

EAP-TPM

A New Authentication Method for 802.11 Based Networks

Carolin Latze

University of Fribourg, Switzerland

ITG-FG-522 Fachgruppentreffen

June 19th, 2009, Heidelberg, Germany

Table of Contents

■ Motivation

- ^ Common WLAN Authentication Methods and Their Problems
 - Captive Portals, EAP-TLS, EAP-SIM

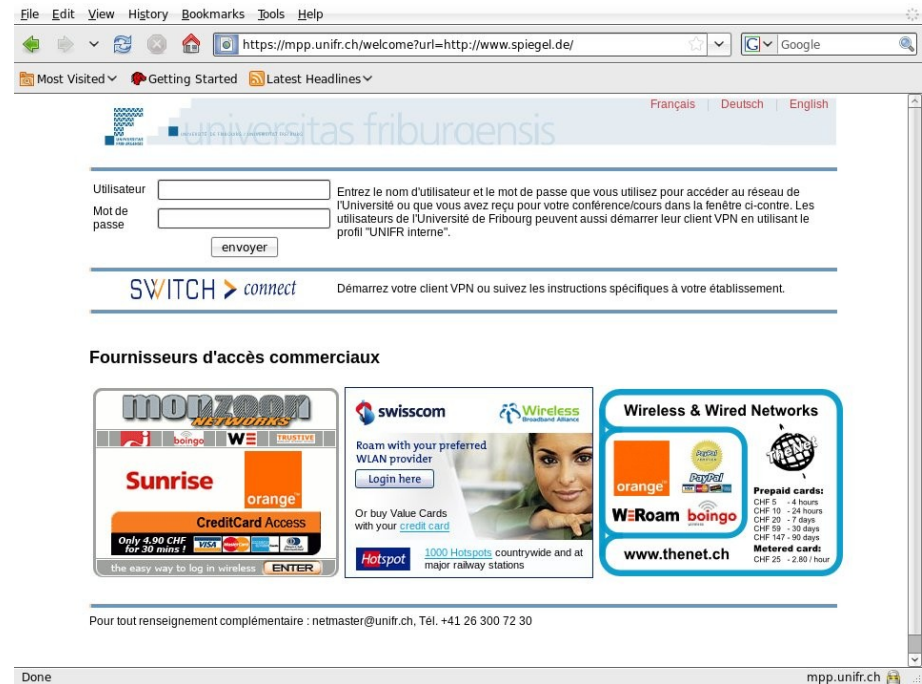
■ Trusted Computing, TPM

■ EAP-TPM

- ^ Theory
- ^ Prototyping
- ^ Standardization
- ^ Real World Reference Setup

Common WLAN Authentication Methods: Captive Portals

- Browser = Authentication Device
- Usually full browser needed
- DNS tunneling attacks easily circumvent authentication



Common WLAN Authentication Methods: EAP-TLS

- Not really commonly used, but one of the best regarding security
- Supports mutual authentication
- BUT: requires the client to request his own X.509 certificate

Certificate request for HSM and SSL Server Certificates

On this page an electronic certificate request can be submitted after a registration was made by a RA.

Company:	<input type="text"/>	Function:	<input type="text" value="No data"/>
Title: *	<input type="radio"/> Mrs <input type="radio"/> Mr <input type="radio"/> Dr	Phone: *	<input type="text"/>
First Name: *	<input type="text"/>	Mobile:	<input type="text"/>
Last Name: *	<input type="text"/>	E-Mail: *	<input type="text"/>
		Availability:	<input type="text"/>
PEM Encoded PKCS #10 Request: *			
<input type="text"/>			
* Mandatory Field			
<input type="button" value="Send"/>			

Common WLAN Authentication Methods: EAP-SIM

- SIM cards are authentication devices users are used to
- Problem:
 - ^ user needs SIM slot in computer
 - ^ SIMs support usually only single sessions

The Trusted Computing Group

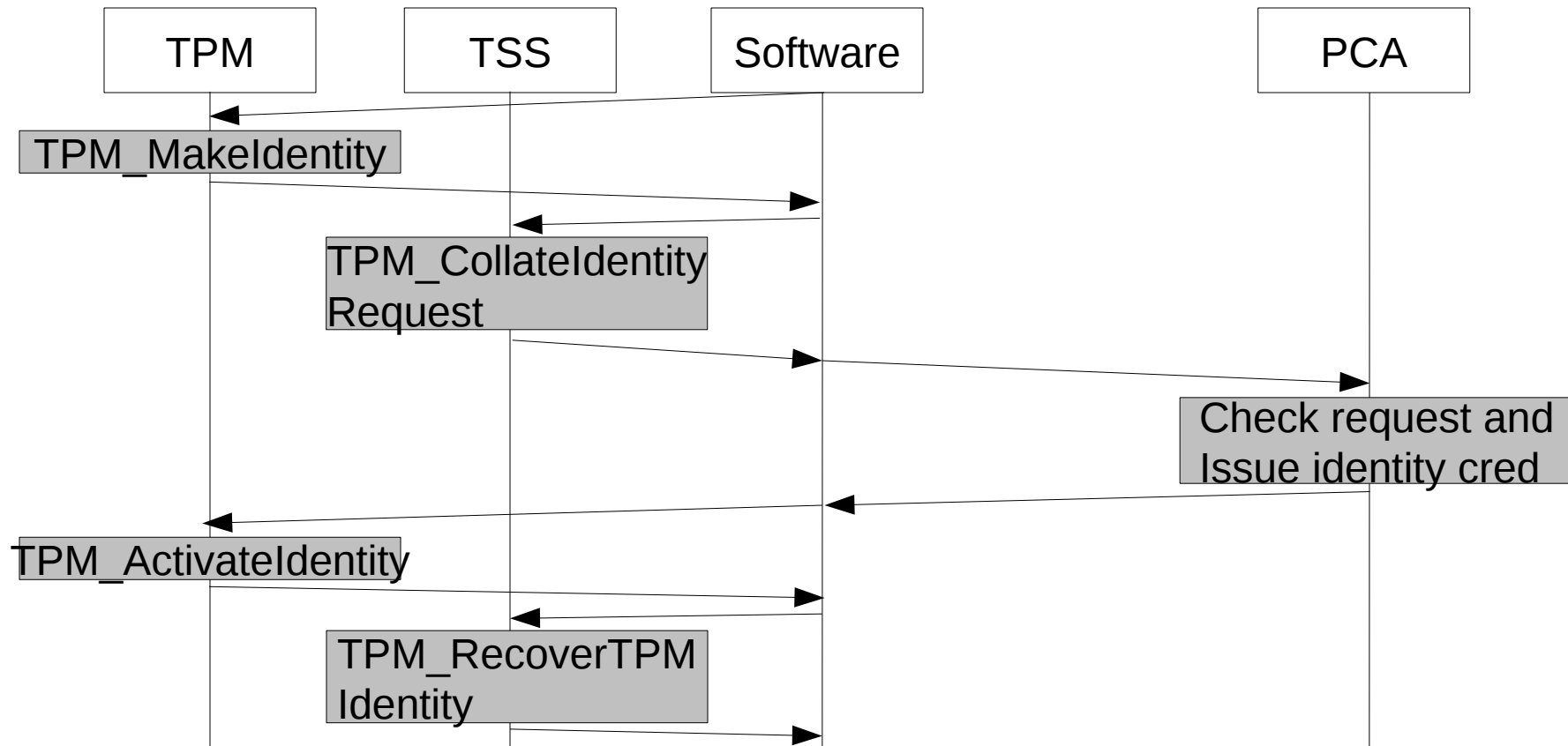
- Industrial standardization body focused on developing, defining and promoting trusted computing standards
- Standardized the Trusted Platform Module (TPM) in 2002



The Trusted Platform Module

- Cryptographic hardware to store keys and hashes
- Provides some cryptographic functions
- No cryptographic co-processor!!!
- May be uniquely identified worldwide
- Provides so called identities

TPM Identities



EAP-TPM

■ TLS < 1.2

^ RFC4346:

```
struct {
  select (SignatureAlgorithm) {
    case anonymous: struct {};
    case rsa:
      digitally-signed struct {
        opaque md5_hash[16];
        opaque sha_hash[20];
      };
    case dsa:
      digitally-signed struct {
        opaque sha_hash[20];
      };
  };
} Signature;
```

^ TPM Spec:

- Identity key is restricted to SHA-1 signing...

■ TLS 1.2

^ RFC5246:

In RSA signing, the opaque vector contains the signature generated using the RSASSA-PKCS1-v1_5 signature scheme defined in [PKCS1]. As discussed in [PKCS1], the DigestInfo MUST be DER-encoded [X680] [X690]. For hash algorithms without parameters (which includes SHA-1), the DigestInfo.AlgorithmIdentifier.parameters field MUST be NULL, but implementations MUST accept both without parameters and with NULL parameters. Note that earlier versions of TLS used a different RSA signature scheme that did not include a DigestInfo encoding.

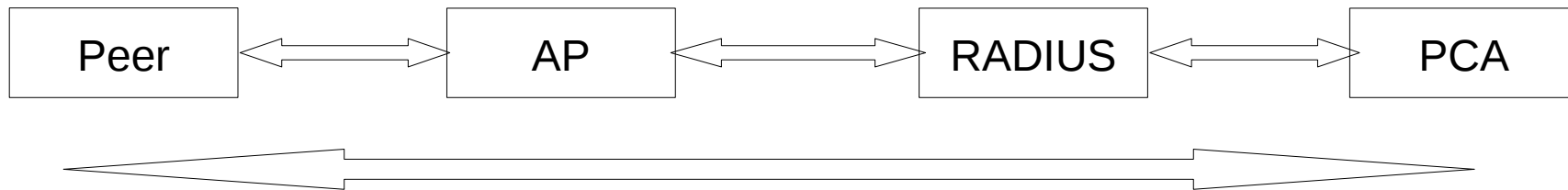
^ That is a standard signature!

EAP-TPM Supporting TLS < 1.2

- RFC3820 “Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile”
 - ^ Does not go together with TPM Spec...
- RFC4680 “TLS Handshake Message for Supplemental Data”
 - ^ Generate key certified by identity key
 - ^ Generate self signed certificate out of certified key
 - ^ Send self signed certificate in handshake and identity certificate in supplemental data

EAP-TPM Proof of Concept

- Perfectly running since Oct 2008 :-)
- Create new unsigned certificate out of identity certificate and send certified key info in X.509 extension
- Needs a verification service knowing all the identity certificates (= Privacy CA itself)



EAP-TPM with Auto-Provisioning

- Users do not want to request a certificate before connecting to WLAN hotspot
- Request certificate during TLS handshake using the RADIUS server as proxy
 - ^ RADIUS sends acceptable CA list
 - ^ if client has no certificate from any of them he sends an alert specifying the CA he wants to ask
 - ^ RADIUS will relay the client's request and the Privacy CA's answer

EAP-TPM Internet Draft

- <http://tools.ietf.org/html/draft-latze-emu-eap-tpm-00>
- First draft submitted in March 2009
- Version 01 with TLS 1.2 ↔ TLS <1.2 differentiation will come in July 2009
- Desired status: Experimental RFC
 - ^ loooooong way :-)

EAP-TPM Reference Implementation and Real World Evaluation

- Done at Swisscom in PWLAN DEV environment
- Evaluation against operator constraints



Conclusion

- Simple but promising protocol
- Proof-of-concept up and running
- Real world (usability) evaluation still ongoing (not part of PhD)
- More comfortable for the user
- Allows to connect embedded devices like mobile phones and mobile game consoles

Questions?

Thanks for your Attention :)