The Cancer Biomedical Informatics Grid (caBIG^{TM}) Security Infrastructure

Stephen Langella[1], Scott Oster[1], Shannon Hastings[1], Frank Siebenlist[2], Joshua Phillips[3], David Ervin[1], Justin Permar[1], Tahsin Kurc[1], Joel Saltz[1]

[1]Department of Biomedical Informatics, Ohio State University, Columbus, OH;
[2]Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL;
[3]Semantic Bits, Reston VA;

Abstract

Security is a high priority issue in medical domain, because many institutions performing biomedical research work with sensitive medical data regularly. This issue becomes more complicated, when it is desirable or needed to access and analyze data in a multi-institutional setting. In the NCI cancer Biomedical Informatics Grid (caBIG^{TM}) program, several security issues were raised that existing security technologies could not address. Considering caBIG is envisioned to span a large number of cancer centers and investigator laboratories, these issues pose considerable challenge. In this paper we present these issues and the infrastructure, referred to as GAARDS, *which has been developed to address them.*

Introduction

The Cancer Biomedical Informatics Grid (caBIG^{TM}) (1) program is funded by the National Cancer Institute (NCI). It provides a coordinated approach to the informatics requirements of basic and clinical cancer research and multi-institutional studies. The goal is to accelerate the delivery of innovative approaches for the prevention and treatment of cancer by facilitating sharing, discovery, and integration of distributed information and analysis programs. Presently, the caBIG^{TM} community is made up of over 800 participants from over 80 organizations working together on more than 70 projects. It is expected that the caBIG^{TM} community will grow to hundreds of organizations and many thousands of cancer-research participants from geographically dispersed medical centers, universities, government agencies, and commercial companies. Security is a critical and challenging issue in caBIG^{TM} because of the scale of the program, the sensitivity of medical information, and the requirement to protect the intellectual properties of researchers, laboratories, and centers.

After evaluating existing security technologies, a caBIG Security Technology Evaluation white paper (2) was written. This white paper, along with numerous working groups within the caBIG^{TM} community, raised key security issues which were not fully addressed in existing systems and which became the motivation for the *Grid Authentication and Authorization with Reliably Distributed Services* (GAARDS) security infrastructure. In this paper we present these issues and describe the design and implementation of GAARDS.

GAARDS has been developed as a component of the caGrid (3) (4) infrastructure, the core Grid software architecture for caBIG^{TM}. caGrid is a service-oriented architecture that provides core services and toolkits for the development and deployment of community-provided services. It is built on top of Grid Services standards (5) using the Globus Toolkit (6). We should note that while GAARDS is motivated by the requirements of the cancer research community, the same or similar requirements are common in other fields of biomedical research in multi-institutional settings. Thus, we believe that the design principles and infrastructure of GAARDS can be employed in security support for a wide range of biomedical research scenarios.

Motivation for GAARDS

The caBIG security evaluation white paper has identified issues in three main areas: authentication and provisioning of user accounts, provisioning of a trust fabric, and authorization.

Provisioning of User Accounts. The Globus Toolkit (GT) implements support for security via its Grid Security Infrastructure (GSI) (7). GSI utilizes X.509 Identity Certificates for identifying a user. An X.509 Certificate with its corresponding private key forms a unique credential ("grid credential") within the Grid. Grid credentials are used to authenticate both users and services. Although this approach is very effective and secure, it is difficult to manage in a multi-institutional environment. Using existing tools, the provisioning of Grid credentials is done manually, which is far too complicated for users. The overall process is further complicated in the case where users wish to authenticate from multiple locations, because a copy of the user's private key and certificate has to be present at every location. Securely distributing private keys is error prone and poses a security risk. Additionally, there are scalability and efficiency problems with vetting user identities. Organizations invest a significant amount of resources into their existing identity management systems and already have processes in place for vetting user identities. In such settings, it would be more efficient to leverage existing identity management systems to provision Grid user accounts. Users would be able to use their existing credentials to "logon" to obtain Grid credentials and access Grid services. This scenario requires a mechanism to allow users to obtain Grid credentials using their existing organization-provided credentials. The mechanism should also remove the complications of using and managing Grid credentials. The GAARDS infrastructure provides this mechanism through a Grid service called Dorian (8); we will provide more details on Dorian later in this paper.

Management of Trust Fabric. In an environment where various credentials are issued by multiple authorities, another key security issue is determining which authorities to accept credentials from and at what level of assurance. In order to authenticate users and other peer-services, Grid services need to maintain a list of authorities that they trust to issue certificates and credentials. In a Grid environment, there may be hundreds of certificate authorities, each issuing thousands of certificates. Moreover, the Grid is a dynamic multi-institutional environment; certificates will be issued and revoked frequently and new authorities will be added regularly. Clearly a Grid-wide mechanism is needed to maintain and provision trusted certificate authorities, enabling Grid services and users to make authentication and authorizations decisions against the most recent trust information. The GAARDS infrastructure provides a Grid-wide trust mechanism called the Grid Trust Service (GTS) (9); more details on the GTS will be provided later in this paper.

Authorization/Access Control. Another key security issued is the need for scalable access control enforcement. It is critical that access control policy is maintained and enforced locally, giving data providers the ability to determine who has access to their data. At the same time, it is also important for scalability that access control policies be based on Grid-level information. Since most systems base their access control policies on membership to groups, a mechanism for organizing and managing groups spanning organizational boundaries is needed. The GAARDS infrastructure provides a service called Grid Grouper (10) to facilitate group management. It is anticipated that existing access control systems would be extended to base their access control policies off of groups managed by the Grid Grouper as well as the local groups that they currently maintain. The Common Security Module (CSM) (11) is an example of such a system. CSM is the access control system used by the caCORE Software Development Kit (12), the toolkit used in developing the majority of caBIG^{TM} applications. It can enforce access control based on groups maintained by the Grid Grouper and its local groups -- CSM has also been adopted in the GAARDS infrastructure as its native access control system.

GAARDS Infrastructure

The GAARDS infrastructure provides services and tools for the administration and enforcement of security policy in an enterprise Grid. Figure 1 illustrates the infrastructure. GAARDS is developed on top of the Globus Toolkit and extends its GSI component to provide enterprise services and administrative tools for: 1) Grid user management, 2) identity federation, 3) trust management, 4) group/VO management 5) Access Control Policy management and enforcement, and 5) Integration between existing security domains and the Grid security domain. GAARDS services can be used individually or in concert to meet the authentication and authorization needs. Below is a list of some of the core services provided by GAARDS:

Dorian (8)– A Grid service for the provisioning and management of Grid users accounts. Dorian provides an integration point between external security domains and the Grid, allowing accounts managed in external domains to be federated and managed in the Grid. It allows users to use their existing credentials (which may be external to the Grid) to authenticate to the Grid.

Grid Trust Service (GTS) (9)- GTS is a Grid-wide mechanism for maintaining and provisioning a federated trust fabric consisting of trusted certificate authorities, allowing Grid services to make authentication decisions against the most recent information.

Grid Grouper (10)- Provides a group-based authorization solution for the Grid. Grid services and applications enforce authorization policy based on membership to Grid-level groups.

Authentication Service - Provides a framework for issuing SAML assertions for existing credential providers so they may easily integrate with Dorian and other Grid credential providers. The authentication service also provides a uniform authentication interface upon which applications can be built.

Common Security Module (CSM) (11) - Provides a centralized approach to managing and enforcing access control policy authorization.

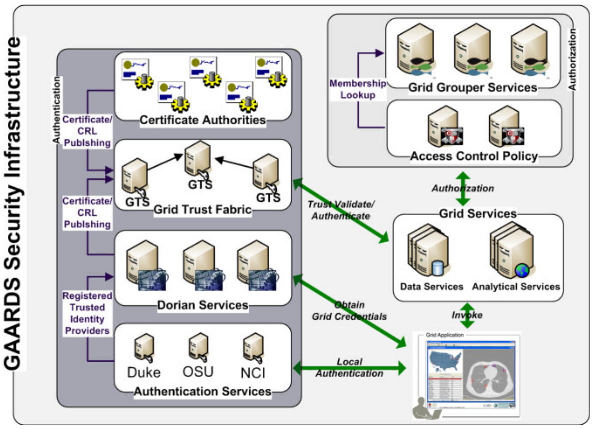

Figure 1 GAARDS Security Infrastructure

In order for users/applications to communicate with secure services, they first need Grid credentials. Obtaining Grid credentials requires having a Grid User Account. Dorian provides two methods to register for a Grid user account: 1) the user can register directly with Dorian, or 2) she can register indirectly via her existing user account obtained from a credential provider in another security domain. In order to obtain Grid credentials via an existing user account, the credential provider must be registered in Dorian as a Trusted Identity Provider. While some users unaffiliated with an existing credential provider will register directly with Dorian, it is anticipated that most users will use their existing local credentials to obtain Grid credentials. The advantages of this approach are: 1) users can use their existing credentials to access the Grid and 2) administrators only need to manage a single account for a given user. In order to provision Grid credentials, Dorian requires proof that local authentication succeeded, typically in the form of a SAML assertion (13). The GAARDS Authentication service provides a framework for existing credential providers to issue SAML assertions to Dorian. The authentication service also provides a uniform authentication interface upon which applications can be built. Figure 1 illustrates the process to obtain Grid credentials. The user/application first authenticates with their local credential provider via the authentication service and obtains a SAML assertion as proof of successful authentication. They then use the SAML assertion to obtain Grid credentials from Dorian. Assuming the local credential provider is registered with Dorian as a trusted identity provider and that the user's account is in good standing, Dorian will issue Grid credentials to the user. It should be noted that the use of the Authentication Service is not required; an alternative mechanism for obtaining the SAML assertion required by Dorian can be used. If a user is registered directly with Dorian, the user may contact Dorian directly to obtain Grid credentials.

After a user has obtained Grid credentials from Dorian he/she may invoke a secure service. The user presents her credentials to the secure service. The service then authenticates the user to validate the credentials. Part of the verification process is checking that the supplied Grid credentials were issued by a trusted Grid credential provider (i.e., Dorian or other certificate authorities). The Grid Trust Service (GTS) maintains a federated trust fabric of all the trusted digital signers in the Grid. Credential providers such as Dorian and other Grid certificate authorities are registered as trusted digital signers and regularly publish new information to the GTS. Grid services authenticate Grid credentials against the trusted digital signers in a GTS.

Once a user has been authenticated to a secure service, the service determines if the user is authorized to call the desired operation. Grid services have many different options available to them for performing authorization. The GAARDS infrastructure provides two approaches that can either be used independently or together. It is important to note that, in addition to these two approaches, any other authorization approach (i.e., user-developed authorization) can be used in conjunction with the GAARDS authentication/trust infrastructure. The first approach is group-based authorization provided by the Grid Grouper. In this approach, Grid services and applications enforce authorization policy based on membership to Grid-level groups. Assuming the groups are provisioned by Grid Grouper, services can determine whether a caller is authorized by simply asking Grid grouper if the caller is in a given group. The second approach is user-resource-operation authorization provided by the Common Security Module (CSM). In this approach, Grid services ask CSM whether a user can perform a given operation on a specified resource. Based on the access control policy maintained in CSM, CSM decides whether or not a user is authorized. In Figure 1, the Grid services defer the authorization to CSM. CSM enforces its group-based access control policy by asking Grid Grouper whether the caller is a member of the groups specified in the policy.

Dorian

Dorian (8) is a Grid user management service that 1) hides the complexities of creating and managing Grid credentials from users and 2) provides a mechanism for users to authenticate using their institution's authentication mechanism. Dorian implements a complete Grid-enabled solution, based on public key certificates and SAML, for managing and federating user identities in a Grid environment. Grid technologies have adopted the use of X.509 identity certificates to support user authentication. Dorian uses SAML authentication assertions as the enabling mechanism for federating users from local institutions to the Grid.

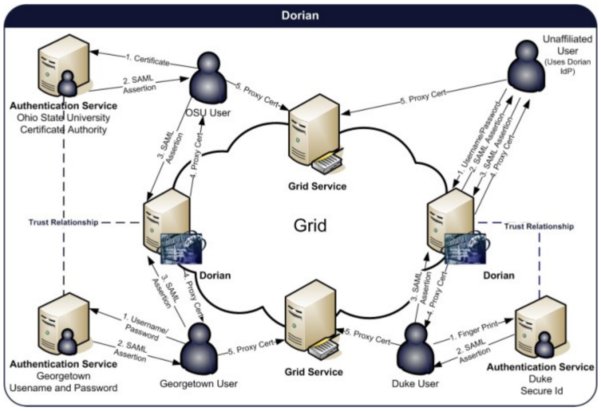

Figure 2 Dorian system

Figure 2 illustrates an example usage scenario for Dorian. To obtain Grid credentials or a proxy certificate, users authenticate with their institution using the institution's conventional mechanism. After successfully authenticating the user, the local institution issues a digitally signed SAML assertion, vouching that the user has authenticated. The user then sends this SAML assertion to Dorian in exchange for Grid credentials. Dorian will only issue Grid credentials if the SAML assertion is signed by a Trusted Identity Provider. For example, in Figure 2, a Georgetown user wishes to invoke a Grid service that requires Grid credentials. She supplies the application with her username and password. The application client authenticates the user with the Georgetown Authentication Service, receiving a signed SAML assertion which it subsequently passes to Dorian in exchange for Grid credentials. These credentials can then be used to invoke Grid services. To facilitate smaller groups or institutions without an existing identity provider (IdP), Dorian also has its own internal IdP. This allows users to authenticate to Dorian directly. This scenario is also illustrated in Figure 2.

Grid Trust Service (GTS)

In a Grid environment, the number of certificate authorities and the number of user identities can grow to be very large. Moreover, in a dynamic multi-institutional environment, the status of identities may be updated frequently. Identities and credentials can be revoked, suspended, reinstated, or new identities can be created. In addition, the list of trusted authorities may change. In such settings, certificate authorities will frequently publish Certificate Revocation Lists (CRL), which specify "blacklisted" certificates that the authority once issued but no longer accredits. For the security and integrity of the Grid, it is critical to both authenticate and validate a given credential against an accurate list of trusted certificate authorities and their corresponding CRLs. The Grid Trust Service (GTS) (9) is a federated infrastructure enabling the provisioning and management of a Grid trust fabric. The salient features of GTS are as follows:

1. A complete Grid-enabled federated solution for registering and managing certificate authority certificates and CRLs, facilitating the enforcement of the most recent trust agreements.
2. Definition and management of levels of assurance, such that certificate authorities may be grouped and discovered by the level of assurance that is acceptable to the consumer.
3. Due to the federated nature of GTS and its ability to create and manage arbitrary arrangements of authorities by level of assurance, it facilitates the curation of numerous independent trust overlays across the same physical Grid.
4. Client validation, allowing a client to submit a certificate and trust requirements in exchange for a validation decision, which allows for centralized certificate verification and validation.

Grid Grouper

The Grid Grouper (10) is a group/virtual organization management solution for the Grid supporting group-based authorization. Grid services and applications enforce authorization policy based on membership to groups defined and managed at the Grid level. The Grid Grouper is built on top of Grouper (14), which is an Internet2 (15) initiative focused on providing tools for group management. Grouper is a java object model which currently supports: basic group management by distributed authorities; subgroups; composite groups (whose membership is determined by the union, intersection, or relative complement of two other groups); custom group types and custom attributes; trace back of indirect membership; delegation. Applications interact with Grouper by embedding Grouper's Java object model inside the application. The Grid Grouper is a Grid-enabled version of Grouper. It provides a service interface to the underlying Grouper object model. Groups are then available and manageable to applications and other services in the Grid. The Grid Grouper provides an almost identical object model to the Grouper object model on the Grid client side. Applications and services can use the Grid Grouper object model much like they would use the Grouper object model to access and manage groups and enforce a group-membership authorization policy.

In Grouper/Grid Grouper, groups are organized into namespaces called stems. Each stem can have a set of child stems and set of child groups, with exception of the root stem which cannot have any child groups. For example, let's take a university compromised of many departments each of which has Faculty, Staff, and Students. To organize the university in the Grid Grouper, a stem would be created for each department. Each department stem would contain three groups: Faculty, Staff, and Students.

Conclusions

The GAARDS infrastructure serves as the core Grid security infrastructure for the caBIG program. It is motivated mainly by the requirements of basic and clinical biomedical research, in particular cancer research, in multi-institutional environments. Its design and implementation, however, is generic and can be employed in different application domains. It provides services and tools for the administration and enforcement of security policy in an enterprise Grid. GAARDS is under active development. We plan to add additional components and enhance existing components based on feedback and additional requirements from the community. One component under development is an authorization module for Globus' GridFTP server that allows GridFTP to utilize the GAARDS infrastructure to enforce access control. This security module, along with the caGrid BDT framework, will allow users to query Grid services and transfer the results of the query over the network very efficiently via GridFTP. We also plan to add support for auditing, provisioning of service/host credentials, directory services, and support for Grid workflows.

The GAARDS infrastructure was recently accepted as a Globus Incubator Project, setting it on a path for adoption into the Globus Toolkit. This will make GAARDS available to a wider community, which will also help drive the future direction and development of the GAARDS infrastructure.

References

1. *Cancer Biomedical Informatics Grid (caBIG).* [Online] https://cabig.nci.nih.gov.
2. **Daemer, Ken Lin and Gary.** *caBIG™ Security Technology Evaluation White Paper.* 2006.
3. *caGrid: Design and Implementation of the Core Architecture of the Cancer Biomedical Informatics Grid.* **Joel H. Saltz, Scott Oster, Shannon L. Hastings, Stephen Langella, William Sanchez, Manav Kher, Peter A. Covitz.** No. 15, s.l. : Bioinformatics, 2006, Vol. Vol. 22.
4. *caGrid.* [Online] http://www.cagrid.org.
5. OGSA - The Open Grid Services Architecture. *Globus.* [Online] http://www.globus.org/ogsa/.
6. *The Globus Toolkit.* [Online] http://www.globus.org.
7. *Security for Grid Services.* **V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, and S. Tuecke.** s.l. : IEEE Press, 2003. Twelfth International Symposium on High Performance Distributed Computing (HPDC-12).
8. *Dorian: Grid Service Infrastructure for Identity Management and Federation.* **Stephen Langella, Scott Oster, Shannon Hastings, Frank Siebenlist, Tahsin Kurc, Joel Saltz.** Salt Lake City, Utah : The 19th IEEE Symposium on Computer-Based Medical Systems, 2006.
9. *Enabling the Provisioning and Management of a Federated Grid Trust Fabric.* **Stephen Langella, Scott Oster, Shannon Hastings, Frank Siebenlist, Tahsin Kurc, Joel Saltz.** Gaithersburg : 6th Annual PKI R&D Workshop, 2007.
10. **Langella, Stephen.** *Grid Grouper.* [Online] http://www.cagrid.org/mwiki/index.php?title=GridGrouper:Main.
11. *Common Security Module (CSM).* [Online] http://ncicb.nci.nih.gov/infrastructure/cacore_overview/csm.
12. *caCore.* [Online] http://ncicb.nci.nih.gov/infrastructure/cacore_overview.
13. *OASIS Security Services (SAML) TC.* [Online] http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=security.
14. *Grouper.* [Online] http://middleware.internet2.edu/dir/groups/grouper/.
15. *Internet 2.* [Online] http://www.internet2.edu/.