Joint Policy Management and Auditing in Virtual Organizations

Timothy J. Smith and Lavanya Ramakrishnan

MCNC-RDI Research and Development Institute
3021 Cornwallis Road, PO Box 13910, Research Triangle Park, NC 27709-2889
tjsmith@anr.mcnc.org, lavanya@cnidr.org

Abstract

A major problem facing organizations using grid-computing models is the reluctance to participate in multi-organizational collaborative environments due to security concerns, such as unauthorized access, and fair resource usage. The Joint control of Virtual Organizations (JoVO) framework enables organizations to form a unified VO, with jointly agreed, knowable and enforceable security policies. The JoVO framework is based on the fault and intrusion tolerant joint control of identity, attributes, and access control policy through the use of threshold-based certification authorities. We propose a set of agents, the Credential Management Agent and Identity and Authorization Agent to aid grid services when operating in a multi-domain environment. One of the key areas of concern in grid computing is the assurance of all parties involved that security policies are appropriate and will be enforced. We propose an automated distributed audit agent framework consisting of white-box and black-box service testing for joint validation of access control policy.

1. Introduction

Organizations are increasingly using the grid-computing model to share and exchange compute resources and data within a single trust domain. However, organizations are reluctant to participate in collaborative multi-domain trust environments due to security concerns, such as unauthorized access, protection of intellectual property, and fair use of resources. Grid applications present a unique range of security issues that need to be addressed in the context of the virtual organization (VO) [11]. Current mechanisms allow organizations to control security policies for the resources they own, but it is often difficult to map some of the social and political arrangements that are associated with shared resources in a VO. Policy changes on one of the resources of the VO may indirectly affect the remaining. Timely detection of such changes and taking adequate measures to notify concerned parties and rectify them is important to maintain the quality of service to be assured in the VO.

Formal automated and augmented mechanisms for jointly controlled information assurance within the VO are critical in the grid infrastructure. The current information assurance and public key infrastructure has limited support for inter-organizational identity, authentication, and access control management.The JoVO framework secures the Virtual Organization infrastructure by - using threshold cryptography to provide joint control of identities, attributes and policy; real-time management of the security policies by an automated distributed audit agent framework; providing agents to allow applications to easily access the JoVO infrastructure.

The Joint control of Virtual Organizations (JoVO) framework is a first step towards enhancing multi-domain trust management. JoVO enables multiple trust-domains to form a virtual organization, with jointly agreed, knowable, and enforceable rules, to enable larger grid organizational topologies. The design is guided by three middleware design patterns: joint control of credentials and policies, proactive management of grid security policies, and separation of security policy from application logic.

Grid applications [1] need jointly controlled security management tools that enable easy mapping of existing security policies into secure collaborative environments like the VO. Participants of a VO like to be able to exercise control over the security state of the shared resources for the entire lifetime of the collaboration. One of the applications we work with is GridIR. GridIR is a system based on the Open Grid Service Architecture (OGSA) [9] framework, enabling complex information retrieval on the grid. The GridIR system consists of the following services: Metadata Services - to allow discovery and interaction with GridIR

[1]The material is based upon work by NASA under award No(s0 NAG 2-1467. Any opinins, findings, and conclusions or recommendations expressed in this material are those of teh author(s) and do not necessarily reflect the views of the National Aeronautics and Space Administration

services; Collection Management Services - to control collection, harvesting, including the ability to push and pull content based on collection events; Indexing and Searching Services - to build indices, including updates, from document collections, processing queries and producing results; and Query Processing Services - for distributed searching and results merging. A GridIR VO typically has multiple organizations with diverse security domains sharing information sources and physical resources. A GridIR VO has to provide at least the same level of information assurance associated with the information sources in a non-grid environment. When these services participate in a multi-organizational VO, credential and policy management become a daunting task for the application. Local mechanisms need to be aggregated with the agreed upon mechanisms in the multi-party VO. The administrators like to easily adapt existing security policies to the VO environment and want to be assured of the overall state of the system. In addition, some basic infrastructure is required to manage and maintain the activities and state of the VO. Dynamics of the VO in such systems are representative of some of the challenges in developing a secure grid-based collaborative environment. The JoVO framework facilitates grid services to operate in a virtual organization environment.

Research in developing the Grid Security Infrastructure [10] (GSI), has progressed alongside the evolution of grids in the last few years. GSI is based on public key encryption, X.509 certificates [5] and the Transport Layer Security (TLS) [8] communications protocol. Community Authorization Service (CAS) [18] adapts some of the concerns, arising in a VO, in a CAS server initiated by a community using its community identity that maintains the resource access policies in a database. Threshold cryptography enables mapping some of the VO's political and social arrangements with technological means. Threshold cryptography provides the means for joint control of credentials and a fault tolerant certification mechanism. Joint control at the granularity of the cryptosystem helps reduce some of the risks involved with secret or private key management. In addition there is very limited support right now on the grid for policy validation or administrative tools that can be used by the administrator to check the state of the VOs. The agent framework we propose helps the administrators to periodically check the security state of the system and be notified in real-time of any existing policies that may be violated over the lifetime of a VO.

The nature of dynamic coalitions or virtual organizations demands an infrastructure that supports heterogeneous machines and operating systems; scales to dozens of administrative domains with thousands of individual users; adapts quickly to changes in policy and to changes in availability of resources; and avoids centralized control and single points of failure. Yalta [7], a secure collaborative space for dynamic coalitions, demonstrates the basic ideas used to build a scalable, reliable application platform for formation, operation and management of secure dynamic coalitions required in environments where there is exchange of highly sensitive information. The project has developed three main technologies: a threshold RSA-based [13] certification authority (CA); an event-driven identity and access control policy management system; and a Jini virtual service gateway/firewall toolkit that provides interdomain brokering and policy enforcement for "security-unaware" services. JoVO builds on the idea of threshold RSA-based certification authority to establish and maintain secure collaborative grid environments.

JoVO (Figure 1) maintains the joint control of identity, attributes, and access control policy through the use of threshold-based certification authorities. A set of agents aid the OGSA services in using this infrastructure when operating in VOs. The Credential Management Agent handles the management and use of credentials for a service, so that the right credential is used at the right time. The Identity and Authorization (IdA) Agent handles complex authentication and authorization decisions, especially those used in longer-term relationships. The agents enhance the separation of security policy from application logic. One of the key areas of concern with distributed computing is the assurance of all parties involved that security policies are appropriate and will be enforced. We propose an automated distributed audit agent framework for joint validation of access control policy. We believe the JoVO framework will serve as a first step to removing security concerns of an organization participating in a VO.

2. Identity, Attribute and Policy Management in a Virtual Organization

JoVO facilitates rapid formation, management, verification, and termination of dynamic, secured, collaborative VOs and addresses policy issues that govern their collaboration. Member agencies, individuals, and their respective services can be integrated within a VO, with authorization controlled according to policies mutually agreed upon by VO participants.

Our security middleware framework enables precise levels of control over how shared services are used, including fine-grained and jointly controlled access control, delegation, and application of local and global policies. This framework, based on OGSA, will enhance the ability of organizations to jointly and dynamically create, offer, manage, and withdraw services with precise access policies. The joint control mechanisms allow for modeling and enforcing a variety of social-political arrangements, enabling technical administration controls to mirror and support the existing relationships. The ability to form complex durable

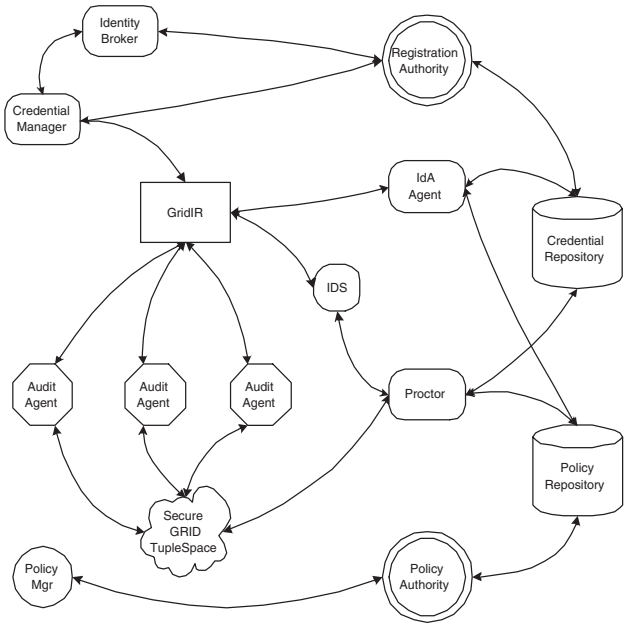

Figure 1. JoVO Component Architecture with GridIR Service as Example.

contracts between parties is crucial to modern life. Authentication and authorization decisions are one form of contract in grid computing. In most systems this decision is made for instantaneous time, to simplify implementation. Currently, in long-term situations the decision is made repeatedly, e.g. Is it true? Is it still true? etc.. This long-term pattern, though simple, complicates implementation, wastes resources, and creates greater coupling between application logic and security policy. The ability of a service to delegate this responsibility to an agent making and monitoring these types of contracts greatly reduces the complexity of a service. The design seeks to increase flexibility, robustness, maintainability and portability by abstracting the security policies out of application layers into middleware [19]. Our OGSA based design will help applications securely participate in VOs without changes to the application layers.

To enable dynamic policy within the VO, we propose an architecture composed of these major elements: Identity and Attribute Threshold Registration Authority(RA), Access Control Policy Authority (PA), and Certification Authority (CA); the credential management agent; the Identity and authorization agent (IdA agent) and its subscribing applications; the credential status protocol (CSP); and the SAML authentication protocol

2.1. Threshold PKI

Threshold cryptography is a technique for a number of parties to jointly generate and use an RSA public and private keypair. The RSA public key is a modulus N, which is a product of strong primes p and q, and a public exponent e. This is the same public-key formulation as a traditional RSA system. The public key is freely distributed, typically in the form of a digital certificate. Using the threshold RSA algorithm developed by Boneh and Franklin, [6, 13] none of the parties ever know the full private key or the factorization of N = pq, and each party holds a share of the private exponent d. A private-key decryption or digital signature can only be computed if a threshold number of parties contribute their share of the private key. This approach is fault-tolerant, because only t out of k shareholders are required to compute a signature. It is also intrusion-tolerant, because at least t shareholders must be compromised for an attacker to have the ability to use the private key.

Computing a signature with the Boneh-Franklin algorithm is easy and efficient. The participants each compute a partial signature, and those partial signatures are simply multiplied together to produce the complete signature. Key generation, however, is more costly than other approaches [20], because many trials may be needed to randomly generate a suitable public/private key pair. Using threshold RSA, we can trade off intrusion tolerance for throughput. By reducing the threshold, we can decrease the number of shareholders that must collaborate on a particular signature. By increasing the number of shareholders, we increase the number of signatures that can be computed in parallel. This decreases intrusion tolerance, however, because it decreases the number of shares that must be compromised in order for an intrusion to occur.

There are two main approaches to inter-trust domain credential usage, cross-certification of certification authorities and bridging certification authorities. We propose a threshold CA that will act as a bridge CA, using identity and credential mapping services from particular domains into the VO. The CA will create a durable and verifiable mapping with a VO credential. This will help reduce interoperability and trust relationship problems, so that VO entities only have to resolve and process VO credentials or policies. The identity, policy and attribute certification authorities will all be implemented using the threshold cryptography technique.

We propose a group of jointly controlled certification authorities to manage identity, attribute, and access control policy issuance in a VO. The identity and attribute registration authority (RA) will issue identity and attribute credentials to entities within the VO, after certification by the threshold/bridge CA. A small agent, known as an Identity Broker, allows an entity to request and receive VO identity

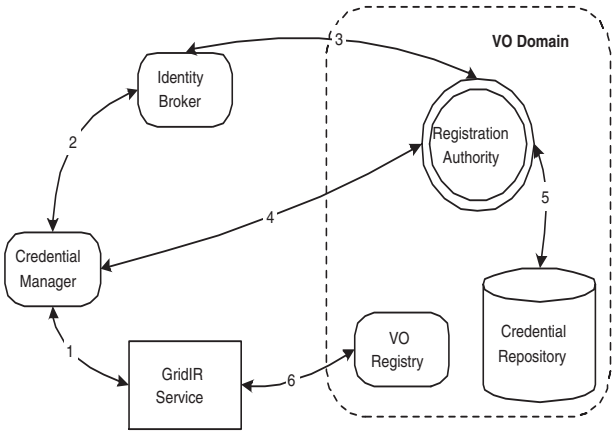

Figure 2. Credential Issuance and Registration components.[1] The GridIR Service delegates the Credential Manager to get a VO identity. [2] The Identity Broker agent helps the Credential Manager to request and receive VO identity from the Registration Authority (RA). [3] The Identity Broker bridges the gap between a local credential and a VO credential. [4] The RA and Credential Manager communicate through asynchronous messaging for credential issuance, renewal and revocation. [5] The identity for the service is stored in the VO's credential repository. [6] The GridIR service uses the VO identity to register into the VO's registry.

credentials via the RA. The access control policy authority (PA) validates and verifies access control policy within the VO, and passes the policy to the CA for certification. The policy proctor examines and monitors [22] entities in the VO for access control policy compliance through a set of distributed software audit agents. In addition to enabling joint control, these authorities will also be fault-tolerant and intrusion-tolerant.

2.2. Proactive Credential and Policy Management

The traditional model for PKI management is a simple request/response driven process. One of the key strengths of JoVO is the active management of keys, certificates, and revocation lists. This proactive style allows the use of shorter than traditional lifetimes for material, giving a reduction in the compromise footprint for the group, and scalable management of certificate renewal process. The coupling of an agent to manage end-entity credentials and the ability of the CA to message, schedule and task these agents creates a scalable public key management infrastructure.

The RA and credential manager would communicate through the proactive credential management (ProCM) protocol. The protocol describes asynchronous messaging for credential issuance, renewal, and revocation. Like traditional approaches, ProCM allows the credential managers to initiate requests to the RA. But more importantly, ProCM allows the RA to direct credential managers to apply for or renew credentials, allowing the RA to manage identity policy and schedule its workload.

2.3. Associated Data Stores

The certification authorities are associated with information stores for managing identity, attributes and policies. The key components of this back-end infrastructure are:

- Registry associated with storing the security meta-data about the services
- Identity repository associated with the certification authorities
- Policy and attribute repository to store the policy information

The registry of OGSA services, associated with storing the service descriptions, will be supplemented with the security meta-data registry to store security related information of the service. The certification authorities will publish and retrieve information from the identity and policy repository. These repositories could be indexed using tools for automatic dynamic index generation and these indices may be used to provide quick, easy access to policy information queries.

3. Dynamic Authentication and Authorization Management

Two key areas of information assurance are authentication and access control policy management. The ability to dynamically change, distribute, enforce, and validate these policies is the key to a robust VO. The proposed middleware components will be able to react and adapt to the changing policy environment. Credential and policy events will propagate through the JoVO installation, influencing interested components. The components will be able to influence each other, and the subscribing applications they support, asynchronously through OGSA event notifications. We utilize the idea of durable authentication and authorization decisions, the ability of the applications to specify conditions and constraints on a decision and have an agent monitor them for change during the specified lifetime.

3.1. Credential Management

With users and services participating in multiple VOs simultaneously, credential management [17] becomes a daunting task for the user. There may be associated with a user or service a multitude of identity and/or attribute certificates at a given time. Both the requestor and the service need to present the right credential for the right connection. Programmatic policy-based presentation of a credential will reduce administrative burden minimizing user intervention during service requests. The Java TLS implementation can be enhanced to support interaction with an authentication policy-based credential manager. The credential manager will use user and VO specified policies to present the appropriate credential for a particular session.

3.2. Credential Validation and Monitoring

Authentication decisions are based on identity, role, or attribute of an entity. Identity, role, and attributes are frequently derived from the presentation of signed digital credentials. These decisions can allow a long-standing session between the parties to be formed, such as a subscription. One of the key responsibilities of the CA infrastructure is to notify users when published certificates or policies have a change in status. One key certificate status change is revocation, which can happen for many reasons: change of information in the user's certificate, compromise of the user's private key, or even the compromise of the CA's private key. Another example of certificate status change is renewal, when validity periods are changed for the private or public key. Policies regarding access rights continually change in a VO. Often services require notification of policy changes relevant to their consumers.

The IdA agent supports credential validation and monitoring, and authentication and durable authorization policy determination. The IdA agent's functionality includes efficient validation of user credentials and real-time credential revocation notification. The IdA agent is a trusted service, controlled by the subscribing application's trust domain. The subscribing application delegates trust to the agent. The IdA agent will be able to support the caching of credentials and revocation notices to reduce the message traffic to the directory services. The query is processed against the revocation repository for validity. If the credential is not revoked and the client is interested in being notified of its revocation in future, the IdA agent needs to keep track of it and notify the client when the credential is revoked.

The IdA agent is both source and destination of Credential Status Protocol (CSP) notification events. It subscribes to an upstream publisher for notifications about credentials that it is interested in. This publisher may be a CA, or another agent. In turn, it accepts subscriptions from downstream and provides notifications to subscribers when changes to relevant credentials occur. The downstream subscriber may be an end entity or another agent. The CA signs and publishes certificate revocation lists and cryptographic heartbeats via the event notification framework of OGSA.

In the OGSA event notification framework, it is the application's responsibility to guarantee the reliable delivery of event notification. Moreover, the source can send the notification more than once if it is not convinced that the receiver has received it. Of equal importance is the authenticity of event notification. The recipient of the revocation event must be convinced that it is the CA that has originated the event notification. To address these concerns, we propose the CSP heartbeat message. The CA will issue a heartbeat message containing the current CRL serial number and current time along with a SHA-1/RSA signature of the CRL serial number and current time. Idempotency is achieved by means of a monotonically increasing sequence number derived from the timestamp.

The Credential Status Protocol (CSP) delivers status and revocation information through a subscriber/publisher mechanism. The protocol allows requesters to subscribe for the status of a particular certificate for a certain period of time. The publisher notifies the subscriber when any change occurs in the certificate status during that time period via CSP[21]. The CSP protocol addresses certificate status in general, and not just revocation, like Online Certificate Status Protocol (OCSP) [15], and is more efficient than the client-polling model used by OCSP or Simple Certificate Validation Protocol (SCVP)[14].

CSP uses the OGSA event notification framework to pass SAML-based event entries regarding security related information about attributes and certificate revocations. Use of SAML [4] in this case becomes extremely important, since the components of the messaging system like the certification authority act as bridge between their cross-domain counterparts. Traditional X.509 CRL-based certificate revocation is also supported.

3.3. Durable Authorization Decisions

The IdA agent will provide durable authentication decision support to a service. The IdA agent will provide this function using SAML assertion rules from the policy repository. The IdA agent builds a logical dependency chain of rules, used as the basis for the authorization decision. The dependency trust-chain for a credential used in the basis is straightforward to determine. The logical chain for an authorization decision involves a large graph traversal with many dependencies. The addition, modification, or deletion of any SAML rule can affect others. These tree graphs would be very useful to the policy authority to determine actual policy usage, or determining the impact of a policy

change on the organization.

The returned decision needs to be bound by a set of constraints, such as usage context or durability of the decision in all the positive, negative, and undetermined cases. The decision, coupled with the constraints, can be viewed as a reservation or contract with the service, using the policy decision point for load balancing, constraining, or reserving a system. If the basis for the decision were to change during its lifetime, subscribed applications relying on this decision would be notified of the change.

For example, a subscription service would take into account the lifetime of the access control decision in calculating the duration of the subscription to the service. In addition to policy rules, the IdA agent could use dynamic context, such as the load of the service host machine to determine authorization decisions. The IdA agent could deny a request and reply with the constraint that the service was overloaded. This would be useful information to the middleware layer of the caller, especially in the case of an asynchronous command; the layer could defer the command for a period of time, and retry the authorization.

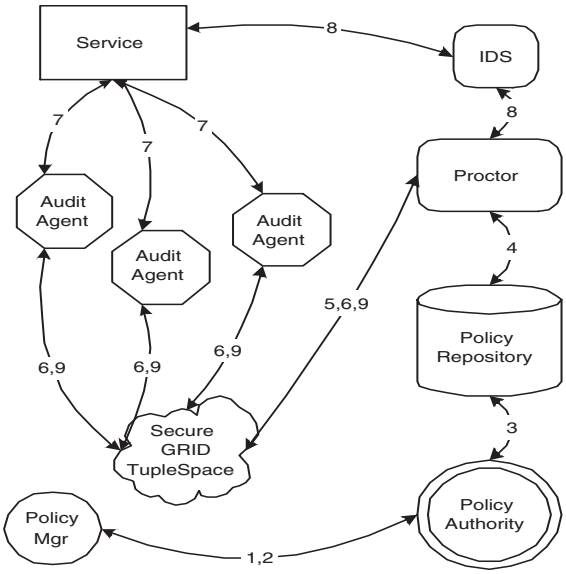

Figure 3. Policy Issuance and Audit Example

4. Grid Glasnost: Trust But Verify

One of the key areas of concern with grid computing is the assurance of all parties involved that security policies are appropriate and will be enforced. Given the complexity of grid systems, formulation of appropriate security policy is a challenge. This challenge becomes increasingly difficult over time as different individuals in different domains with different perspectives make changes to policy. Security policy changes that result in the loss of appropriate access by a system or user are usually discovered by the affected party and rectified by administrative personnel. Changes that result in inappropriate access to resources are usually not discovered in a timely manner, if ever. Inappropriate access control policy may be discovered only by an external audit. We propose an approach employed in software engineering, the use of unit, system, and integration tests to validate the correct function of an access control policy. A jointly controlled distributed agent framework for white-box and black-box service testing is used for joint validation of access control policy.

We believe that only through full lifecycle management of security policy will confidence be established in VO information assurance claims. We view uncertainty of information assurance as a primary inhibitor to wider usage of inter-organizational grid capabilities. We propose a suite of capabilities that will allow administrators to check, deploy, validate, and audit access control policy in the grid framework. An access control policy authority (PA) validates and verifies access control policy within the VO. The PA stores the signed policy in a policy repository. A policy proctor examines and monitors entities in the VO for access control policy compliance through a set of distributed software audit agents.

The distributed software audit agents would conduct tests, generated by the policy proctor, based on current authorization and access control policies. The agents would receive short-term credentials, necessary for the tests they are to conduct, from the threshold CA, via the ProCM protocol. For example, to test a role-based access rule, the proctor would schedule the agent to conduct a test during a certain time frame. The proctor would notify the RA, that certain short-term credentials with that role membership are needed by the agent to conduct validation tests during the test period. The proctor would then direct the agents to obtain the preapproved credentials. For very sensitive accesses, the proctor would direct the agent that a threshold-based RSA key be generated for the short-term credential, with the proctor holding one part and the agent holding the other part of the key. This would force the involvement of both parties in the use of that private key, preventing misuse and agent hijacking.

The proctor will generate, and the agents will conduct, both behavioral (black-box) and structural (white-box) testing of the grid infrastructure to ensure that it complies with the security policies deployed. General and specially written policy transformation modules, specific to a resource type, can generate validation test cases from these inputs.

We propose a three-phase testing approach: service deployment validation, service accreditation, and service policy audits. The first phase, service deployment validation, would involve the use of service specific white-box testing

to ensure the correctness of the service deployment. This would exercise major success and failure paths of a service, and would greatly aid administrators in discovering flaws in the deployment or integration with the host, network, or VO. These tests, ideally written by the service authors, could test the service in depth for correct function. The second phase, service accreditation, would involve black-box testing, that is, from a functional viewpoint, does the service respond as it should, given the current access control policy. This would be done with the proctor-generated tests executed by the distributed validation agents. A human inspector might also be utilized to validate the physical security aspects of the service installation. The inspection process would produce a certified accreditation attribute credential, utilized in service registration metadata, for requestors to inspect. The third phase, service policy audits, would again involve black-box testing of a statistically significant portion of the services on a regular basis to ensure that they continue to comply with current policy.

Figure 3 illustrates an example of actions resulting from a valid policy change. The policy manager for an entity (1) originates policy request to the PA. The PA evaluates the proposed policy using general and resource-specific logic for conflict with existing policy. The PA approves policy request, and (2) sends policy request reply to the policy manager, and (3) stores the signed policy to the policy repository. The policy repository (4) notifies subscribers, such as the proctor, of the new policy arrival. The proctor receives the signed policy, and programmatically generates validation tests from it. The proctor, through the tuplespace, (5) discovers the available audit agents, and then schedules selected validation tests with the agents. The audit agents (6) receive the validation tests from the proctor via the tuplespace. The agents then (7) conduct the tests against the service. The service (8) reports unauthorized accesses from certain validation tests to the intrusion detection system (IDS). The audit agents then (9) report validation test results back to the proctor via the tuplespace. The proctor conducts an analysis of the agent validation test results to determine if appropriate access was given to parties and access was denied to ineligible parties by the resource. Additionally, the proctor analyzes the IDS reports for accuracy of categorization of intrusions and responses relative to the current security posture. Finally, the proctor reports the results to the interested parties.

Audits will be both reactive and proactive. Some audits will be the result of policy changes; others will be conducted at random, to give a statistically valid survey of security stature and compliance of an administrative domain. One of the large research challenges is efficient joint scheduling of validation tests and sharing of results. When jointly controlled automated audits are part of the normative administrative process in a distributed system, inappropriate access control policy can be quickly discovered and rectified, without negative social and political consequences.

5. Security Context of OGSA Services

We believe that there are some characteristics of the security infrastructure that are tied to the service architecture, support of which will enable forming more secure VOs. The registry in OGSA maintains the references to the Grid Services. If some or part of a registry entry could be proof-carrying [16] signed entries, the authenticity of the registry information can be easily verified by OGSA clients.

The security information is an integral part of the registration meta-data. The security information could vary from coarse classification of security level of the service to access control information for the service. Clients may like to query the security attributes before requesting a task from the service. For example, negotiations during service registration may lead to assigning security levels of low, medium, or high with the service attributes. Thus a client would be able to perform queries of the type ”list all services providing service of type A, with at least a security level of medium”.

6. Related Work

There are different authorization systems that are used in the context of VOs and otherwise. PRIMA (Privilege Management and Authorization Services) [12] focuses on high-level attribute certificates with associated lifetimes to allow dynamic, short-lived collaborations to be formed. VOMS (Virtual Organization Membership Service) [2] from the European DataGrid project relies on ’Pseudo certificates’ returned from VOMS server to generate proxy certificates that contain information associated with roles of the user in the specific VO. Liberty Alliance [3] allows for single sign on capabilities between various web services based on a single network identity. JoVO allows users to use their local identities to access Grid services across various virtual organization spanning mulitple administration domains. It also enables the participants of a VO to exercise greater control on the security state of the system. This, joint-controlled framework when coupled with an agent framework that monitors the security parameters of such an environment, greatly reduces the risks of security threats and breaches

Shibboleth [1] is developing a SAML architecture to support inter-institutional sharing of web resources subject to access controls independent of specific implementation. It provides an easy mechanism for users to use their authentication information in the local domain to be authorized to use remote web resource. Our framework in contrast, allows various participants of the VO to exercise control over

the identity management of grid users. Shibboleth supports the policy based user credential management, where a user can specify which identities can be released to the target sites. We expand on this idea to allow various degrees of control to application code to manage user credentials for the user.

7. Summary

We presented here JoVO, a framework based on joint control of identity, attributes and access control in a virtual organization through the use of threshold based certification authorities. The automated distributed audit agent framework in JoVO helps assure all participants of the current security state of the virtual organizations and helps to monitor and alert administrators of possible security risks or breaches. Our initial experiments with threshold certificate authorities have proved its scalability, reliability and fault and intrusion tolerant capabilities. The Credential Management Agent and Identity and Authorization(IdA) aids OGSA services to adapt the JoVO framework by separting the security policy from the application logic. JoVO is a step towards minimizing multi-domain trust issues that hinder sharing of data and resources in a grid environment. JoVO provides the tools to form virtual organizations and helps maintain the level of information assurance jointly agreed upon in the virtual organization policies.

8. Acknowledgements

We would like to acknowledge the following people for contributing ideas, requirements and/or feedback: Daniel Stevenson, Dorcas Stapelton, Bonnie P. Hurst, Steve Thorpe, Kevin Gamiel, Greg Byrd, Krithiga Thangavelu, Stephanie Bryant, Xiaoyong Wu.

References

[1] Shibboleth Architecture Draft v05.

[2] Virtual Organization Membership Service(VOMS) Architecture.

[3] Liberty Alliance Version 1.1 Specification. November 2002.

[4] Security Assertion Markup Language (SAML) 1.0 Specification. *OASIS*, November 2002.

[5] C. Adams and S. Farrell. Internet X.509 Public Key Infrastructure Certificate Management Protocols. *RFC 2510, IETF*, March 1999.

[6] D. Boneh and M. Franklin. Efficient generation of shared RSA keys. *Crypto '97, Lecture Notes in Computer Science, Springer Verlag*, 1233:425–439, 1997.

[7] G. T. Byrd, F. Gong, C. Sargor, and S. T. J. Yalta: A Secure Collaborative Space for Dynamic Coalitions. *IEEE 2nd SMC Information Assurance Workshop, West Point, New York*, 2001.

[8] T. Dierks and C. Allen. The TLS Protocol Verson 1.0. *RFC2246, IETF*, January 1999.

[9] I. Foster, C. Kesselman, J. Nick, and S. Tuecke. The Physiology of the Grid: An Open Grid Service Architecture for Distributed Systems Integration. *Open Grid Services Architecture WG, Global Grid Forum*, 2.9(Draft), June 2002.

[10] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke. A Security Architecture for Computational Grids. *Proceedings of 5th ACM Conference on Computer and Communications Security Conference*, pages 83–92, 1998.

[11] I. Foster, C. Kesselman, and S. Tuecke. The Anatomy of the Grid Enabling Scalable Virtual Organizations. *International Journal:Supercomputer Applications*, 2001.

[12] M. Lorch and D. Kafura. Supporting Secure Ad-hoc User Collaboration in Grid Environments. *Proceedings of 3rd International Workshop on Grid Computing,Baltimore*, November 2002.

[13] M. Malkin, T. Wu, and D. Boneh. Experimenting with shared generation of RSA keys. *Proceedings of the Internet Society's 1999 Symposium on Network and Distributed System Security(SNDSS)*, pages 43–56, 1999.

[14] A. Malpani, P. Hoffman, and R. Housley. Simple Certificate Validation Protocol (SCVP). *IETF Internet Draft*, November 2000.

[15] M. Myers, R. Ankey, A. Malpani, S. Galpering, and C. Adams. X.509 internet public key infrastructure Online Certificate Status Protocol (OCSP). *RFC 2560, IETF*, June 1999.

[16] G. C. Necula and P. Lee. Proof-Carrying Code. *Proceedings of the 24th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages(POPL'97)*, 1997.

[17] J. Novotny, S. Tuecke, and V. Welch. 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.

[18] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke. A Community Authorization Service for Group Collaboration. *Proceedings of IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002*, 2002.

[19] L. Ramakrishnan, H. Rehn, J. Alameda, R. Ananthakrishnan, M. Govindaraju, A. Slominski, K. Connelly, V. Welch, D. Gannon, R. Bramley, and S. Hampton. An Authorization Framework for a Grid Based Component Architecture. *Grid 2002*, pages 169–180.

[20] V. Shoup. Practical Threshold Signatures. *In Theory and Application of Cryptographic Tehniques*, pages 207–220, 2000.

[21] T. J. Smith, G. T. Byrd, X. Wu, K. Thangavelu, R. Wang, and A. Shah. Dynamic PKI and Secure Tuplespaces for Distributed Coalitions. *DARPA Information Survivability Conference and Expo III*, April 2003.

[22] B. Tierney, R. Aydt, D. Gunter, W. Smith, M. Swany, V. Taylor, and R. Wolksi. A Grid Monitoring Architecture. *GGF Document*, GFD(1.7).