Unified Application Data Access Management

Status: Draft (Albert Wu)

Summary: UCLA needs a way to consistently manage an application's access to data and other systems. An application identity management framework based on Grouper/Signet may be the solution.

Current Situation

UCLA is undergoing an explosive growth of applications and web services. These applications are becoming increasingly interconnected. Most of these applications need data. However, there is no consistent mechanism to manage data release. The campus data stewards current grant data access on a per application, per data source basis. There is no way for campus data stewards to manage the re-transmission of data other than saying "Thou shalt not re-transmit data." This restriction puts a severe constraint on the IT community's ability to deploy a service oriented architecture where data can flow freely and securely in all direction. Worse, the inconsistencies between data release creates opportunities for inadvertent leak of sensitive data.

Opportunities for Improvement

With UCLA deploying Shibboleth as its intra-campus WebSSO solution, it has the basics of an application identity registry. It also introduces an interesting foundation for expressing data access privileges (Shibboleth ARP). This basic registry can be expanded to support a generalized web service to web service authentication framework based on WS-* stack.

Furthermore, if one thinks of an application as a subject in Signet terms, Signet (or its derivative) can be used to manage data access across various systems. The Signet privilege statements can potentially be transformed into Shibboleth ARP, LDAP access rules, SQL database ACL, etc. This would provide the data stewards with unprecedented ability to manage data release across the enterprise, while enabling a true SOA environment to flourish.