Towards a Secure and User Friendly Authentication Method for Public Wireless Networks

Carolin Latze
University of Fribourg
Switzerland
Table of Contents

- Motivation
  - 2G and 3G Cellular Networks
  - IEEE 802.11 Networks
- Trusted Computing
- TLS TPM Extension
Motivation

Authentication in 2G Cellular Networks
Motivation
Authentication in 3G Networks

Distribution of Authentication Vectors from BLR to VLR/SGSN

Verify AUTN(i)
Compute RES(i)
Compute CK(i) and IK(i)

User Authentication Request
RAND(i), AUTN(i)

User Authentication Response
RES(i)

Authentication Data Request
IMSI

Authentication Data Response
AV(1..n)

Generate Authentication Vectors
AV(1..n)

Store A(1..n)
Select A(i)

Compare RES(i) and XRES(i)
Select CK(i) and IK(i)

Authentication and Key Establishment
Motivation
Conclusion Authentication in Cellular Networks

- All the complexity is hidden in SIM
- SIM belongs to one provider
- Same SIM cannot be used with other provider
Motivation
Authentication in IEEE 802.11 Based Networks I/III

Pour tout renseignement complémentaire : netmaster@unifr.ch, Tél. +41 26 300 72 30

UNIVERSITÉ DE FRIBOURG / DEPARTMENT OF INFORMATICS
Motivation
Authentication in IEEE 802.11 Based Networks II/III

Peer

EAP-Request/Identity
(ID)

EAP-Response/EAP-Type=EAP-TLS
(TLS Start)

EAP-Request/EAP-Type=EAP-TLS
(TLS client_hello)

EAP-Response/EAP-Type=EAP-TLS
(TLS server_hello,
TLS certificate,
[TLS server_key_exchange,]
TLS certificate_request,
TLS server_hello_done)

EAP-Response/EAP-Type=EAP-TLS
(TLS certificate,
TLS client_key_exchange,
TLS certificate_verify,
TLS change_cipher_spec,
TLS finished)

EAP-Request/EAP-Type=EAP-TLS
(TLS change_cipher_spec,
TLS finished)

EAP-Response/EAP-Type=EAP-TLS

EAP-Success

Authenticator
Motivation
Authentication in IEEE 802.11 Based Networks II/III

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: 
Title: * Mrs Mr Dr
First Name: *
Last Name: *
Function: No data
Phone: *
Mobile: 
E-Mail: *
Availability: 

PEM Encoded PKCS #10 Request: *

* Mandatory Field

Send
Motivation:
Authentication in IEEE 802.11 Based Networks III/III
Motivation: Authentication in IEEE 802.11 Based Networks III/III

EAP-Request/Identity

EAP-Response/Identity

EAP-Request/SIM/Start (AT_VERSION_LIST)

EAP-Response/SIM/Start (AT_NONCE_MT, AT_SELECTED_VERSION)

Obtain GSM Triplet From AUC

EAP-Request/SIM/Challenge (AT_BAND, AT_MAC)

GSM Algorithms
Verification of AT_MAC
Derivation of session keys

EAP-Response/SIM/Challenge (AT_MAC)

EAP-Success
Motivation: Authentication in IEEE 802.11 Based Networks III/III

Peer

EAP-Request/Identity

EAP-Response/Identity

EAP-Request/SIM/Start (AT_VERSION_LIST)

EAP-Response/SIM/Start (AT_NONCE_MT, AT_SELECTED_VERSION)

Obtain GSM Triplet From AUC

EAP-Request/SIM/Challenge (AT_RAND, AT_MAC)

GSM Algorithms Verification of AT_MAC Derivation of session keys

EAP-Response/SIM/Challenge (AT_MAC)

EAP-Success

Authenticator
Trusted Computing

- TCG is an industrial standardization body
- Trusted solutions are expensive and proprietary – TCG was formed to overcome that problem
- Specified trusted/ authenticated boot
- Specified TPM
Trusted Platform Module

- Small piece of trusted hardware
- Cheap!!!!
- Endorsement credential:
  - ^ Statement that it is end.cred. | pubek | TPM type and properties | ref to signing TPME
- Conformance credential
- Platform credential:
  - ^ Statement that it is plat.cred. | ref to end.cred. | ref to conf.cred. | platform type and properties | ref to signing PE
- Identities (Attestation Identity Keys)
TPM Identities

- Bound to a certain TPM
- Special purpose keys
TPM Identities

- Bound to a certain TPM
- Special purpose keys
GSM SIM = WLAN TPM
TLS TPM Extension I/II

- Use TPM for easier certificate handling
- AIK certificate is limited to sign TPM originated data...
TLS TPM Extension I/III

- Use TPM for easier certificate handling
- AIK certificate is limited to sign TPM originated data...

```c
typedef struct tdTPM_CERTIFY_INFO {
    TPM_STRUCT_VER   version;
    TPM_KEY_USAGE    keyUsage;
    TPM_KEY_FLAGS    keyFlags;
    TPM_AUTH_DATA_USAGE authDataUsage;
    TPM_KEY_PARMS    algorithmParms;
    TPM_DIGEST       pubkeyDigest;
    TPM_NONCE        data;
    BOOL             parentPCRStatus;
    UINT32           PCRInfoSize;
    [size_is(pcrInfoSize)] BYTE* PCRInfo;
} TPM_CERTIFY_INFO;
```
TLS TPM Extension I/II

- Use TPM for easier certificate handling
- AIK certificate is limited to sign TPM originated data...

```c
typedef struct tdTPM_CERTIFY_INFO {
    TPM_STRUCT_VER               version;
    TPM_KEY_USAGE                keyUsage;
    TPM_KEY_FLAGS                keyFlags;
    TPM_AUTH_DATA_USAGE          authDataUsage;
    TPM_KEY_PARMS                algorithmParms;
    TPM_DIGEST                   pubkeyDigest;
    TPM_NONCE                    data;
    BOOL                         parentPCRStatus;
    UINT32                       PCRInfoSize;
    [size_is(pcrInfoSize)] BYTE* PCRInfo;
} TPM_CERTIFY_INFO;
```

```
Certificate ::= SEQUENCE {
    tbsCertificate        TBSCertificate,
    signatureAlgorithm    AlgorithmIdentifier,
    signatureValue        BIT STRING
}
```

```
TBSCertificate ::= SEQUENCE {
    version        EXPLICIT Version DEFAULT v1,
    serialNumber   CertificateSerialNumber,
    signature      AlgorithmIdentifier,
    issuer         Name,
    validity       Validity
    subject        SubjectPublicKeyInfo,
    issuerUniqueID IMPLICIT UniquelIdentifier OPTIONAL,
    subjectUniqueID IMPLICIT UniquelIdentifier OPTIONAL,
    extensions     EXPPLICIT Extensions OPTIONAL
}
```
TLS TPM Extension II/III

- SKAE
TLS TPM Extension II/III

- SKAE → complicated
- TPM Certificates
TLS TPM Extension II/III

- SKAE → complicated
- TPM Certificates → not standard conform
- child certificate
TLS TPM Extension II/III

- SKAE → complicated
- TPM Certificates → not standard conform
- child certificate → CA:false
- X.509 proxy certificate
TLS TPM Extension II/III

- SKAE → complicated
- TPM Certificates → not standard conform
- child certificate → CA:false
- X.509 proxy certificate → subject=NULL
TLS TPM Extension III/III

Client

ClientHello (w/ extensions)---------->

SupplementalData
Certificate*
ClientKeyExchange
CertificateVerify*
ChangeCipherSpec
Finished

<----------

Server

ServerHello (w/ extensions)
Certificate
ServerKeyExchange
CertificateRequest*
ServerHelloDone

----------->

ChangeCipherSpec
Finished

* indicates optional or situation dependant messages
TPM > SIM

- More than one identity per module
  - Different operators for roaming
- WLAN only WISP
  - SIM support is expensive!
- Zeroconf for companies
  - Do not request identities in advance (TPMs are trusted)
Zero Configuration
Evaluation EAP-TLS Software vs. TPM
Conclusion

- Secure (proven) and comfortable user authentication
- Very easy to implement in real world environment
  ^ Processes will be bigger issue
- Added values since TPM allows for more applications
- TPM is already integrated into most of the new computers
- IEEE 802.1AR defines TPMs to be suitable as DevID module!
Question?

Thanks for your attention!