Role of Policies in a Distributed Trust Framework

M. Casassa Mont (mcm@hplb.hpl.hp.com)
A. Baldwin (ajb@hplb.hpl.hp.com)
C. Goh (cng@hplb.hpl.hp.com)

Hewlett Packard Laboratories – Bristol, UK

Abstract

The last few years have seen an explosive growth of the e-service offered over the Internet. E-service provision is evolving from a centralized model to a distributed and dynamic one. Identity, rights, non-repudiation, access control and QoS are extremely important aspects in such a distributed e-service framework. This paper briefly describes our distributed trust model that underpins the e-service framework and the role policies have within it.

1. Introduction

The last few years have seen an explosive growth of the e-service offered over the Internet. Furthermore e-service provision is evolving from a centralized model to a distributed and dynamic one [1]. In this new world, users go over the Internet to a series of outsourced e-services rather than to internal corporate services. It is up to the users to decide whom they trust or their companies may provide them with policies defining who to trust. Equally, services say trust me; to support this statement a service advertises its compliance with policies provided from a variety of sources to potential customers. A distributed trust model is needed to communicate trust properties [2] and control access between users and services. After a description of some aspects related to e-services, we briefly describe our distributed trust model and the role policies play within it.

2. E-Services

Whilst the emphasis of this paper is not on describing what e-services are or how they are realised [3] the aim is to clarify the trust relationship between such Internet-based services. Some assumptions are made about properties associated with e-services. Firstly, they are Internet enabled services accessible to users or other services. Secondly, it is believed that e-services will be composed and that the e-service will use other e-services to fulfil users' requests. Finally, trust is a two-way thing and the e-service must validate the user and, equally, it must present an identity [4] and trust credentials allowing the user to believe it can deliver the service.

3. Distributed Trust Model

The basic trust concepts that underpin our distributed trust model are "trusted third party" and "non-repudiation". This paper doesn't intend to describe "non-repudiation" in detail, but put simply it provides a long term proof of intent and it is implemented by standard PKI techniques. This section focuses more on the role of trusted third parties as certificate authorities (CAs), rights providers and policy providers (described in the next section).

In the e-service world each user or e-service is vouched for by other entities and trust is derived by finding mutually acceptable trust providers, for example, the standard CA trust hierarchies [5]. Each entity will have credentials [6] issued by "rights providers" that implies they have rights to 'do something'. Credentials are given by one entity to a user or a set of users (or service) and a third party e-service can check and potentially change them.

A user from a set of potential users accesses one of a set of e-services. To do this they contact an e-service who validates their identity using standard PKI techniques with an identity provider (a CA). An e-service can also

interact with other e-services in order to fulfil some tasks. We identify three basic mechanisms for communicating users' identities, rights and requests between these services: one service performs a task on behalf of another service; the secondary service allows the primary to act as a trusted proxy; or the primary service passes the users identity and credentials through to the secondary service.
The e-service provider establishes that a user is allowed to perform a task and in doing so asks the user to present a set of credentials or the e-service uses internal rights database. An e-service can check for combinations of the users' rights that fulfil access control conditions associated with a requested transaction. In this way the "rights framework" acts as a trust model whose definition is provided in a distributed manner with no controlling body. The e-service still has a local copy of the service side of the trust model defining which rights are required to access a particular e-service, as well as the appropriate enforcement mechanism.
The various mechanisms described above provide a way of distributing and executing a trust model; the next section describes the role policies have in our distributed trust model.

4. Role of Policies in our Distributed Trust Model

Policy [7] is a much-overloaded concept in network and system management; it is used to describe everything from the specification of corporate policies on computer use to a data driven configuration in a router. This paper does not aim to produce a definitive definition of policy but a definition is given to clarify the usage of the word.
Policy is a high level concept (in a traditional corporate environment this would be specified and understandable by high level manager) that is gradually refined into terms that relate more specifically to the actual infrastructure being managed [8]. In this way a policy is a constraint on how a system should work or how people should use the system. It is defined at a high level and refined so that it is meaningful in terms of the real systems and the various locations and organisations in which they exist [9]. Policies are governing the way a system works and as such they are relatively static with well-controlled procedures for change. In the terms being used, a policy need not be directly enforceable but should be a meaningful system constraint that is directly or indirectly measurable.
Policy forms an essential component allowing the management of e-services to be tied into a trust relationship. Policies can be used as a mechanism for enhancing trust within an e-service environment. An e-service takes on policies and must act in accordance with these policies. These policies are either the result of a trust relationship between two parties or they are specified requirements given by a third party enabling trust relationships to be established.
As a management tool policies are pervasive throughout an e-service framework specifying management constraints for all pieces of the framework. Policies are defined by a "policy provider" and disseminated to an e-service or user who can implement them as they see fit. Along with providing policy the policy provider takes on a responsibility to ensure that these policies are being met. Depending on the contract, they must either audit the policy recipient; or on a failure the policy provider must take some form of responsibility. Some examples where policies are used to define or aid in the definition of the trust are: policies constraining trust relationships; policy to constrain behaviour; policy on PKI usage and access control policy. Policies are not constrained to issues surrounding security; one of the richest areas for policy is in the management of quality of service. For example, QoS is one of the aspects that concur to build trust on an e-service provider.
In the traditional corporate IT world policies are designed by the MIS department and disseminated down through local IT departments to machine configurations and rules given to users. The new e-service world is considerably different in that there is no longer this hierarchical controlling force but instead there are many policy-defining bodies each of which are responsible for a small set of policies specifying very particular requirements.
Policies are used to specify constraints on the way users and services run their systems and the associated business functions. In doing this there are a number of, sometimes implicit, contractual agreements which should be enforced and provide an adequate system of redress. In the case of "regulators" who provide credentials, they sign and manage those credentials and in doing so they make certain guarantees to be responsible for some aspect of an entity's behaviour. They would expect the service to make guarantees to them that they will abide by the given policies and would probably have associated audit requirements. Each service would also have a number of local policies defined by their management as a tool to ensure the correct running of unregulated aspects of the service.

Policy enforcement mechanisms do not change between the traditional use of policy and this more distributed policy approach. There is a range of enforcement mechanisms from dictating the use of certain components to the configuration of systems to higher-level enforcement systems, such as for access control [10].

Each of the possible enforcement mechanisms relies on somebody correctly configuring the services and computer systems and as such audit becomes an essential part on any policy enforcement system.

5. Our work in the area

Our work in the area focuses on policy management [11] (policy representation, refinement and deployment), fine-grained access control at the service level [12], PKI and non-repudiation.

6. Conclusion

Policies can be used as a mechanism for enhancing trust within an e-service framework. Two major aspects were identified in our distributed trust model underpinning that framework: trusted third parties and non-repudiation. Third party can vouch for a certain aspect of an e-service by ensuring they meet a series of policies and then telling the world that this is the case. Trust can be established under this basis in that the fragments of expected behaviour are defined and there is a trail of responsibility in case of failure. Examples where policies are used to define or aid in the definition of the trust are: policies constraining trust relationships; policy to constrain behaviour; policy on PKI usage and access control policy. As a management tool policies are pervasive throughout an e-service framework specifying management constraints from various sources for all pieces of such a framework.

7. References

[1] HP E-Services (http://www.hp.com/e-services/index.html)

[2] Web Security: A Matter of Trust - World Wide Web Journal, summer 1997, Vol. 2, No. 3 – O'Reilly

[3] HP E-Services: e-Speak (http://www.hp.com/e-services/technology/index.html)

[4] Jalah Feghhi, Jalil Feghhi, Peter Williams - Digital Certificates: Applied Internet Security - Addison Wesley

[5] "ITU-T Recommendation X.509 (1997 E): Information Technology, Open System Interconnection, The Directory: Authentication Framework", June 1997

[6] Farrell, S. (1998) *An Internet Attribute Certificate Profile for Authorization*, IETF Internet Draft <draft-ietf-tls-ac509prof-00.txt> - August 20, 1998

[7] Sloman, M. (1993) *Specifying Policy for Management of Distributed Systems* - Proceedings of the 4th IFIP/IEEE international workshop on Distributed System Operations & Management (DSOM) 1993.

[8] Wies, R. (1995) *Using a Classification of Management Policies for Policy Specification and Policy Transformation* – Proceedings of the IFIP/IEEE International Symposium on Integrated network Management, Santa Barbara, CA, USA.

[9] Goh, C. (1997) *A Generic Approach to Policy Description in System Management*, Proceedings of the 8th IFIP/IEEE international workshop on Distributes Systems Operations and Management (DSOM)

[10] Sandhu R.S., & P Samarati (1992) A*ccess Control Principles and Practice*

[11] Baldwin A, Casassa Mont M, Goh, C. (1998) *POWER: Policy Wizard Engine for Refinement* – HP Labs Bristol

[12] Casassa Mont, M., Baldwin A. (1999) *Access Control System for Internet Services* - HP Labs Bristol