a password or a mobile phone number which will be used to send the user an one-time password using SMS. As captive portals are usually also used for advertisements they are quite huge and cannot be accessed and filled out in an automated manner. Furthermore, they are usually not very comfortable on small screens of embedded devices like mobile phones.

Sometimes there is also the possibility to use a VPN client as authentication device. If an organization is able to place its VPN concentrator with the public wireless LANs open garden, members of that organization can directly connect to the organization via VPN. SWITCH in Switzerland provides such an access for students of Swiss universities [7].

The last authentication method for public wireless LANs (PWLANs) at least in Switzerland is EAP-SIM [8]. In order to connect to a hotspot using EAP-SIM, the user has to have a data SIM and a SIM slot equipped mobile device. Especially the latter constraint often leads to problems and users usually end up in using PCMCIA cards with SIM slots.

III. EAP-TPM

In 2001, the Trusted Computing Group (TCG) released the first specification for the so called Trusted Platform Modules (TPMs), which has been updated in 2006 [5]. The TPM is a module that provides secure storage for hashes and keys and some cryptographic functions. Furthermore it is possible to request so called TPM identities that are tamper resistant since they cannot leave the TPM. Those identities are basically X.509 certificates restricted to SHA-1 signing and without the possibility to create child certificates. IEEE 802.1AR defines those identities as suitable for peer authentication in networks

[6]. The basic idea of EAP-TPM is to use those certificates for peer authentication in wireless LANs.

EAP-TPM is based on EAP-TLS using mutual authentication, but as only TLS 1.2 makes use of standard signatures during the handshake, it is only possible to directly use the identity certificates in EAP-TPM using TLS 1.2 or higher. If TLS prior to 1.2 is used, EAP-TPM makes use of the supplemental data extension for TLS [9]. For the TLS handshake itself a so called certified key will be generated using the identity certificate. Afterward, a self-signed certificate has to be created using the certified key, which will serve as client certificate. In order for the authentication server to be able to verify that the client uses a valid identity certificate, the identity certificate has to be sent within the supplemental data extension.

EAP-TPM as described above requires the user to request an identity certificate before connecting to the EAP-TPM secured network. Although that is a valid requirement for operator controlled setups there may be cases where it is sufficient if the user gets that certificate during his first connect. EAP-TPM provides an auto-provisioning feature which allows the user to request his identity certificate during the authentication process itself [3]. This feature is possible since the TPM can automatically and securely request a new identity.

IV. Proposed Demo

In 2009, Swisscom gave the authors the possibilities to implement the first real-world reference prototype of EAP-TPM within Swisscom's PWLAN testbed. The prototype makes use of FreeRADIUS [10] as back-end authentication server, which has been integrated into the PWLAN infrastructure. On the client side, wpa_supplicant [11] has been used as peer. Furthermore, GnuTLS [12] has been used as SSL Library, since the most popular library (OpenSSL [13]) does not provide TLS 1.2 support yet. wpa_supplicant already comes with GnuTLS support, FreeRADIUS does not. Therefore one of the challenges of the prototype was to implement an EAP-TLS module for FreeRADIUS that makes use of the GnuTLS library. Additionally, GnuTLS did not support the TPM out of the box, which has been implemented too.

The demonstrator to be shown will show the process of obtaining a new identity in order to underline its comfort even for inexperienced users. Furthermore it will show the complete authentication in detail and outline how easy it is to deploy EAP-TPM within an existing PWLAN infrastructure. In order to demonstrate those features, one or two notebooks are needed, where one represents the peer and the other one the certificate authority releasing the identity certificates. Furthermore an access point is needed that has a VPN connection to the PWLAN authentication backend where the FreeRADIUS is running. Using this setup it is possible to show a client connecting to Swisscom's PWLAN using EAP-TPM.

Concluding, the following components are needed to show the demo proposed above:

- 1 - 2 Notebooks [the authors]
- 1 Access Point [the authors]
- 1 Desk [LCN organization comittee]
- 3 Power Plug [LCN organization comittee]
- Internet access that allows for VPN tunnels

The time needed to setup the demo is not more than one hour.

References

[1] C. Latze, U. Ultes-Nitsche, F. Baumgartner, *Extensible Authentication Protocol Method for Trusted Computing Groups (TCG) Trusted Platform Modules*, Work in Progress, 2009, http://tools.ietf.org/html/draft-latze-emu-eap-tpm-00

[2] C.Latze, U.Ultes-Nische, F.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

[3] C.Latze, U.Ultes-Nitsche, F.Baumgartner, *Towards a Zero Configuration Authentication Scheme for 802.11 Based Networks*, IEEE Conference on Local Computer Networks (LCN 2008), Montreal, Canada, October 2008

[4] D. Simon, B. Aboba, R. Hurst, *The EAP-TLS Authentication Protocol*, RFC 5216, 2008, http://tools.ietf.org/html/rfc5216

[5] Trusted Computing Group, *TPM Specification Version 1.2 Revision 103: Part 1 3*, 2006, http://www.trustedcomputinggroup.org/resources/-tpm_specification_version_12_revision_103_part_1__3

[6] *Secure Device Identity*, IEEE 802.1AR Draft 2.1, 2009, http://www.ieee802.org/1/pages/802.1ar.html

[7] *SWITCH PWLAN*, http://www.switch.ch/mobile/pwlan/

[8] H. Haverinen, J. Salowey, *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*, RFC 4186, 2006, http://tools.ietf.org/html/rfc4186

[9] S. Santesson, *TLS Handshake Message for Supplemental Data*, RFC 4680, 2006, http://tools.ietf.org/html/rfc4680

[10] *freeradius - the world's most popular RADIUS server*, http://freeradius.org/

[11] *Linux WPA/WPA2/IEEE 802.1X Supplicant*, http://hostap.epitest.fi/wpa_supplicant/

[12] *GnuTLS*, http://www.gnutls.org

[13] *OpenSSL*, http://www.openssl.org