This project involves the development of inter-domain role-based authorization capabilities for the Session Initiation Protocol (SIP).

Authorization mechanisms require database/directory queries to ascertain the privileges of a user. In an inter-domain scenario, this authorization mechanism may become burdensome. Burden may arise in that given the number of users in the various domains, the databases may become unmanageably large. Secondly, users and system administrators alike would be reluctant to have sensitive user information stored in so many different locations. This necessitates a new mechanism to effectively handle cross-domain authentication and authorization.

A role-based security policy allows authorization decisions to be based on roles that the user asserts rather than on his or her identity. By basing authorization decisions on the functions or “roles” of the users, complex access control lists are no longer needed for every resource. All that is required is a set of simple mappings containing the various roles and their respective privileges. Such an approach also promotes the privacy of user identity and use data.

Requirements for cross-domain, role-based authorization (RBA) can be satisfied by an approach that conveys user information between domains in the form of attributes. Such an approach would not need the information of one user to be stored in another domain, and conveying the attributes of the user would allow the user’s role to be defined facilitating a more granular, role-based authorization process. To convey the security attributes across domains, one could make use of the Security Assertion Markup Language (SAML). The SAML specifications include (among other things) bindings and profiles describing how SAML might be incorporated into other communication protocols and frameworks. One SAML binding and profile specification presently exists; it provides the basis for federated RBA for web resources.

To provide RBA for real-time communications, we are presently defining how SAML would operate within SIP. SIP is an application layer signaling protocol created by the Internet Engineering Task Force (IETF). SIP allows an entity to locate other entities on a network and invite them to partake in a session. SIP recommends various methods for performing authentication and authorization. However, it does not presently support inter-domain role-based authorization.

Student Projects:
One project will involve implementing SIP profiles and bindings for SAML. We have presently defined two profiles for using SAML in SIP; one describing the transfer of SAML assertions by value and the other by reference. The student will work to implement this model within the Vovida (vovida.org) open source VoIP platform.

A second project will involve the development of a threat model for each of the profiles.
This will involve a thorough analysis of the vulnerabilities and countermeasures in the context of various deployment environments.

This work is part of an initiative within the Video Middleware (VidMid) working group of Internet2 to develop middleware functionalities in the areas of security for cross domain multimedia applications such as videoconferencing. This work also relates and will contribute to the SIPPING working group of the IETF.