An Overview of Privilege Management Infrastructure (PMI)

Darren P. Mundy
University of Hull, UK

Oleksandr Otenko
Oracle Corporation, UK

PRIVILEGE MANAGEMENT INFRASTRUCTURE: AN OVERVIEW

Public key infrastructures (PKI) are now in place in a number of organizations and there is a vast amount of material available that can be used to obtain familiarisation with the concept (Adams & Lloyd, 2002; Raina, 2003). Although related to PKI, privilege management infrastructure (PMI) is a more recent development in the network security field. PMI has been designed to supply the authorization function lacking in the PKI model. This article will provide an overview of PMI, will provide a number of examples of present PMI architectures, such as PERMIS (Chadwick, Zhao, Otenko, Laborde, Su, & Nguyen, 2006), AKENTI (Thompson, Essari, & Mudumbai, 2003), and Shibboleth (Carmody, 2001), and will provide some examples of practical PMI usage.

WHAT IS PMI?

PMI can generally be thought of as the infrastructure supporting a strong authorization subsystem via the management and use of privileges (Adams & Lloyd, 2002). PMI is essentially a term used to encompass the management of authorization processes such as access control, rights management, levels of authority, delegation of authority, and so on. A PMI helps an organization to provide secure access to any target resource that they specify based on policy. A policy should detail such information as which users are allowed access to which resources, what actions they are allowed to perform, when they are allowed access, for example, time constraints, what privileges they need to be able to access the resource and carry out an operation.

Organizations need to be sure that access to their resources is controlled by a variety of security mechanisms, for example:

1. To ensure that the party requesting access is who they say they are (authentication);
2. That the party has sufficient rights to access the resource (authorization);
3. That confidential material is only read by those authenticated and authorized parties (privacy); and
4. That the transaction is monitored (audit and control).

PMI addresses only authorization. To address other points, corresponding subsystems should be deployed.

PMI ARCHITECTURES FOR TRUST ESTABLISHMENT

Prior to the introduction of privilege management infrastructures (PMI), access control systems trust only the “local” information they know about the outer world. This is very effective for small groups of people (e.g., multi-user Operating Systems). However, when the number of users willing to cooperate increases, such as in Grid situations or on the Web, it becomes more difficult to reflect all of the circumstances of the world locally. Dynamicity of relationships between the resource owner and the users accessing the resource also increases the difficulty of managing the privileges that each of the users has, limiting scalability of such systems.

To facilitate scalable solutions, trust in the people must be established in a distributed manner, and a means of distributing trust is required. This can be achieved in a number of ways. This section describes how this is done in three different PMI models. It starts with the approach adopted by X.509, and is followed by descriptions of the Akenti and Shibboleth architectures.

X.509

In X.509 PMI, there is a single root of trust, the Source of Authority (SOA). It stands for the owner of a resource, or an agent acting on his behalf. The SOA specifies the rules for establishing trust relationships, and access control rules. All such rules are written in the form of a policy, which governs the access control system. The SOA is also the ultimate authority in assigning privileges to end-entities, which will use the resource.

The SOA distributes the privilege to assign privileges to other entities, which are called Attribute Authorities (AAs), and the process of assigning this privilege is called delegation. These authorities, in their turn, may be allowed to assign privileges to end-entities, or delegate them further to other Attribute Authorities. Thus, the PMI forms a tree of authorities, with a singular root, which is the Source of Authority. The leaf nodes are end-users, who can only assert their privileges, and cannot delegate them to other entities.

The fact of assignment of privilege to an entity (either to AA or to an end-user) is noted as an X.509 Attribute Certificate (AC), which is a digitally-signed document, describing who has assigned what privilege to what entity. The privilege in such ACs is specified in the form of a privilege attribute that has to be interpreted by the access control system.

The access control system can discover trust relationships between the SOA (the resource owner) and the end-entities by obtaining their ACs and validating their contents using the policy written by the SOA. To achieve this, the access control system must obtain the ACs of the end-entity attempting access, the ACs of the Authority assigning the privilege to it (remember, that X.509 ACs specify who the grantor was), and ACs of all AAs that granted the privilege to do this to the authority, and to each of those AAs. Then the system needs to validate each of the assignments that occurred against the policy: If accepted, then the end-entity has been assigned a privilege in a trustworthy way, and an access control decision can be made; if the assignment of some privilege is not allowed by the policy, the privilege assignment is not trustworthy and should be discounted when making an access control decision.

In X.509, privilege assignment is valid if the granted privilege is a subset of all the privileges that the grantor has, the only exception being the Source of Authority, which can assign any privilege to any entity. To be able to make judgments if a granted set of privileges is a subset of the privileges that the grantor had, the privilege attribute values must have order. Some access control models (MAC, RBAC) naturally have ordering of privilege attribute values; other models may need enhancement (Otenko, 2004).

X.509 PMIs can span organization boundaries. This enables cross-organizational collaboration, important in environments where resource sharing is important, like in computational Grids and education. It is possible for Attribute Authorities in one organization to assign roles to its members, and for the Source of Authority in another organization to recognize the authority of these AAs to assign roles and place constraints on the extent to which this recognition of authority happens.

The X.509 PMI does not cover the questions of user privacy. Whereas the privileges of the user are his attributes, there is no mechanism to ensure unlinkability of the attributes and the real user. In fact, the PMI needs to be able to link the attributes to the end-user identity to make a decision. In X.509, the attributes are linked to the end-user by a cryptographically-protected Attribute Certificate, which makes the task of ensuring end-user anonymity particularly hard. It is important that some form of trust negotiation happens prior to exchange of any end-user attributes to ensure that the target system obtains only the attributes that it needs to make a decision.

To summarize, X.509 PMIs form a tree with the root in the Source of Authority, which is essentially the owner or the governor of the resource. Trust relationships are established by issuing X.509 ACs with privilege attributes to entities. The SOA writes a policy to which all the trust relationships must conform. In cross-organizational collaborations, the policy reflects the resource consumption agreement between the owner of the resource and the organizations that are using the resource. The rules for validating privilege assignments ensure that trust does not increase when it is distributed down the PMI tree away from the SOA. PERMIS is one of the implementations of X.509 PMI with Role-Based Access Controls (Chadwick, 2004).

Akenti

Akenti is an access control system that has been developed by Lawrence Berkeley National Laboratory, USA (Thompson et al., 2003). It implements a model of PMI that is somewhat different from the (traditional) X.509 model.