Intrinsic Security in the SORCER Grid
Abhijit Rai

Objective:
• Develop robust, scaleable and multi-layered security solutions for federated services including a generic secure wrapper for legacy code.

Approach:
• Deploying the following security requirements into the SORCER environment:
  ▪ Requestor/Provider identification and authentication
  ▪ Proxy verification
  ▪ Authorization
  ▪ Resource control and containment
  ▪ Privacy and Integrity
  ▪ Non-repudiation
  ▪ Accountability

Task Description
A grid is a vast repository of virtual services. Grids are being built with systems that build up, rather than replace, legacy components. And that makes securing virtual services more difficult.

Schedule
1. Background Research 09/01
2. Authentication and Identification 09/15
3. Proposal Presentation 09/30
4. Facilitate Authorization 10/15
5. Implement Proxy Verification 10/30
6. Enable Auditing Capabilities 11/15
7. Thesis Defense and Demo 12/10

Benefits
1. Controls access to the federated services in the SORCR grid.
2. Provides multi-layered authorization with the help of policy objects, guarded objects, and JAAS.
3. Builds trust between client and the service by proxy verification.
4. Audits (Reporter provider) execution of federated providers.