Certificate Use in 802.1X/EAP-TLS

Verification, validation, and trust

ISO/IEC JTC1 SC6
Ottawa, Canada
February 2014

Agenda

- Overview of certificates and certificate processing
- The OCSP Protocol
- Certificate processing in 802.1X/EAP-TLS

Characteristics of a Public Key Infrastructure

- Infrastructure may be hierarchical
  - A peer's certificate may be signed by somebody with whom you do not have a trust relationship but whose certificate is signed by someone with whom you do
  - Establishment of certificate chains may be necessary
- Issuers of certificates revoke certificates and support checking of revocation two ways:
  - Off-line using Certificate Revocation Lists (CRLs), periodically generated by Certification Authority (CA)
  - On-line using OCSP, using a server run by the certification authority
- Certificates are revoked when compromise occurs
- Presentation of a valid, legitimately signed, and unrevoked certificate is not enough– not all PKIs are created equal

Assumptions on Certificate Processing

- An entity wishing to validate a peer's certificate has a trust anchor or a trust anchor database
- Trust anchor database only contains certificates of Certification Authorities (CAs) that are trusted to issue certificates for the purpose at hand
- A trust anchor database is specific to the purpose at hand– for example, wireless access to a specific network
- Not all trust anchors or trust anchor databases are suitable for a specific purpose at hand!

Assumptions on Certificate Processing (continued)

- The Certification Authority (CA) is the Trusted Third Party
- Trust placed in Certification Authorities:
  - They do an appropriate amount of due diligence prior to issuing a certificate (to bind an identity to a key)
  - They can be trusted to issue certificates to entities that can legitimately perform the purpose at hand
  - They will apply appropriate constraints on certificates, if necessary
  - They will revoke a certificate if comprise occurs.

Steps Taken for Certificate Validation

1. Establish trust in issuer: Is issuer of received certificate in the trust anchor database? If not, is it possible to construct a chain to the issuer? If not, then fail.
   - Each certificate in the chain, up to the trusted CA, must be individually and separately validated (steps 2-6) in order establish trust in the issuer
2. Check issuer's signature: Is integrity of received certificate intact (is the trusted issuer's signature valid)? If not, then fail.
3. Check lifetime: Has certificate validity period expired or is it not yet valid? If so, then fail.
4. Check constraints: Is the received certificate constrained to prevent the use for which it was presented? If so, then fail.
5. Check Name (optional): Does the subject name match some external information– e.g. DNS name, SSID, etc.– that the purpose at hand requires? If not, then fail.
6. Revocation check (optional): Has this certificate been revoked? If so, then fail.

Agenda

- Overview of certificates and certificate processing
- The OCSP Protocol
- Certificate processing in 802.1X/EAP-TLS

OCSP

- OCSP stands for “On-line Certificate Status Protocol”
- OCSP answers a single question: “has this certificate been revoked?”
  - The OCSP server does not do any other kind of certificate validation
  - Alternative to an on-line certificate status check is to use a Certificate Revocation List (CRL)
- OCSP server is “on-line” (hence the name)

OCSP

- OCSP extension to TLS allows for the client, who may not have network connectivity, to connect to an OCSP server through the TLS server
  - Protocol is secure against forgery by TLS server
  - Protocol provides for liveness proof to client
- 802.1X/EAP-TLS server always has access to OCSP server since it has network connectivity

Agenda

- Overview of certificates and certificate processing
- The OCSP Protocol
- Certificate processing in 802.1X/EAP-TLS

Type of 802.1X/EAP Deployment

- Deployed in the only way supported by TePA
  - All supplicants and all authenticators have certified public keys
  - Supplicant and authenticator share a trusted third party (or can chain up to a position of trust)
- Supplicant (Authenticator) validates the certificate received by the Authenticator (Supplicant)
- Supplicant and Authenticator have the means to build a certification path to a common root
- Certificate revocation check using OCSP server or Certificate Revocation List (CRL)

The Issue of Trust

- The AS is ***NOT*** the trusted third party, the Certification Authority (CA) is
- Trust anchor database (TADB) is generally bootstrapped prior to deployment
  - Not all TADBs are equal
  - A browser's TADB is not suitable for network access

Certificate Processing in 802.1X using EAP-TLS

- Inherited requirements
  - 802.1X specifies using EAP, e.g. EAP-TLS
  - EAP-TLS specifies using TLS
  - TLS uses the PKI and CRL profile of RFC 5280
  - RFC 5280
    - Describes X.509v3 certificates and extensions
    - Defines additional Internet-specific extensions
    - Describes the X.509v2 CRL format
    - Defines an algorithm for X.509 certificate path validation

Certificate Processing in EAP/TLS

- Supplicant
  - Trust that a CA will only issue properly named and constrained certificates to entities that can perform network access control.
  - Have trusted CA's certificate in Trust Anchor Database
  - Successful certificate validation implies that an entity that proves possession of the private analog to the certified public key is named and constrained by the certificate
  - Authentication using the peer's certificate provides an authenticated identity and, optionally, a set of constraints
  - Authorization is based on the trust placed in the CA as limited by any constraints or by the subject name

Certificate Processing in EAP/TLS

- Authenticator
  - Trust that a CA will only issue certificates to clients that have properly identified themselves and, optionally, that the certificate is client constrained
  - Have trusted CA's certificate in Trust Anchor Database
  - Successful validation implies that the entity proving possession of the private analog to the certified public key is named and constrained by the certificate
  - Authentication using the peer's certificate provides an authenticated identity
  - Authorization is based on the trust placed in the CA as constrained by the name and any certificate attributes
  - AAA server can be used to further refine authorization to obtain, for instance, VLAN information for a particular client named by the subject of its certificate

Summary

- 802.1X with EAP-TLS insures security through compliance with established standards
- Certificates and PKI are properly used
  - Establishment of TADB
  - Verification of presented certificates
  - Determination of a verifiable identity to authenticate
- TLS authentication of verified identity
- Authorization
  - Through TADB and trust placed in issuer of peer's certificate
  - Through constraints placed in peer's certificate
  - Optionally, authenticator can use AAA server to obtain additional authorization information

Merci!

Thanks!