Videoconferencing Middleware

Secure environments for Videoconferencing
Possible Scenario

Alice, a student at one campus, wants to call Bob, a faculty member at another campus. Alice attempts the call, and her campus verifies it is okay for her to place this call. Bob’s campus verifies that Alice is allowed to call Bob. Bob is notified that Alice is calling, and can choose to accept/deny the request based on that information.
Tasks

Developing middleware for secure video conferencing, including:

• Resource Registration
• Resource Discovery
• Call Initiation

This division allows for:

• independence of underlying protocols from resource discovery and vice versa
• Offers flexibility in policy decision points
• Minimal changes to SIP and SHIB (hopefully)
Where are we today?

• A long discussion of the problem
• A set of scenarios are being developed
• A number of flows have been suggested
• Still a number of unresolved issues
Videoconferencing with native SIP (simplified)
Session Initiation Protocol

- SIP provides
  - Resource registration
  - Resource discovery
  - Call initiation
  - Authentication

- SIP does not do (well)
  - Flexible resource registration and discovery
  - User authentication across security domain
  - Authorization

Can Shibboleth/SAML help?
Resource Registration

Three possible methods

• **Web based**
  – User logs on to the Directory Server and populates it with its attributes.

• **SIP based**
  – User Agent registers with the registrar server

• **Extending SIP registration**
  – Some how combining the above
Resource Discovery

• The user browses a web site (presence server) that indicates the address of the entities that can be contacted.
  – This contact information is a protected resource and hence authorization is needed for access
  – Shibboleth?

• Other methods based on SIP
  – Proxies make routing decisions to reach target proxy
  – Target proxy determines availability of target user
Call Initiation

• Two possible methods have been suggested to secure the call session.
  – One method involves the caching of a normal INVITE at the target domain while some type of authorization is performed.
  – The other method requires adding information to the INVITE message at the origin, which could be used for authorization and/or authentication by intermediates.
Some general concerns

- Handling “non-secured” calls
- Privacy/Anonymity
- Network administration policy
- Incompatibility with existing SIP
- Replicating SIP functionality
- Increase in round-trip time
Open Issues

• Resolving scenarios
• Resolving flows
• Deciding on the role of Shib
• Implementation
• And more
Conclusions