LionShare: Federated Security in a Peer-to-Peer Environment

Derek Morr
Emerging Technologies
LionShare criteria

- Can’t share files anonymously
- Can share with access controls
- Searches are anonymous
- Retrieval is pseudonymous
- We can’t mandate authN mechanisms
- Reuse existing infrastructure where possible
Our solution

- X.509 for authN – SASL–CA
  - Like U. Much kCA but more flexible
- XACML for authZ
  - Using Shibboleth Attribute Authority
Why the SASL-CA?

- We wanted PKI without the headaches
- Short-lived certificates
- Never store private key
- Run-time negotiation of authN mechanisms
- Needed different certificate types
- Needed flexible attribute sources
SASL-CA Architecture
Certificate Contents

- Server certificate
- Has a regular DN
- Used to share files on a network

**Ex:** CN=DEREK VAUGHAN MORR(dvm105@psu.edu)/dvm105@psu.edu, OU=TEACHING & LEARNING TECHNOLOGY, O=Pennsylvania State University, L=UNIVERSITY PARK, ST=Pennsylvania, C=US
Certificate Contents

- **Client certificate**
- Has an opaque DN (a Shibboleth handle)
- Used to request files from other peers and obtain attributes

**Ex:**
```
CN=AGOCMHOJNN2TJUYVY672M672UBW7FQ20XGKX
RCOTHPQ7TQDUPGUEKPGNVDWJBBNFC2T3RLVVCMTJFXW
6B1DBM6LLYNSCUNZITWHRGZY
```
Queries

Either use standard Gnutella filename-based query or a metadata-based search.

Queries are unsigned, unencrypted and unauthenticated.

This was chosen for scaling issues.
QueryReply

- Cryptographic hash of the file
- Traditional metadata stream
- IEEE–LOM, Dublin Core, etc
- List of required attributes
- Digital signature of the metadata
  Signed with server peer’s server cert.
Attributes

- Users decide, at run-time, which attributes to release to whom.
- Individual peers query the AA to obtain signed attribute assertions.
- Attributes must be created with Holder-of-Key confirmation using the client peer’s client cert.
<Subject>
  <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format emailAddress">dvm105@psu.edu</NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
    <SubjectConfirmationData xsi:type="saml:KeyInfoConfirmationDataType">
      <ds:KeyInfo>
        <ds:KeyName>Derek's Key</ds:KeyName>
      </ds:KeyInfo>
    </SubjectConfirmationData>
  </SubjectConfirmation>
</Subject>
Outstanding Issues

- Firewalls and NAT
- Gnutella PUSH protocol
- SAML and XACML not compatible in 1.0
- How to handle users outside the federation
LionShare
Requirements

- Enterprise authentication system
- Directory service (eduPerson-enabled)
- Shibboleth Identify Provider
- SASL-CA
- Membership in a federation
Resources

LionShare
http://lionshare.its.psu.edu/

SAML
http://www.oasis-open.org/committees/tc_home.php?
wg_abbrev=security

XACML
http://www.oasis-open.org/committees/tc_home.php?
wg_abbrev=xacml