A Roadmap for Integration of Grid Security with One-Time Passwords

April 18, 2004

Jim Basney, Von Welch, Frank Siebenlist

jbasney@ncsa.uiuc.edu, franks@mcs.anl.gov, vwelch@ncsa.uiuc.edu

1 Introduction

Recent security attacks have pointed to vulnerabilities in multi-use authentication secrets (e.g., static passwords). These attacks have not been limited to network sniffing, but instead have involved the introduction of Trojan services and modifications to kernels on multi-user or compromised computers in order to capture keystrokes directly. The success of this strategy has meant that previous tools for protecting passwords as they pass over the network (e.g., Kerberos [9], SSH [12]) are vulnerable, as the attackers can gain access to a user's password as it is being typed.

These attacks are leading many sites to investigate one-time password (OTP)[6] solutions for authentication. Many of these sites are also involved with one or more Grid deployments and need to provide similar OTP functionality for their Grid users.

We present here a roadmap for how Grid security will be integrated with OTP in order to meet the higher security demands of sites while also allowing them to continue their participation in Grids and other distributed science activities.

We follow with a brief overview of Grid security, in particular user credentials. We discuss our approach for integrating Grid security and one-time passwords through the instantiation of a new Grid credential service and our plans for implementing such a service. We conclude with a discussion of our future plans.

2 Overview of Grid Security

Grid security uses X.509 identity certificates [1] and a common protocol based on transport layer security (TLS, SSL)[3] for identification and authentication of Grid users. An X.509 certificate, in conjunction with an associated private key, forms a unique credential set that a Grid entity (service or user) uses to authenticate itself to other Grid entities; the TLS-based protocol is used to perform authentication and then provide message protection (encryption, integrity checking), as desired, on the subsequent data stream. A user's X.509 certificate and associated private key are normally managed by users and kept on a filesystem of the user's choosing. The private key is encrypted with a pass phrase that the user must supply whenever they access it.

These credentials are normally accessed only infrequently (on the order of daily) in order to generate X.509 Proxy credentials [15]. Proxy credentials are a Grid extension to identity credentials (standardized through the IETF) that allow a user to delegate their privileges to a temporary key pair. Proxy credentials are normally valid for a short period of time, typically 8 hours. This limited lifetime allows the proxy credentials to be less protected than the long-term identity credentials; they are typically stored on the local

disk protected with only local filesystem permissions. (The same technique is typically also used for Kerberos credentials.) The proxy certificate can then be used in the same manner as an identity certificate, enabling single sign-on by allowing the user to authenticate with the easily accessed proxy credentials until they expire and must be regenerated through an access to the identity credentials (requiring a pass phrase to decrypt the private key).

3   Integration of Grid Security and OTP

While there has not yet been a documented attack involving the unauthorized use of Grid credentials, there is concern that an attacker could gain access to a system containing a user's Grid credentials, make a copy of the encrypted private key, and install a Trojan application to gain access to the encryption pass phrase. In this section we present our approach to protecting against this and similar attacks while still allowing the science enabled by Grid security to progress.

3.1   Introduction of the Grid Credential Service

Original Grid deployments consisted of loose collections of collaborators who worked together without the benefit of production-quality Grid operations infrastructure. In these environments, many tasks, for example, the burden of credential management, fall to the users out of necessity. Several things have changed that make this model less ideal:

- With attacks on systems installing Trojans and other mechanisms for eavesdropping on keystrokes, there is a growing distrust of computers that are accessible by many users;

- Support for large Grid deployments has become more common, allowing for alternatives to user-managed credentials;

- As Grids have grown, user management of credentials has become a growing problem. Users have difficultly in managing credentials reliably, resulting in frustration on the part of the users, support issues due to lost credentials or forgotten passwords, and security concerns due to poorly protected credentials.

Because of these changes, we believe it is time to change the fundamental nature of how Grid credentials are managed, from a user-based model to a model based on Grid credential services that can be deployed and managed by professional administration and security staff.

The architecture of a Grid credential storage service is shown in Figure 1. The most important features of this architecture are the following.

- Users do not manage their own long-term credentials. Instead, they authenticate to the Grid credential storage service and receive back a credential.

- The service authenticates the user using the pluggable authentication module (PAM) [14], so that each deployment of the service can integrate with the authentication mechanism of choice.

- The service can either function as credential store, in which case it stores individual user credentials, or as an online CA, in which case it contains credentials that generate credentials for users as needed.

- The service returns a short-lived credential (either an identity credential or proxy credential) to the user to enable their access to the Grid. This credential is short lived (under administrative control of the credential service administrator, but expected to be typically 8 hours), after which time the user must contact the credential service again to obtain a new credential.
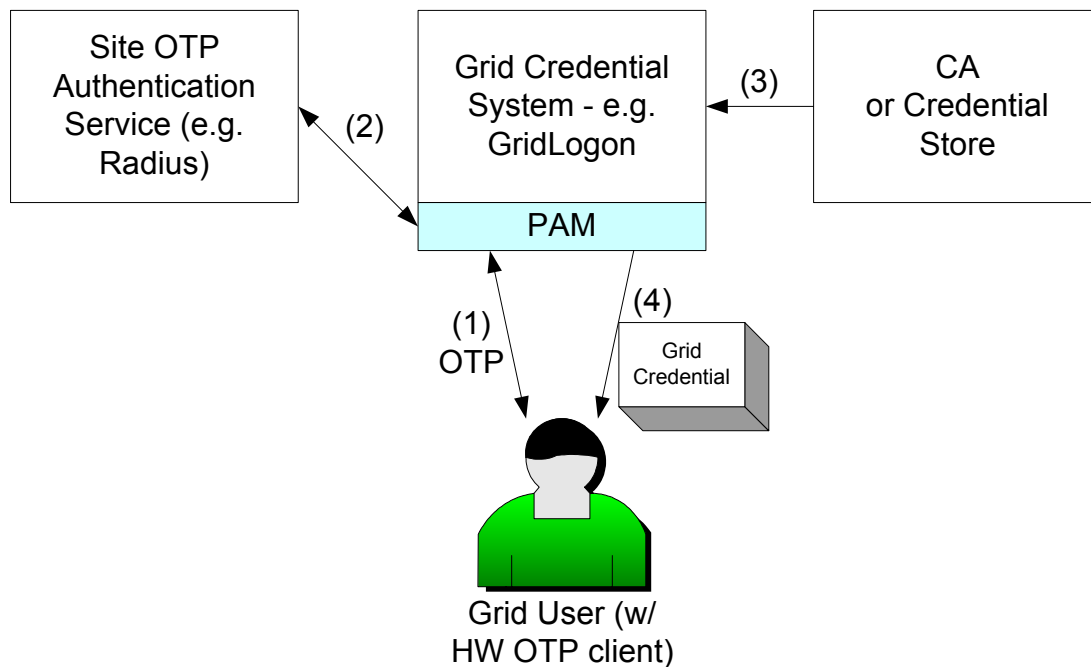

Figure 1: Architecture of a Grid credential system, of which our proposed implementation, called GridLogon, is an example. (1) User authenticates to the service using a one-time password. (2) Authentication is done through a pluggable authentication module (PAM) interface to an existing local authentication service. (3) GridLogon then generates a credential for the user by either accessing a credential store that houses the user's long-term credential or a CA credential. (4) The new credential is returned to the user.

We believe there are a number of benefits to this approach:

- It relieves the users from the process of acquiring and managing long-term X.509 credentials, a burdensome and error-prone process for most users.
- Relying parties typically have more trust in professional operations staff to manage long-term credential than users. A Grid credential service can be secured using similar techniques developed for similar services such as Kerberos KDCs.
- Accesses to the credentials can be audited and monitored to detect misuse during or after the fact.
- Since authentication is managed by the system, which can integrate it with existing systems, enforce local policies on strength, reuse, etc.

- Users can access their credentials from any location, granting a greater freedom of mobility, while avoiding the need to copy credentials in an ad hoc manner over the network (a potentially insecure process).
- If the user forgets their password, re-issuance of their credentials can be done automatically by the organization and the user is simply given a new password.

3.2 Implementation Plans

We will develop an implementation of a Grid credential service called GridLogon. GridLogon will be build on and extend the current MyProxy [11] service for credential management, which was developed at NCSA.

Initial efforts are underway at NCSA to produce a basic integration of PAM with MyProxy to form an initial implementation of GridLogon. This implementation will be evaluated at NERSC under the auspices of the DOE Science Grid in a testbed with an OTP-based Radius service [13].

After proving the validity of the approach in the NERSC testbed, development will continue to harden the implementation and extend MyProxy to support the online-CA model described in the previous section, in addition to its current holding of long-term identity credentials. We expect to have an initial version of GridLogon available in this Summer.

3.3 Credential Store versus Online CA

As we describe in Section 3.1, the design of the Grid certificate service allows it to operate as either an online CA or as store for user's long-term credentials. Our goal is also to allow for both of these modes of operation in our implementation of GridLogon (initially we will support the credential store mode due to ease of implementation due to existing code.)

We believe there are a number of pros and cons for each of these approaches and that each may be better suited to different deployments. Some highlights of the benefits of each are:

- The online CA approach allows for each of administration. There is only one set of credentials, which may allow for those credentials to be more easily protected in, for example, a hardware token.

- The online CA approach allows for the credential service to return X.509 identity certificates as opposed to a proxy certificate (in a similar manner to KCA [10]). This could allow for supporting a larger base of applications, such as web browsers.

- The credential store approach can allow for each credential to be encrypted by a different pass phrase that would have to be supplied by a user to obtain a credential. This would provide additional protection in case the system hosting the grid credential service was compromised.

3.4 Operation of a Grid Credential Service in Credential Store Mode

In this section we describe how a Grid credential service operates in the mode of being a credential store.
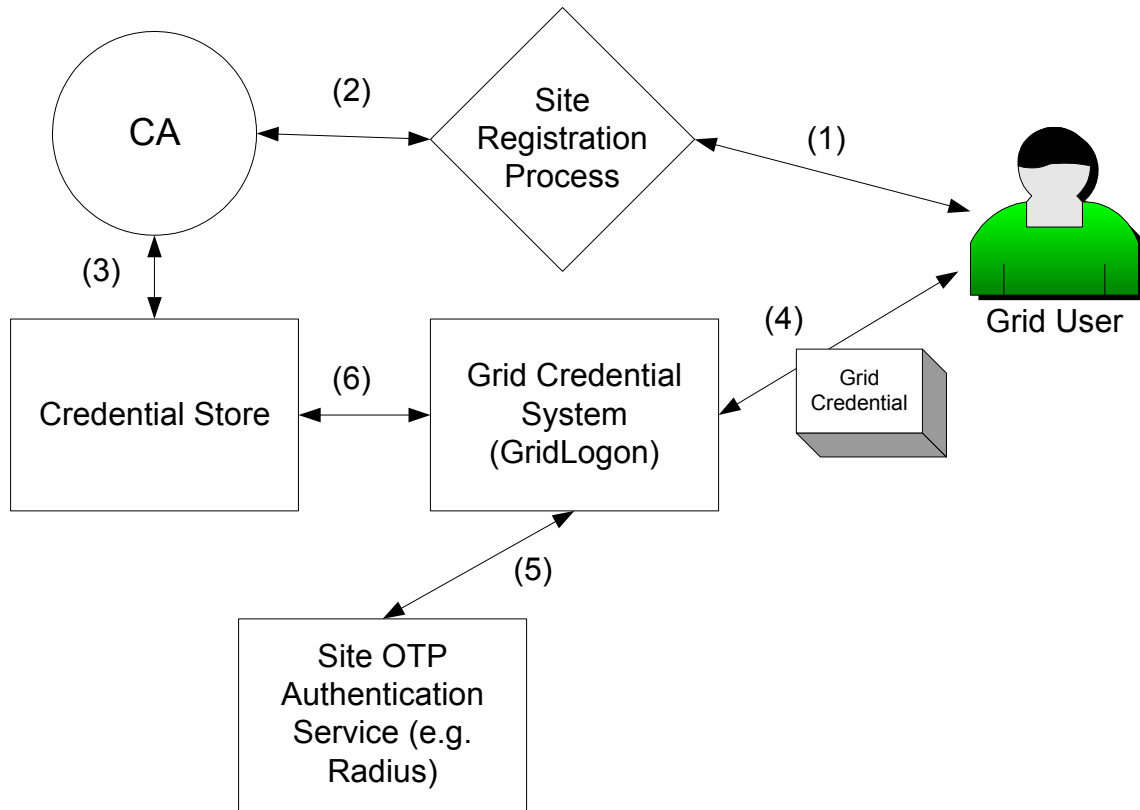

Figure 2: Operation of a Grid credential service in credential store mode. Steps are described in the text.

Figure 2 shows a Grid credential service operating as a credential store. In this mode of operation individual user credentials (i.e. long-term identify certificate and associated private keys) are stored in the service and users are issued proxy certificates from those credentials.

The steps shown in the figure include both the registration phase, which is typically done once, and then the user logon phase which is performed by the user on a routine basis. The registration phase steps are:

1. The user registers with the site through the site's normal new user registration process.

2. As part of the registration process, a CA at the site issues a set of credentials for the user.

3. These credentials are stored in the Grid certificate service credential store. These credentials may be encrypted at this point and the encryption pass phrase returned to the user.

We note that work has already been done to integrate the SimpleCA [4] package, part of the Globus Toolkit, with MyProxy to make this integrate of CA and credential store straight forward.

After registration the user will routinely contact the credential service to obtain a credential. The steps of that process are:

4. The user contacts the credential service and performs OTP authentication. If the user's credential is encrypted they would also need to provde the decryption key.

5. The credential service uses a locally deployed PAM module to verify the user's authentication with a local authentication service.

6. Having authenticated the user, the credential service accesses the user's credential and generates a proxy certificate which is returned to the user.

3.5 *Operation of a Grid Credential Service in Online CA Mode*

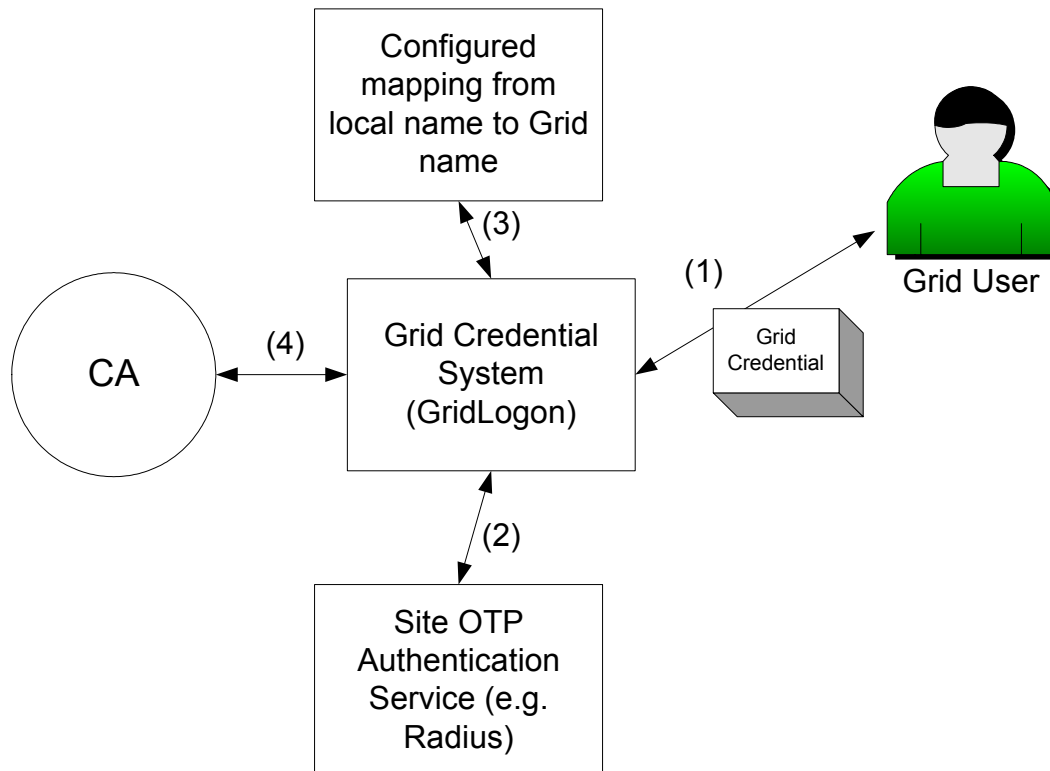In this section we describe how a Grid credential service operates in the mode of being a online CA.

Figure 3: Operation of a Grid credential service as an online CA. Steps are described in the step.

Figure 3 shows the operation of a Grid credential service in the mode of an online CA. In this mode, the Grid credential service has a set of CA credentials, which it uses to sign and issue credentials for users as requested. The steps of this process are:

Roadmap for Integration of Grid Security and One-Time Passwords

1. The user contacts the Grid credential service and performs OTP authentication.

2. The Grid credential service uses an authentication service through PAM to authenticate the user.

3. The Grid credential service uses a local configuration database to map the user's local identity to the distinguished name that should appear in their certificate.

4. The Grid credential uses the CA credentials to sign a certificate for the user and returns this to the user.

4 Cross-Domain Trust

Grid security is about enabling controlled access to resources across domains. One issue that will need to be overcome with Grid credential services is that relying parties must establish trust in these services in order to accept credentials issued by them. If these trust relationships fail to materialize, users will be forced to have credentials for each site they need access to. At best this will require the user to have a range of OTP logins and tokens and, at worst, will prevent the user for doing cross-site distributed computing to support their scientific goals. In either case distributed computing to support science will be greatly hampered.

We note that this is a non-trivial trust establishment process, one that greatly hampered cross-domain Kerberos deployment. While the establishment of the necessary trust relationships will not be an easy process, it is one that we believe can be overcome since there is strong motivation from all the parties involved – site security professionals and scientists alike. We see organizations such as the DOE Science Grid, the DOE Grids CA and the NSF TeraGrid project bringing together the interested parties already and providing the mechanisms by which these trust relationships will be established.

To further facilitate cross-site trust, we will support standardization in the Global Grid Forum methods for encoding the use of a Grid credential store in credentials it issues. This will allow a relying party to identify if a credential was issued by a Grid certificate service and the specific methods it used (e.g., online CA versus credential store, was a hardware storage module used).

5 Related Work

There are several similar efforts which have contributed ideas to the credential service model described in this roadmap and shown the effectiveness of the direction:

- Fermi National Laboratory (FNAL) has deployed a Kerberized Certificate Authority [8] in order to allow users to use their local Kerberos credentials to obtain Grid credentials when needed.

- The National Energy Research Scientific Computing Center (NERSC) has developed a prototype using MyProxy to store long-term credentials for users and deliver them to a user when needed [2].

- The Virtual Smart Card (VSC) [7] developed at SLAC holds user credentials in a similar manner.

- Peter Gutmann recently proposed and prototyped a "Plug-and-Play PKI" [5] to allow users to bootstrap all the trust information they need for a PKI from a single password.

Smart cards have emerged as a general method to allow users to be issued and securely carry X.509 credentials. However we note there are a number of issues that taken together significantly hamper their deployment in the multi-domain VOs this proposal addresses, namely: cost, difficulty of distribution, and ubiquity of hardware and software support. We also note solutions based on smart cards tend to be concerned with the application of those credentials towards document and email signing, which is not foreseen as a major use in Grids at this time.

6 Future Work

In this section we briefly discuss areas of future work and research for Grid credential services.

6.1 Supplying Security Configuration

In order to use user security configuration issues, it may be possible to have a Grid credential service return and install security configuration in addition to credentials. We envision the service returning a set of CA credentials which that the user should trust. The GridLogon client would then make sure this configuration was appropriately installed. This would enable true mobility and ease of configuration for the client.

6.2 Hardware Protection for Private Keys

There has already been investigation in using hardware devices in conjunction with MyProxy to increase the security of the stored credentials [Lorch paper]. We will continue to follow these efforts and seek to enable this integration of the Grid credential service and hardware credential storage.

6.3 Revocation

Since the Grid credential service is part of the process for issuing all credentials, it could be leveraged to help with revocation issues. We will seek to maintain sufficient audit logs on the Grid credential service so that there is sufficient information for revocation of credentials as those revocation capabilities become available.

6.4 Grid Logon Through SSH

Some Grid deployment may want to offer a mode of operations where users do not interact directly with a Grid credential service but instead use SSH to authenticate to a Grid site and obtain Grid credentials as part of their logon. To facilitate this we envision a PAM module to be used that would authenticate the user through the Grid credential service (which in turn authenticates to the site OTP authentication service).

7 Summary

We have presented a roadmap for the integration of one-time passwords with Grid security through the use of a Grid credential service. Implementation of the Grid credential service is underway and expected to be available this summer.

References

1. CCITT Recommendation, X.509: The Directory – Authentication Framework. 1988.

2. Chan, S., Grid Security at NERSC/LBNL, Globus Security Workshop, 2004. http://grid.ncsa.uiuc.edu/gw04-security/GW04-SecWkshp-nersc.ppt

3. Dierks, T. and Allen, C., The TLS Protocol Version 1.0, RFC 2246, IETF, 1999.

4. Globus Simple CA, http://www.globus.org/security/simple-ca.html, 2004.

5. Peter Gutmann, "Plug-and-Play PKI: A PKI your Mother can Use", Usenix Security Symposium, 2003.

6. Haller, N., Metz, C., Nesser, P., and Straw, M., A One-Time Password System, RFC 2289, IETF, 1998.

7. Hanushevsky, A., and Cowles, R., Mechanisms to Secure Grid Certificates, CHEP, 2003. http://chep03.ucsd.edu/files/81.ppt

8. KCA at FNAL, http://computing.fnal.gov/security/pki/KCA.html, 2003.

9. Kohl, J., and Neuman, C., The Kerberos Network Authentication Service (V5), RFC 1510, IETF, 1993.

10. Kornievskaia, O., Honeyman, P., Doster, B., and Coffman, K., Kerberized Credential Translation: A Solution to Web Access Control. 10th Usenix Security Symposium, 2001.

11. Novotny, J., Tuecke, S., and Welch, V., An Online Credential Repository for the Grid: MyProxy. Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10), IEEE Press, August 2001

12. OpenSSH, http://www.openssh.org, 2004.

13. Rigney, C., Rubens, A., Simpson, W., Willens, S., Remote Authentication Dial In User Service (RADIUS), RFC 2138, IETF, 1997.

14. Samar, V., and Lai, C., Making Login Services Independent of Authentication Technologies. Third ACM Conference on Computer Communications and Security, 1996.

15. Welch, V., Kesselman, C., Mulmo, O., Pearlman, L., Tuecke, S., Gawor, J., Meder, S., and Siebenlist, F., X.509 Proxy Certificates for Dynamic Delegation, PKI R&D Workshop, 2004.