GridLogon: A Grid Service for Security Usability

Jim Basney and Von Welch

{jbasney,vwelch}@ncsa.uiuc.edu

Problem Statement

In order to establish trust with Grid resources, users need to have a non-trivial quantity of credentials and information. To prove their trustworthiness to resources they need an X.509 identity certificate and private key and possibly one or more attribute assertions, such as those issued by VOMS or CAS, which are becoming more common as resource providers move to role-based access control for greater manageability.

In addition, trust establishment is a two-way street – users must also establish their trust of the resources they use. This requires a variety of information about what the user's trust roots are – today, what certificate authorities (CAs) they trust and their signing policies; in the future we see additional roots such as names of trusted information servers, jobs brokers, etc.

Installing all this security information manually is error-prone: typical Grid users do not have (or want to have) a deep understanding of distributed system security but Grid security configurations are very brittle (meaning a small error can cause all security operations to fail). Complicating this is the dynamic nature of the Grid environment. The list of CAs a user trusts will vary over time as CAs are added based on changes in their virtual organization's (VO's) structures or the user's membership in VOs. Even if the list of CAs remains static, CAs publish lists of revoked certificates (CRLs) which may be frequently updated. Finally, the users themselves may be mobile, using different Grid access points at different times, requiring that all the security configuration be installed and up-to-date on any system that the user is currently using.

Today the user's Grid security configuration must be manually administered, meaning that a user must acquire an identity credential, locate trusted CA certificates and signing policies for all their trusted CAs, verify the information hasn't been tampered with by malicious parties (something that is generally ignored today), and then correctly install all this trust information. And then they must maintain it and move it around with them.

Based on the authors' personal involvement with establishing Grids, Grid CAs and Grid Toolkits, this configuration of user trust credentials and roots is arguably one of the largest hurdles to users getting onto Grids. With a trend towards role-based access control and VO information services to advertise available resources, this problem will only get worse unless something is done to help, as users will need not only CA information, but information regarding trusted attribute authorities, trusted directory services and so forth.

Proposed Work

Peter Gutman has recently proposed the concept of a "Plug-and-Play PKI" [1] to allow users to bootstrap all the trust information they need for interfacing with a PKI from a

single password. His goal was to literally make a PKI usable for his "recently-calibrated reference mother."

We propose to build off of the concepts introduced by Gutmann to build a Grid Logon Service. The goal is a service that allows a user, armed with nothing more than the name of a Grid Logon Service, a username and password, to bootstrap to being entirely configured to interact with normal Grid security systems. The Grid Logon client would allow them to connect to the Grid Logon service in order to download not only their credentials, but all trust root information. After downloading the information it would not only use it to configure the local system for functionality, but also following the best practice security procedures.

In essence, we proposal to make the Grid Login Service the user's one-stop shopping experience for Grid security. Running a Grid Login Service initially gains the user initial access to the Grid through establishment of their security credentials and configuration. Subsequent invocation allows for maintaining their security credentials and configuration. We develop our solution to be extensible, so that it not only solves the problem for the information that needs to be configured today, but can easily adapt to changing security technology and allow for additional or changed security configuration over time.

Our solution will be developed to work with the current stable version of the Globus Toolkit. Additionally we may support older versions (e.g. GT2) of the Globus Toolkit as appropriate depending on their level of deployment in the SciDAC communities. Our goal is to develop and support a high-quality production system that could be run for Grid communities by a production-quality organization (e.g. like the DOE Grids CA being run by ESNet today).

Some highlights of our proposed work are:

- *Establishment of trust with the Grid Logon Service.* Users will use the Grid Logon service to bootstrap all future trust, ensuring that the information they obtain from it is not tampered with is important. Given the small amount of information the user has to establish this trust, basically just a shared secret in the form of a password, this is a non-trivial problem. To solve this problem we will investigate the use of the Secure Remote Password (SRP) protocol with the Grid Logon Service to allow for mutual authentication of the user and the Grid Logon Service.
- *Integration with other security services.* In addition to allowing for the user to obtain identity credentials through the Grid Logon Service, we will integrate with attribute services such as CAS and VOMS so that users can obtain credentials from these services at the same time as the rest of their security configuration.
- *Social aspects.* We recognize that one of the larger hurdles in gaining acceptance of this work will be social and political rather than technical. Many in the Grid community consider user identity credentials held by a service rather than the user to be a violation of their CA policies. We believe that for Grids to prosper in the long-term, users will need help from services such as GridLogon to correctly configure their security environment. Hence part of our effort with this work will

be to overcome these non-technical hurdles through discussions in groups such as the Grid PMA (www.gridpma.org).

Relationship to Existing Work

A number of existing pieces of work exist today that we leverage or consider in our proposed solution to this problem.

MyProxy is an online credential repository developed by the authors. It potentially solves part of the problems described above by maintaining a user's identity credential in an online service and allowing a user to automatically download and install the credential by authenticating to the service with a simple password. It however does not address any of the problems of configuring the user's trust roots for establishing their trust of resources.

KX509/KCA is a system to allow a user to obtain an X.509 credential from a Kerberos credential. It does not address any issues of trust roots. In the longer term, it may be desirable to integrate the kx509 client into the Grid Logon client so that a user would be given a common interface when using KCA.

The work of the IETF Sacred working group provides similar functionality to MyProxy in that it would theoretically allow users to download and install their credentials from a central server. Like MyProxy, it also does not address any of the problems of configuring a user's trust root information. For example, the current Sacred protocol draft assumes TLS server authentication, i.e., assumes the client has a pre-configured set of trusted CA certificates. At this time of this writing, we can find no freely available open-source implementation of the Sacred standards. (We asked on the working group mailing list.)

A number of standards (or proposed standards) exist for allowing a user to outsource their authentication processing that could be applied to X.509 identify certificates used in today's Grid environments. For example XML Key Management Service (XKMS) and the Simple Certificate Validation Protocol (SCVP) allow a client to outsource their processing of authentication information to a trusted service. The Online Certificate Status Protocol (OCSP) allows a user to outsource the checking of revoked certificates and replaces CRLs. All of these solve parts of the problem of configuring a user's trust roots. However none of these solve the problem of the user acquiring their credentials. All of these solutions would also require modification to existing Grid client software to implement as well as establishing highly-available online services since each authentication by a user would require contacting these services.

Many commercial systems exist to solve this problem [2]. One common technique is to bootstrap with the default set of CA certificates installed in SSL-enabled web browsers to contacting credential services such as Microsoft .NET Passport and Liberty Alliance Identity Federation systems. Entrust Roaming PKI uses SPEKE authentication to download credentials from an online server. VeriSign Roaming Service uses a Ford-Kaliski scheme that requires users to contact two or more Roaming Servers to authenticate without revealing the password to any of the servers. NSD Security's Secure Identity Appliance uses split keys. Microsoft Roaming Profiles provide access to user's PKI credentials plus CA certificates and CRLs. RSA Security Keon Web Passport and Baltimore UniCERT Roaming also support downloading browser plug-ins that provide

access to user credentials. The primary disadvantage of all of these systems is that they are proprietary and provide limited interoperability with Open Source security software.

References

[1] Peter Gutmann, "Plug-and-Play PKI: A PKI your Mother can Use", Usenix Security Symposium, 2003. http://www.cs.auckland.ac.nz/~pgut001/pubs/usenix03.pdf

[2] Sarbari Gupta, "Security Characteristics of Cryptographic Mobility Solutions", Proceedings of the 1st Annual PKI Research Workshop, Gaithersburg, Maryland, April 2002. http://www.cs.dartmouth.edu/~pki02/Gupta/paper.pdf