

Distributed Security Architectures

PI: Mary Thompson, LBNL

Abstract

The overall goal of this project is to provide assured, policy-based access control for computer mediated resources such as data archives and instrument systems, that operate in wide area network environments and for grid services such as remote computations, network monitoring, and resource discovery and reservation.

We propose to continue investigating and implementing practical solutions to the security needs of distributed systems based on the emerging PKI standards and implementations. In particular, to provide a modular authorization service that compares a requestor's authenticated X.509 identity certificate with a set of signed policy documents describing the access policy for the requested resource. These policy documents are created and maintained by stakeholders for the resource, independent of the resource server platform.

Current work focuses on integrating our authorization mechanism with the core of emerging standards such as the IETF's Transport Layer Security (TLS), the Grid Security Interface (GSI), WebDAV protocols, and Generic Authentication and Authorization interface (GAA). In order to facilitate Akenti's use by new and continuing applications the types of supported policies and the interfaces are being expanded.

Motivation

DOE scientific resources - instruments, data, and collaborations - that are accessed via open networks or as part of the DOE Science Grid require protection against unauthorized use. Our experience with collaboratory environments which span several administrative domains has emphasized the importance of having uniform cross-domain standards and procedures for setting and enforcing policy on resources. The current practice of using local access control files on each server machine does not scale to the number of machines and stakeholders that will participate in the next generation of collaboratories and grids.

Another requirement of Grid and collaboratory environments is the need for a user to delegate his access rights to processes that are running on his behalf. This need typically arises when a job that is executing on behalf of a user needs access to data or additional compute resources that are only available to the user. The program needs to present a proxy credential that securely identifies it as operating on behalf of the user. Current state of the art, supports unrestricted delegation in certain contexts, but the need for more restricted delegation and broader recognition of proxy certificates is clear.

Approach and Challenges

We have built a research prototype implementing a multiple stakeholder use condition and user attribute model of authentication. Called Akenti [7], it provides a flexible, easily managed mechanism, which strongly controls access to distributed resources, by widely distributed users. Akenti also addresses the issues raised when the resources are controlled by multiple stakeholders from different administrative domains. The stakeholders are the people with authority to grant access to resources and may be both physically and organizationally remote from the resource. Akenti makes access control decisions based on one set of digitally signed documents that represent the authorization instructions and another set that represent user attributes. Existing public-key infrastructure and secure message protocols provide confidentiality, message integrity, and user identity authentication, during and after the access decision process. Akenti enables stakeholders to remotely and securely create and distribute instructions authorizing access to their resources. .

Our experience using Akenti within the Diesel Combustion Collaboratory [5] and with other applications emphasizes several lessons. One lesson is that a major challenge in designing usable access control mechanisms is to balance the richness and extensibility of the features with the comprehensibility of the resulting access policies. If there is insufficient flexibility as to what can be expressed the stakeholder is unable to set his desired policy. If on the other hand there are too many features, he may set a policy and not understand clearly what access is allowed to what users. This motivates more research into policy languages including the ability to handle multiple policy languages, to clearly provide for role-based models of authorization and to allow for more dynamic policies. It is our belief that the best approach to the usability of rich policy languages is to provide the stakeholders with a wide variety of tools to set and test authorization policy.

Another lesson learned is the importance of having a standard definition and implementation of proxy certificates to allow processes to run with a user's credentials. This motivates the implementation of a new TLS record protocol [4] to create such certificates, changes to the path validation algorithms to verify chains of proxy certificates and to return the initiator's identity and extending the Akenti authorization mechanism to understand proxy certificates.

Goals

As stated above, the fundamental goal of the Akenti authorization system is to provide assured, multiple stakeholder control over distributed resources accessed by physically and administratively distributed users. This goal in turn requires distributed management of all information needed for access decisions. To achieve this end we use X.509 identity certificates generated and managed by multiple institutions to identify users; we use trusted third-party certification of user attributes; and we build on existing protocols for cross domain authentication such as TLS and GSI. If the Akenti authorization system is going to be useful to the community, it must meet the following goals:

- Be easily integrated with applications including those that require a light-weight authorization mechanism such as agent systems and secure group applications; Continue to support other DOE grid and collaboratory research environments and middleware.
- Provide a rich policy language and set of authorization models that allow authorization for sets of resources, individual objects and actions on objects.
- Present an easy to use interface for stakeholders to set and evaluate policy.
- Be capable of supporting emerging approaches like GAA [6], GSI [1], the newly designed delegation certificates [8], WebDAV [2,3] and XML policy certificates.

Milestones

- Year 1
 - Release version 1.1 of the Akenti libraries and certificate generators. This version is more robust and extensible code than version 1 and supports new, more flexible certificate formats.
 - Release the stand-alone server version of Akenti.
 - Have Akenti recognize delegated proxy X509 certificates.
 - Release an early version of GSI/SSL library support for the creation and acceptance of proposed IETF standard X509 proxy certificates.
- Year 2 and 3
 - Akenti will be integrated with GSI as an optional replacement for the Globus Map file.
 - Implementation of the TLS proxy delegation protocol that handles the trace delegation and restricted rights will be completed.
 - Further definition of the Akenti policy language proxy restriction will be done and the first implementation finished.
 - Support for additional dynamic and conditional policies as required by grid and collaboratory applications will be provided.
 - Further investigation of alternative certificate formats: e.g. signed XML, ASN.1 and PKIX Attribute Certificates will be undertaken.

Connections to other projects

Integrating Akenti with GSI will be done as part of the SciDAC National Fusion Collaboratory proposal to provide X.509 identity based authentication and policy based authorization for remote job execution and data access.

We will have a stand-alone Akenti server available on the DOE Science Grid nodes for Grid applications to use to as an option for authorization.

We are working with the Reliable and Secure Group Communication project at LBNL to provide authorization for members to join a secure communication group.

Akenti will be used in an SBIR phase 1 implementation of CoDeveloper, a CORBA-based tool to facilitate code development by collaborators in different administrative domains.

References

1. Butler, R., Engert, D., Foster, I., Kesselman, C., Tuecke, S., Volmer, J., Welch, V., "A National-Scale Authentication Infrastructure" IEEE Computer, 33(12):60-66, 2000.
2. Clemm, G., Hopkins, A., Sedlar, E., Whitehead, J. "WebDAV Access Control Protocol", draft-ietf-webdav-acl-04.txt
3. Goland, Y., Whitehead, E., Faizi, A., Carter, S., Jensen, D., "HTTP Extensions for Distributed Authoring -- WEB-DAV", IETF RFC2518
4. Jackson, K., Tuecke, S., and Engert, D., "TLS Delegation Protocol," Internet Draft draft-ietf-tls-delegation-01.txt, 2001, <http://www.ietf.org/internet-drafts/draft-ietf-tls-delegation-01.txt>
5. Pancerella, C., Rahn, L., Yang, C., "The Diesel Combustion Collaboratory: Combustion Researchers Collaborating over the Internet", Proceedings of ACM/IEEE SC99 Conference, November 13-19, 1999, Portland, Oregon, USA
6. Ryutov, T., Neuman, C. "Access Control Framework for Distributed Applications" IETF Internet-draft draft-ietf-cat-acc-cntrl-frmw-05.txt November 22, 2000
7. Thompson, M., Johnston, W., Mudumbai, S., Hoo, G., Jackson, K., Essiari, A. "Certificate-based Access Control for Widely Distributed Resources", Proceedings of the Eight Usenix Security Symposium, Aug, 1999
8. Tuecke, et.al., "Internet X.509 Public Key Infrastructure Proxy Certificate Profile", draft-ietf-pkix-proxy-01.txt, <http://www.ietf.org/internet-drafts/draft-ietf-pkix-proxy-01.txt>