Privilege delegation using attribute certificates in ISO SC33

Tim Moses
Director, Advanced Security Technology
April ‘98
Related documents

- OpenGroup Distributed Security Framework
  - Basic Security Facilities - Authorisation
- ANSI X9.57, ISO/TC68 WD 15782
  - Attribute certificate syntax
  - Specific to public-key techniques
- ANSI X9.45
  - Selected attribute syntax
  - Canonicalized “document” syntax
  - Delegation model
Related documents (cont’d)

- Internet draft “TLS Extensions for AttributeCertificate based authorization”
  - draft-ietf-tls-attr-cert-00.txt
- IS 9594-8, ITU-T X.509
  - Attribute certificate syntax
  - Specific to public-key techniques
ISO SC33 generalized “control” model

Claimant (privilege) → Verifier

Control policy

service request

Service (sensitivity)
Applicability of generalized control model

- Where identity-based controls are inadequate
- Where role-based controls are more suitable
- Need to scale across organizational or geographical domain boundaries
- Need to scale across many applications
- Need some measure of central control, avoiding administrative bottle-necks
Example 1 - Funds disbursement

- **Service**
  - Disburse funds

- **Service sensitivity**
  - Value of transfer

- **Claimant**
  - Authorizer of transfer

- **Claimant’s privilege**
  - Signing authority

- **Control policy**
  - Signing authority must be greater than or equal to the value of the transfer
Example 2 - Classified eMail

✧ Service
  • Encrypt a classified document for a recipient

✧ Service sensitivity
  • Document classification

✧ Claimant
  • Recipient

✧ Claimant’s privilege
  • Recipient’s security clearance

✧ Control policy
  • Clearance must be greater than or equal to the classification
Example 3 - Applet access control

- **Service**
  - Access desktop resources

- **Service sensitivity**
  - Set of resources for which access is requested

- **Claimant**
  - Applet

- **Claimant’s privilege**
  - Set of resources for which access is granted

- **Control policy**
  - Requested desktop resources must be a subset of those granted
Delegation

Why should the Verifier “trust” the Claimant’s claimed privilege?

- Out-of-scope for the OpenGroup framework

Process of delegation

- The Delegator entrusts privilege to a Delegate

Delegate’s privilege should be a “subset” of the Delegator’s privilege

“Subset” is defined in the context of the Control Policy
General delegation model

Source of authority

Verifier

claims privilege

delegates privilege

Claimant

delegates privilege

trusts unconditionally

Verifying

Orchestrating Enterprise Security
Privilege set

Intermediate claimant

Direct claimant

Minimum acceptable privilege for the Service Sensitivity according to the Control Policy

Source of authority
Delegation requirements

- Verifier-centred view
- Authorities have the controls necessary to impose restrictions on subsequent links in the delegation path
- No bottle-neck for privilege assignment
- Strong similarity to X.509 v3 control of the public key certification path
  - X.509 extensions require “interpretation” in the context of privilege delegation
Delegation controlled by certificate extensions

- Attribute authority identifier
- Owner attribute identifier
- Attribute value mappings
- Basic constraints
- Name constraints
- CRL Distribution points
Definition of attribute certificate extensions

- Attribute authority identifier field
  - Assists Verifier in locating the issuer’s corresponding privilege for delegation path validation

- Owner attribute identifier field
  - Assists Verifier in locating the owner’s corresponding role certificate for delegation path validation
Definition of attribute certificate extensions - continued

- Attribute value mappings field
  - Allows mapping of privilege or sensitivity across domain boundaries

- Basic constraints
  - Allows control over delegation path length

- Name constraints
  - Allows control over delegation name space

- CRL distribution points
  - Allows scalable revocation of privilege
Additional work items

- Delegation is just one aspect of the overall problem

- Syntax of Service Sensitivity vector
  - Confidentiality label, EDI transaction elements, XML document elements, desktop resources, etc.

- Syntax of Claimant privilege
  - Clearance, signing authority, desktop resources

- Syntax of Control Policy
  - Formal language syntax with boolean range

- Protocols
  - TLS, S/MIME, PKINIT
Summary

- Authority topic is being tackled in a number of forums
- ISO, ANSI and IETF are addressing the topic using public-key techniques
- ISO SC33 addressing the use of certificate extensions to control delegation