TeSSA^2

A Revocation, Validation and Authentication Protocol for SPKI Based Delegation Systems

{Yki.Kortesniemi, Tero.Hasu}@hut.fi
Jonna.Sars@nixu.fi

Outline

- Certificates
- Revocation
- Quota
- Proposed changes to SPKI
- The revocation protocol
- Conclusions

Certificates

- Certificates are fixed-form digitally signed documents
  - Self-contained
- Two main types
  - Name/Identification (e.g. X.509)
  - **Authorisation** (e.g. SPKI)
- SPKI - Simple Public Key Infrastructure
  - Five-tuple: Issuer, Subject, Tag, Delegation, **Validity**

Need for revocation

- Certificates are good for granting rights
- But how do you revoke them in case of
  - exposure of private key
  - misuse of rights
- Certificates can not be deleted
  - unlike ACL entries
- Requirements for revocation
  - deterministic
  - revocation interval controlled by issuer

Current revocation solutions

- CRL and variations (e.g. Delta-CRL)
  - Support offline operation
  - Can include unnecessary information → waste bandwidth
- Revocation Trees
  - maintaining the tree requires computation
- Bill of health

SPKI Validity

- Several possibilities (all optional)
  - not before
  - not after
  - CRL (Certificate Revocation List)
  - Reval
    - Bill of Health
  - One-time
    - free-form online condition

Problems with SPKI

- Using CRLs offline is very difficult
  - multiple issuers → multiple CRLs
  - multiple uses → multiple CRLs
  - asynchronous → need network connection often
- Consolidating the revocations into only a few CRLs is not good because of
  - different revocation intervals and uses

Need for quota 1/2

- Certificates mainly limit usage to a time interval
  - Within that limit can use the resource at will
- We want more fine grained limits, such as
  - 3 hours per day (e.g. a database)
  - 5 times (e.g. a bus ticket)
  - up to $1000 per month (e.g. a credit card)

Need for quota 2/2

- Requirements for quota
  - Quota model is selectable by the certificate issuer
  - Prevents unauthorised usage of quota
  - Prevents unauthorised monitoring of quota usage

Proposed changes to SPKI

- Deprecate CRL
- Introduce Renew
- Introduce Limit

- Define query format
- Define negative replies

The revocation protocol 1/2

- Supports all SPKI revocation methods (CRL, D-CRL, bill of health)
- Supports quota (new online check type)
- Fulfils the requirements
  - deterministic, interval chosen by issuer
  - quota model chosen by issuer
  - prevents unauthorised usage and monitoring of quota

The revocation protocol 2/2

- Security based on ISAKMP
- Operation
  - User establishes connection to verifier (authentication)
  - The chain is completed
  - User authorises quota checks
  - Simple checks are made (= all except quota)
  - Quota checks are made
  - Service is granted

Critique of protocol

- Has overhead
  - Can sometimes be distributed over several uses
- Creates state data in the verifier
- Requires online connection

Conclusions

- Offline revocation methods like CRL are not practical for SPKI
- SPKI specification should be completed
- Introducing quota opens up new possibilities
- Protocol can be implemented on top of ISAKMP or another similar protocol