Cardea: Providing Support for Dynamic Resource Access in a Distributed Computing Environment

Rebekah.Lepro
NASA Ames Research Center

Cardea: Providing Support for Dynamic Resource Access in a Distributed Computing Environment

Rebekah.Lepro
NASA Ames Research Center

Introduction

The environment framing the modern authorization process span domains of administration, relies on many different authentication sources, and manages complex attributes as part of the authorization process. Cardea facilitates dynamic access control within this environment as a central function of an inter-operable authorization framework. The system departs from the traditional authorization model by separating the authentication and authorization processes, distributing the responsibility for authorization data and allowing collaborating domains to retain control over their implementation mechanisms. Critical features of the system architecture and its handling of the authorization process differentiate the system from existing authorization components by addressing common needs not adequately addressed by existing systems. Continuing system research seeks to enhance the implementation of the current authorization model employed in Cardea, increase the robustness of current features, further the framework for establishing trust and promote interoperability with existing security mechanisms.

Framing the authorization problem

As system evolves, the need to control access to resources that belong to a system increases. Regardless of system complexity, authorization begins with an offline evaluation of each protected resource to determine requirements that must be satisfied for access to be granted to that resource [MUD01]. Traditionally, a long-term local identity represented a unique set of permissions to a single resource [HUM01]. With this model, authorizing each new user required the creation and configuration of a new local identity to represent the permissions particular to the new user. Although group authorization can significantly reduce the total volume of authorization data, it can only provide a common definition for identities, group or permission within an administrative domain [MIR01, PEA01]. As there is no correlation between the local identities in separate administrative domains, each domain must execute an authorization process regardless of whether the authorizations have already be granted in another domain. Further, executing appropriate authorization decisions within a local domain for an external user requires a common awareness of authorization data between the two participating domains {JOH01].

In efforts to achieve trusted and common representations for authorization data, in support of distributed authorization and related problems, several standards are currently maintained or are under development by both the World Wide Web Consortium (W3C)[W3C] and the Security Services Technical Committee of OASIS [OASIS]. These standards include the Security Assertion Markup Language (SAML)[SAML], the eXtensible Access Control Markup Language (XACML)[XACML] and XML Digital Signature Recommendation (XMLDSig)[XMLDSig]. Each of these standards defines a common language in XML for representing authorization data and providing framework support for transactions related to that data.

Cardea

Cardea is a distributed authorization system, developed as part of the NASA Information Power Grid [IPG01, FOS01, FOS02], which strives to reach several goals that are not satisfied by existing authorization solutions. The first goal is to separate local identity from authorization data in its distributed authorization model thus reducing exclusive reliance on preconfigured local identities to enforce authorization decisions. The second system goal is to facilitate standard authorization communication between domains by providing a standard representation of global identity and attribute data. Thus allowing each domain to retain control over the mechanisms it uses to provide security services such as authentication and secure communication channels. To accomplish these goals, Cardea dynamically evaluates authorization requests according to a set of relevant characteristics of the resource and requester rather than considering specific local identities. Potentially accessed resources within an administrative domain are protected by local access control policies, specified with the XACML syntax, in terms of requester and resource characteristics. Further, potential users are identified by X.509 Proxy Certificates [RFC3459, TUE01] but codified only according to the characteristics they can reliably demonstrate. The exact information needed to complete an authorization decision is assessed and collected during the decision process itself. This information is assembled appropriately and presented to the PDP that returns the final authorization decision for the actual access request together with any relevant details.

Cardea is currently implemented in the Java language as a set of independent components. Conceptually, the system contains a SAML Policy Decision Point (SAML PDP), one or more Attribute Authorities (AA), one or more Policy Enforcement Points (PEP), an Information Service (IAS), and an XACML Policy Decision Point (XACML PDP). Although all these components may be co-located on the same machine to use local communication paradigms, they may be distributed across several machines and their functionality exposed as web service portTypes. See Appendix A for a diagram of inter-component communications.

Communication between components is specified directly by the XACML and SAML standards, such as the request and response formats for obtaining information. Although XACML and SAML are transport independent, the initial implementation binds these protocols to the Simple Object Access Protocol (SOAP) v. 1.1 [SOAP]. Support for SOAP-based communication comes from the Java reference implementations of the API for XML messaging [JAXM] and utilizes the Apache Axis [AXIS] architecture as an engine to transmit SOAP messages atop the http and https communication protocols. The Axis engine extracts the raw SAML or XACML construct from a message payload and forwards to the appropriate endpoint, as configured. From this point, message content is treated as native SAML and XACML and is thus shielded from its method of delivery.

To preserve message integrity, the body of each SOAP message is signed using XMLSig before transmission to the intended recipient. Custom handlers specified for the request and response flows within Axis provide common mechanisms to sign and verify this content of independently of content generation logic. As each message is signed only after processing is complete, the native format of the signed content is opaque to the signing process. Therefore, no dependencies between signature and content must be supported.

Future Directions

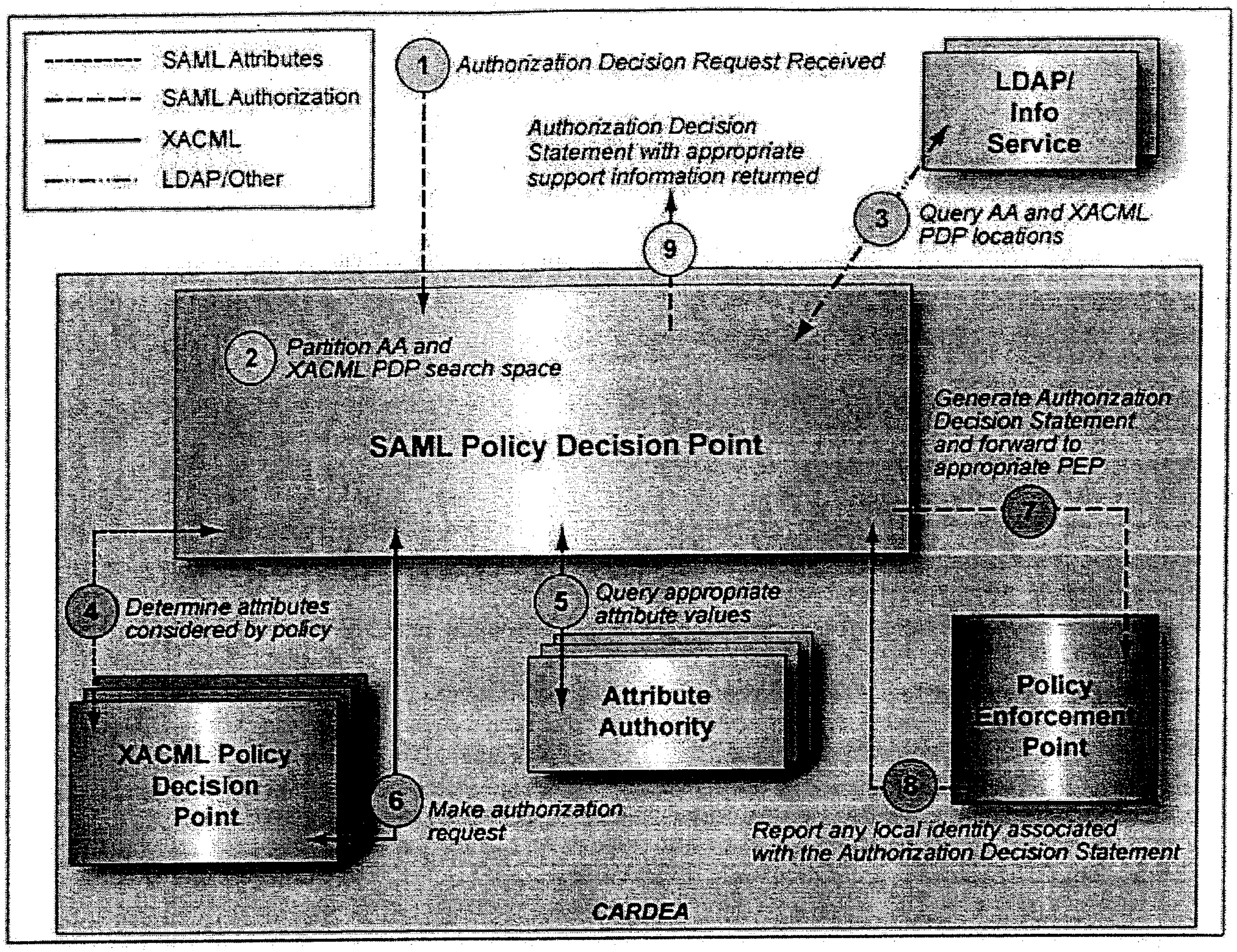
Work on the Cardea system will proceed in two complimentary directions. First, work will be performed on integrating basic system functionality into the existing NASA computing infrastructure. Integrating the functionality requires both interfaces to existing systems as well as modification on policies and processes to support the framework. During this development, work will focus on specific issues that offer stand-alone benefits rather than providing only a complete system at project end. The ultimate goal of this area is provision of authorization, dynamic session management and resource usage reporting capabilities. Providing any of these functions separately or in combination supports several scenarios that are not obtainable with existing resource access systems. The following tasks specifically concentrate on advancing existing system functionality rather than augmenting the current system with new capabilities.

- Define NASA access control policies using the XACML specification. Perform necessary infrastructure support work to ensure logic represented in the policies complies with governing NASA security policy. Determine and implement necessary security for the actual policy files.
- Build a trusted attribute authority to support IPG credentialed entities. Standard attribute definitions for each supported attribute within the authority must be established. This authority must integrate with existing NAS user management systems that already manage attribute values. Finally, the appropriate support framework for secure communications with the attribute authority must be developed.
- Expose each function as a standard grid services so that it may easily communicate with existing grid infrastructures and leverage their authentication mechanisms.

Any dynamic resource access system must also consider resource usage and allocations. Therefore, work to provide basic resource usage and allocation functionality will proceed in parallel to authorization work. Resource usage reporting will allow users and user administrators to query their previous usage as well as provide a framework to report consumption information to the hosting and home domain for each session.

Finally, authorization decisions must ultimately be enforced at the resource level. Therefore, coupling the new authorization functions with dynamic session management capabilities will support easier user accounting administration for a grid environment that supports constant change to resource and user populations. Thus, the final research goal is to develop or integrate with a dynamic session management system for authorization policy enforcement that relies only on authorization decision information rather than a unique identity for each potential user. Ultimately, the system will manage any local identities created to support an independently generated authorization decision. This ability, together with the resource accounting features outlined above provides the ability for cross-grid account-less access, assuming cross grid allocation issues are resolved. As this capability is still emergent, research this year will focus on investigating and evaluating solutions and their fit with existing authorization portions.

Appendix A



SAML Attributes
SAML Authorization
XACML
LDAP/Other
1 Authorization Decision Request Received
LDAP/ Info Service
Authorization Decision Statement with appropriate support information returned
9
3 Query AA and XACML PDP locations
2 Partition AA and XACML PDP search space
SAML Policy Decision Point
Generate Authorization Decision Statement and forward to appropriate PEP
7
4 Determine attributes considered by policy
5 Query appropriate attribute values
Attribute Authority
Policy Enforcement Point
XACML Policy Decision Point
6 Make authorization request
8
Report any local identity associated with the Authorization Decision Statement
CARDEA

Figure 1. The Cardea Architecture

References

[AXIS] http://xml.apache.org/axis, visited 2003-07-14

[FOS01] I.Foster, C.Kesselman, and S. Tuecke:
The Anatomy of the Grid: Enabling Scalable Virtual Organizations,
International Journal of Supercomputer Applications. 15(3); p.200-202. 2001.

[FOS02] Foster, I., Kesselman, C., Tsudik, G., and S. Tuecke: *A Security Architecture for Computational Grids.* ACM Conference Proceedings, Computers and Security, ACM Press, p. 83-91, 1998.

[HP98] Cheh Goh: *Policy Management Requirements*, Hewlett Packard Laboratories Technical Report, HPL-98-64, April 1998, http://www.hpl.hp.com/techreports/98/HPL-98-64.html.

[HUM01] Humphrey, M., Knabe, F., Ferrari, A. and A. Grimshaw: *Accountability and Control of Process Creation in Metasystems.* Proceedings of the 2000 Network and Distributed System Security Symposium (NDSS2000), February 2000.

[IPG01] The Information Power Grid - http://www.ipg.nasa.gov

[JAXM] http://java.sun.com/xml/jaxm/, visited 2003-07-31

[JOH01] Johnston, W. Mudumbai, S and M. Thompson: *Authorization and Attribute Certificates for Widely Distributed Access Control,* IEEE 7th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1998.

[MIR01] Miroslaw, K. Meyer, N. and P. Wolnieewicz: *Simplifying Administration and Management Processes in the Polish National Cluster.* Poznan Supercomputing Center, 2001.

[MUD01] S. Mudumbai et al: *Akenti A Distributed Access Control System.* Online at http://www-itg.lbl.gov/security/publications.html.

[PEA02] L. Pearlman et al: *A Community Authorization Service for Group Collaboration*, IEEE Workshop on Policies for Distributed Systems and Networks,2002.

[RFC2459] Housley, R., Ford, and D. Polk: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, IETF RFC, January 1999.

[SAML] Phillip Hallam-Baker, Eve Maler, et al: *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*, Oasis Standard, November 5th, 2002

[SOAP] Don Box et al: *Simple Object Access Protocol (SOAP) 1.1,* World Wide Web Consortium Note, May 2000

[TUE01] S. Tuecke et al: Internet X.509 Public Key Infrastructure Proxy Certificate Profile. IETF draft, 2001.

[XACML] Simon Godik, Tim Moses, et al: eXtensible Access Control Markup Language (XACML) Version 1.0, OASIS Standard, February 18th, 2003.

[XMLDSig] Mark Bartel et al: XML Signature Syntax and Processing, World Wide Web Consortium Recommendation, February 2002.