

Securing Collaborative Environments

Mary Thompson, Deb Agarwal, Keith Jackson

Workshop on Advanced Collaborative
Environments

WACE Summer 2002



Collaborative Environments

- Person to person collaboration facilitated by computer tools
- Members from diverse organizations
 - ▶ Want to connect from home, conferences, airports
- Some persistent shared resources at diverse sites
 - ▶ Documents, Persistent services
- Does not necessarily have a persistent central authority, e.g. peer-to-peer
 - ▶ May be built incrementally



Ad-hoc communication groups

- Built incrementally, members invite others to join
- Short-lived, but may produce persistent data
 - ▶ Meeting logs,
 - ▶ Co-authored documents
- Access Grid sessions
- Chat sessions



Security requirements

- Authentication of users
 - ▶ Universal name and key mapping
- Authorization of users
 - ▶ Authentication and access policy (static)
 - ▶ Delegation from trusted party (more dynamic)
- Privacy of data
 - ▶ Access control and encryption
- Integrity of data
 - ▶ HashMACs and signatures

Common Authentication Mechanisms

- Username-Password
 - ▶ Usually local to one domain
- PGP keys
 - ▶ Trust by relying party depends on out-of-band method or “web of trust”
 - ▶ Doesn't scale well
- Kerberos ids - shared secret
- X.509 – public/private keys



Kerberos Ids

- Unlocked by password (kept in user's head)
- Central KDC server must be available
- For trust across diverse organizations cross-realm agreements must exist



X.509 Identity Certificates

- Cross-realm trust established by each domain trusting the same CAs
- Requires CA infrastructure
- Users must have machine readable credential available whenever they connect to remote resource
- Globus proxy credentials provide for single-sign-on by delegating a short-lived unencrypted X.509 proxy credential
- On-line proxy servers can create a proxy for a user who authenticate via a password



Authorization certificates

- Grant rights to the holder
- Rights can be dynamically delegated by a trusted party, e.g. creator of a communication group
- Two open-source academic implementations exist
 - ▶ SPKI/SDSI - 1999 IETF RFC2692,2693, for SPKI (Ellison), SPKI/SDSI code release from MIT (Rivest, Lampson)
 - ▶ KeyNote 1999 IETF RFC2704 (Blaze, et.al AT&T labs)
- Holder of certificate still has to prove that it is his certificate (public/private key pair)



Authorization Certs (cont)

- Virginia Tech, Markus Lorch, Dennis Kafura
- Use PKIX –compliant Attribute Certificates (ASN.1)
 - ▶ Contains resource, subject DN, privileges
 - ▶ A trusted user can delegate some of his rights to a new user in a signed attribute certificate
 - ▶ All users must have X.509 certs.
 - ▶ Currently supports “access to machine” privileges and file “read,write and execute” privileges
- The attributes certs are used by a system that uses the POSIX acl extensions to allow privileges to be added for a “minimal” uid.
- <http://zuni.cs.vt.edu/grid-security/>



Secure Communications

- TLS (OpenSSL)
 - ▶ Depends on X.509 credentials
 - ▶ Provides integrity, confidentiality and authentication
 - ▶ Widely available open-source implementations
- GSI
 - ▶ OpenSSL plus delegated credentials
- Secure group communication (SGL)
 - ▶ Uses X.509 credentials for authentication
 - ▶ Akenti for authorization
 - ▶ SGL for group key agreement



Multi-level solutions needed

- Secure communication based on X.509 certs
- User X.509 certs require too much infrastructure for ad-hoc collaborations and are hard to use away from “home”
- Username/password can work in small and dynamic collaborations but might give fewer privileges
- Dynamically created key pairs and delegated authorization certificates could be used for incrementally building trust.

