Using Trust for Restricted Delegation in Grid Environments

Wenbao Jiang[1], Chen Li[1], Shuang Hao[2], and Yiqi Dai[2]

[1] Department of Information System,
Beijing Information Technology Institute, No35 BeiSiHuanZhongLu,
Beijing, 100101, China
jiangwenbao@tsinghua.org.cn, lichen@biti.edu.cn
[2]Department of Computer Science and Technology,
Tsinghua University, 100084, China
haoshuang98@mails.tsinghua.edu.cn,
dyq@theory.cs.tsinghua.edu.cn

Abstract. Delegation is an important tool for authorization in large distributed environments. However, current delegation mechanisms used in emerging Grids have problems to allow for flexible and secure delegation. This paper presents a framework to realize restricted delegation using a specific attribute certificate with trust value in grid environments. The framework employs attribute certificates to convey rights separately from identity certificates used for authentication, and enables chained delegations by using attribute certificate chains. In the framework the verifier can enforce securely authorization with delegation by checking the trust values of AC chains, and judge if a delegation is a trusted delegation by evaluating the reputation value of the delegation chain. The paper discusses the way of computing trust and reputation for delegation, and describes some details of delegation, including the creation of delegation credential and the chained delegation protocol.

1 Introduction

Delegation is an essential tool of cooperation in distributed systems, especially in Grids that have emerged as dynamic, inter-domain, distributed computing environments [1]. Within Grids, A user must be able to delegate a service the ability to run on that user's behalf, so that the service is able to access the resources on which the user is authorized. For small ad-hoc collaborations with often only temporary existence, it is required that an entity can delegate a subset of its rights to another entity and the receiving entity can combine these rights with other delegated or own rights, so that the entities can share data, program and computational resources without the need for administrator intervention.

Delegation of rights always carries with it a risk of misuse; therefore, it is important to realize *restricted delegation*, which can minimize exposure by delegating the precise set of rights necessary for the task. Unfortunately, The conventional approach when a user must ask a service to perform some operation on her behalf is to grant *unlimited delegation*, which is to unconditionally grant the service the ability

Robert H. Deng et al. (Eds.): ISPEC 2005, LNCS 3439, pp. 293 – 301, 2005.

to impersonate the user. For delegations within a Grid, the crucial issue is the determination of those rights that should be granted by the user to the service and the circumstances under which those rights are valid. Delegating too many rights could lead to abuse, while delegating too few rights could prevent task completion [2].

The Grid Security Infrastructure (GSI) [3] is a security mechanism of the Globus Toolkit, which is widely used by Grid efforts worldwide. GSI realize delegation using *proxy certificates,* which may be used like standard X.509 identity certificates for authentication. GSI originally supported only unlimited delegation. The Community Authorization Service (CAS) [4] extends GSI delegation mechanisms by using *restricted GSI proxy certificates* [5] that allow for fine-grained control of delegated rights. The delegation mechanism using GSI proxy certificates supports impersonation, which allow entity A to grant to another entity B the right for B to authenticate with others as if it were A. This impersonation scheme is easy to integrate with many existing identity-based authorization systems. However, the impersonation scheme bears the danger of violating the "least privilege principle" [6], as it is often problematic to clearly define the minimum subset of privileges needed by the proxy. Moreover, the delegation approach using impersonation is unsuitable for some strong authorization mechanism, such as attribute-based authorization systems based on the use of Privilege Management Infrastructure (PMI) [7].

This paper focuses on the approach to realize restricted delegation based on attribute certificates with trust values, which allows for very flexible and secure delegation. The remainder of this paper is organized as follows. Section 2 introduces some definitions used. Section 3 gives a broad overview of our approach. Section 4 discusses the way of computing trust and reputation. Some details of delegation, including the creation of delegation credential and the chained delegation protocol, are described in Section 5. Finally, the conclusions are drawn in Section 6.

2 Definitions

A principal is a participant in a security operation; it is generally a user, a process operating on behalf of a user, a resource, or a process acting on behalf of a resource.

Delegation is the process whereby one principal grants the ability to act on its behalf to another principal. We focus here on the Delegation of rights, which assumes that a principal A has herself a set of rights, and it delegates all or a subset of them, to another principal B who can then act, instead of A, to exercise that particular set of rights. In a delegation we classify the participating principals as follows:

- The initiator, who is the originator of the delegation
- The grantor, also called the delegating principal, who delegates its rights to another principal
- The grantee, also called the delegated principal, who receives the delegation made by the grantor
- The verifier, also called "end point" or "end server", who enforces the authorization.
- The intermediary, who is a principal between the initiator and the verifier in the delegation.

Trust is an ambiguous concept that defies exact definition. This has given rise to an evident lack of coherence among researchers in the definition of trust [10,11]. For our purposes, however, we use the following definition by [10]:

Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity but rather it is subject to the entity's behavior and applies only within a specific context at a given time.

We use trust value (TV) as a trust metric, which is a dynamic value and spans over a set of values ranging from *fully trustworthy* to *fully untrustworthy*. In the paper we adopt a percentage as a trust metric, hence TV is a value between 0 and 1, 1 denotes fully *trustworthy,* 0 denotes *fully untrustworthy.*

When evaluating the trust value of an entity, we can rely on the reputation of the entity. The definition of reputation that we will use in this paper as follows:

The reputation of an entity is an expectation of its behavior based on other entities' observations or the collective information about the entity's past behavior within a specific context at a given time.

3 Overview

Our approach, illustrated in Figure 1, uses ACs as delegation tokens, and adopts AC chains to implement chained delegation, which is similar to the delegation model in X.509 PMI [7]. Rights are securely assigned and delegated to entities by embedding the rights in attribute certificates. The grantor of the right will sign the AC to the grantee. Every AC serving as delegation token includes a trust value (TV), which denotes trust degree that the grantor assigns to the delegation. Given the PKCs of the grantor and the intermediaries in the delegation path, a verifier (resource) can check by the AC chain if the grantor and the intermediaries are authoritative and determine whether the delegation is valid.

To illustrate the scenarios of delegation in Grid environments, Figure 1 depicts a virtual organization (VO) containing three domains. Each domain has a set of entities, including users, services, resources, and so on. Hence, we have introduced an implicit hierarchy based on entities, domains, and VO.

The SOA (Source of Authority) is the root of trust within a domain, and serves as the grantor and initiator in a delegation. For a chained delegation the SOA is the initial issuer of ACs that assigns privileges to privilege holders. It authorizes the privilege holder to act as a grantor, which further delegates that privilege to other entities through the issuance of ACs that contain the same privilege (or a subset thereof). The SOA may impose constraints on the delegation that can be done. A universal restriction on delegation is that no grantor can delegate more privilege than it holds. A grantor may also further restrict the ability of downstream grantors.

Each reputation service (RS) provided by the SOA is responsible for calculating the reputation values of other domains, and maintaining a dynamic reputation metric for entities within its domain. The verifier can enforce the authorization securely by check the reliability of chained delegation using AC chain's TV. The TV is built on reputation and direct trust relation between entities. The direct trust relation is computed based on DTT (direct trust table) maintained by each entity, and the

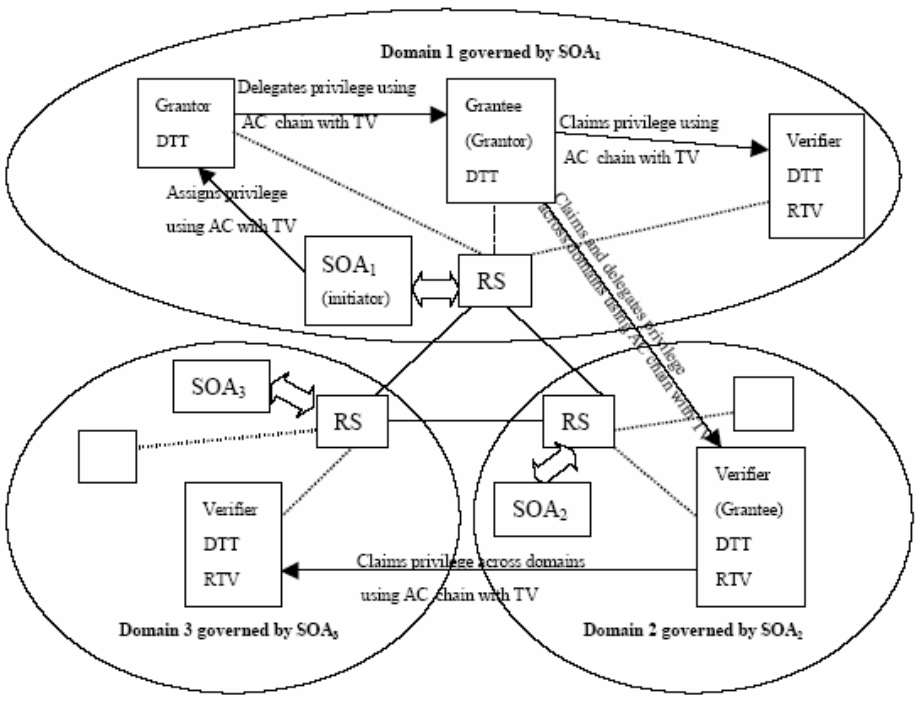

Fig. 1. The restricted delegation framework using trust in Grids

reputation is obtained from RS provided by SOA. When making trust-based decision to an access request, the verifier specifies an RTV (required trust value), and reject to access if the TV of delegation chain is smaller than the RTV. Similarly, the verifier may specify an RRV (required reputation value), which can be used to judge if a delegation is a trusted delegation by evaluating the reputation value of the delegation chain.

In order to realize trusted delegation, we employ a specific AC with TV for delegation, which has a different certificate structure from standard AC as defined in X.509 PMI. The main fields of our AC include:

- Issuer: the information identifying the issuer of AC, including the issuer and serial number of the issuer's PKC;
- Holder: the information identifying the holder of AC, including the issuer and serial number of the holder's PKC;
- Attribute: sets of rights (group membership, role, security clearance, or other authorization information) associated with the AC holder;
- ValidityPeriod: time periods when delegation is permissible;
- MaxPathLength: the maximum length of subsequent ACs chain in the delegation path;
- TrustValue: the trust degree that the grantor assign to the delegation
- SerialNumber: An integer value that uniquely identifies the AC within the scope of its issuer.

4 Computing Trust and Reputation

Azzedin et al. [10] have proposed that trust relationships in grid environments are based on a weighted combination of the direct relationship between domains as well as on the global reputation of the domains. We use the following notations as introduced in [10] to compute and envaluate trust for delegation:

- Let D_i and D_j denote two domains.
- Let $\Gamma(D_i, D_j, t)$ denote a trust relationship for delegation at a given time t of D_i towards D_j .
- Let $\Theta(D_i, D_j , t)$ denote a direct relationship for delegation at time t of D_i towards D_j .
- Let $\Omega(D_j , t)$ denote the reputation of D_j for delegation at time t.
- Let $DTT(D_i, D_j)$ denote a direct trust table entry of D_i for D_j. It is a table that records the trust value from the last transaction between D_i and D_j .

4.1 Computing and Evaluating Reputation

4.1.1 Computing the Reputation Value of Domains

The reputation value of domain D_j is computed as

$$\Omega(D_j, t) = \frac{\sum_{k=1}^{n} DTT(D_k, D_j) \times R(D_k, D_j)}{\sum_{k=1}^{n} (D_k)} \quad (1)$$

where $k \neq j$, $R(D_k,D_j)$ is the recommender's trust level.Since reputation is primarily based on what domains say about another domain,the recommender's trust factor $R(D_k,D_j)$ is introduced to prevent cheating through collusions among a group of domains. Hence, $R(D_k,D_j)$ is a value between 0 and 1 and will have a higher value if D_k and D_j are unknown or have no prior relationship among each other and a lower value if D_k and D_j are allies or business partners.

4.1.2 Computing the Reputation Value of Entities

Similarly, the reputation value of entities E_j within the domain is computed as:

$$\Omega(E_j, t) = \frac{\sum_{k=1}^{n} DTT(E_k, E_j) \times R(E_k, E_j)}{\sum_{k=1}^{n} (E_k)} \quad (2)$$

where $k \neq j$, E_K and E_j denote two entities within the domain. The meaning of other notations is similar to those in Formula (1).

4.1.3 Evaluating the Reputation Value of Delegation Chains

1) Delegation chains within a domain

Suppose the delegation path of a delegation chain is $A \rightarrow E_1 \rightarrow E_2 \rightarrow \ldots \rightarrow E_n \rightarrow B$, where A is the initiator, B is the verifier, and the others are the intermediaries within a domain. Then, the reputation value of the delegation chain is computed as:

$$RV\ (DC\ ,t) = \Omega\ (A,\ t) \times \prod_{j=1}^{n} \Omega\ (E_j, t) \tag{3}$$

2) Delegation chains across domains

Suppose the delegation path of a delegation chain is $A \rightarrow D_1 \rightarrow D_2 \rightarrow \ldots \rightarrow D_n \rightarrow B$, where A is the initiator, B is the verifier, and the others are the intermediaries across n different domains. Then, the reputation value of the delegation chain is computed as:

$$RV(DC,t) \ = \Omega\ (A,\ t)\ \times \prod_{j=1}^{n} \Omega\ (D_j,\ t) \tag{4}$$

4.2 Computing and Evaluating Trust

4.2.1 Computing Trust Value

The trust value (TV) of an AC denotes a trust relationship for the delegation of the grantor (E_i) towards the grantee (E_j). Hence, the TV is computed as:

$$TV = \Gamma(E_i, E_j, t) = \alpha \text{ x } \Theta(E_i, E_j\ , t) + \beta \text{ x } \Omega(E_j\ , t) \tag{5}$$

Where $\alpha, \beta \geq 0$, $\alpha + \beta = 1$. $\Theta(E_i, E_j\ , t)$ denotes a direct relationship for delegation at time t of E_i towards E_j, hence it can be computed as:

$$\Theta(E_i, E_j\ , t) = DTT(E_i, E_j) \tag{6}$$

$\Omega(E_j, t)$ denotes the reputation of E_j for delegation at time t. It can be computed as formula (2) if E_i and E_j are within a domain. We take the reputation of its domain (D_j) as the reputation of entity (E_j) if E_i and E_j are across different domains, in this way $\Omega(E_j\ , t)$ can be compute as formula (1).

4.2.2 Evaluating the Trust Value of Delegation Chains

Suppose the certificate chain of a delegation chain is $AC_1 \rightarrow AC_2 \rightarrow \ldots \rightarrow AC_n$, the trust values of certificates are as follows: TV_1 for AC_1, TV_2 for AC_2 , …, TV_n for AC_n. Then, the overall trust value of the delegation chain, expressed as TV(DC), is computed as :

$$TV\ (DC\ ) = \prod_{j=1}^{n} TV_j \tag{7}$$

5 Details of Delegation

As noted above, an AC serving as an delegation credential may defined as a signed 7-tuple:

$$DT_{xy} = <X, Y, P_{xy}, T_{xy}, L_{xy}, TV_{xy}, N_{xy}>_X$$

Where X denotes the AC's "Issuer", Y denotes the AC's "Holder", P_{xy} denotes the AC's "Attribute", T_{xy} denotes the AC's "ValidityPeriod", L_{xy} denotes the AC's

"MaxPathLength", TV_{xy} denotes the AC's "TrustValue", N_{xy} denotes the AC's "SerialNumber". $<M>_X$ denotes "M signed by X's private key".

Suppose $DT_{xy}=<X, Y, P_{xy}, T_{xy}, L_{xy}, TV_{xy}, N_{xy}>_X$ and $DT_{yz} = <Y, Z, P_{yz}, T_{yz}, L_{yz}, TV_{yz}, N_{yz}>_Y$ are two ACs of a AC chain, and DT_{yz} is a subsequent AC of DT_{xy} in the delegation path (X→Y→Z), then: (1) $P_{yz} \leq P_{xy}$, (2) $L_{yz} < L_{xy}$, (3) $T_{yz} \leq T_{xy}$. This is called three types of restrictions on the chained delegation.

5.1 Creating Delegation Credential with Trust Value

When a grantor (A) creates an AC with trust value, serving as an delegation credential, to a grantee (B), we can summarize the basic steps as follows:

Step 1: The grantor gets DTT(A,B) from her own DTT (direct trust table), then computed the direct relationship of A towards B, expressed as Θ(A, B, t), as in Formula (6).
Step 2: The grantor queries the grantee's reputation, expressed as Ω(B, t), from the RS in the grantor's domain.
Step 3: The grantor computes the Trust Value of the delegation, expressed as TV_{AB}, as in Formula (5).
Step 4: The grantor produces the delegation credential with trust value, DT_{AB}, by using her PKC to sign a 7-tuple containing TV_{AB} and other information as follows:

$$DT_{AB}=<A, B, P_{AB}, T_{AB}, L_{AB}, TV_{AB}, N_{AB}>_A$$

5.2 The Chained Delegation Protocol

Figure 2 shows an example of chained delegation, which the delegation path is SOA→A→B→C→S. It can be divided into four different delegation steps: (1) The initiator SOA assigns attributes to A, and initiates the delegation with A (SOA→A). (2) A delegates relevant privilege attributes to B (A→B). (3) B further delegates relevant privilege attributes to C (B→C). (4) C sends a request to server S (C→S). With the form of " sender → receiver: message ", these steps are described as follows:

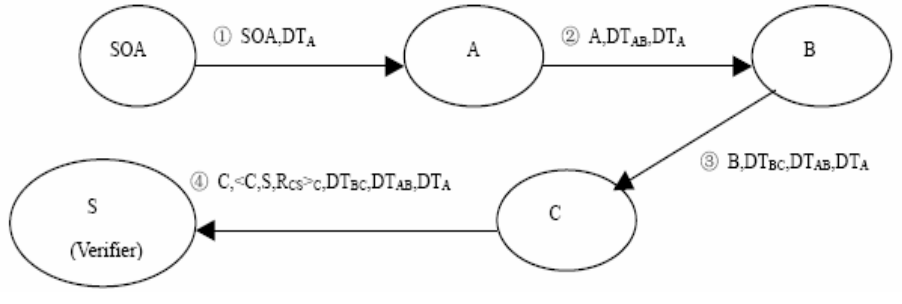

Fig. 2. A chained delegation process

Step 1: SOA→A: SOA, DT_A
Where
DT_A=<SOA, A, P_A, T_A, L_A, TV_A, N_A>$_{SOA}$

Step 2: A→B: A, DT_{AB}, DT_A
Where
DT_{AB}=<A, B, P_{AB}, T_{AB}, L_{AB}, TV_{AB}, N_{AB}>$_A$
DT_A=<SOA, A, P_A, T_A, L_A, TV_A, N_A>$_{SOA}$
Restrictions: (1) $P_{AB} \leq P_A$, (2) $0 \leq L_{AB} < L_A$, (3) $T_{AB} \leq T_A$.

Step 3: B→C: B, DT_{BC}, DT_{AB} , DT_A
Where
DT_{BC}=<B, C, P_{BC}, T_{BC}, L_{BC}, TV_{BC}, N_{BC}>$_B$
DT_{AB}=<A, B, P_{AB}, T_{AB}, L_{AB}, TV_{AB}, N_{AB}>$_A$
DT_A=<SOA, A, P_A, T_A, L_A, TV_A, N_A>$_{SOA}$
Restrictions: (1) $P_{BC} \leq P_{AB}$, (2) $0 \leq L_{BC} < L_{AB}$, (3) $T_{BC} \leq T_{AB}$.

Step 4: C→S: C, <C,S,R_{CS}>$_C$, DT_{BC}, DT_{AB}, DT_A
Where
DT_{BC}=<B, C, P_{BC}, T_{BC}, L_{BC}, TV_{BC}, N_{BC}>$_B$
DT_{AB}=<A, B, P_{AB}, T_{AB}, L_{AB}, TV_{AB}, N_{AB}>$_A$
DT_A=<SOA, A, P_A, T_A, L_A, TV_A, N_A>$_{SOA}$
R_{CS} denotes a request from C to S
Restrictions: (1) $P_{BC} \leq P_{AB} \leq P_A$, (2) $0 \leq L_{BC} < L_{AB} < L_A$, (3) $T_{BC} \leq T_{AB} \leq T_A$.

6 Conclusions

We present a framework to realize restricted delegation using a specific attribute certificate with trust value in Grid environments. The framework employs attribute certificates to convey rights separately from identity certificates used for authentication, and enables chained delegations by using attribute certificate chains. With separate credentials for privileges and identities, we can securely combine privileges from arbitrary sources and build a system that is based on the "least privilege principle", which is not supported by impersonation schemes, such as GSI proxy certificates. Furthermore, in our framework the verifier can realize secure authorization with delegation by checking the trust values of AC chains, and can judge if a delegation is a trusted delegation by evaluating the reputation value of the delegation chain.

References

1. I. Foster, C. Kesselman, and S. Tuecke, "The Anatomy of the Grid", *Intl. J. Supercomputer Applications*, vol. 15, no. 3, pp. 200-222, 2001
2. G. Stoker, B. White, E. Stackpole, et al, "Toward Realizable Restricted Delegation in Computational Grids", In *Proceedings of the International Conference on High Performance Computing and Networking Europe (HPCN Europe 2001),* Amsterdam, Netherlands, June 2001.

3. I. Foster, C. Kesselman, G. Tsudik, et al, “A security architecture for computational grids”, *In ACM Conference on Computer and Communications Security Conference*, San Francisco, 1998, pp. 82-89.
4. L. Pearlman, V. Welch, I. Foster, et al, “A Community Authorization Service for Group Collaboration”, *In IEEE Workshop on Policies for Distributed Systems and Networks*, 2002.
5. S. Tuecke, D. Engert, and I. Foster, “Internet X.509 Public Key Infrastructure Proxy Certificate Profile”, Internet Draft, August 2001.
6. J. R. Salzer and M. D. Schroeder, "The Protection of Information in Computer Systems", *Proceedings of the IEEE*, Sept. 1975
7. ITU-T Recommendation X.509 | ISO/IEC 9594-8: Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks .
8. RFC3281, An Internet Attribute Certificate Profile for Authorization .
9. Morrie Gasser, Ellen McDermott, “An Architecture for practical Delegation in a Distributed System”, *1990 IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, CA, May, 1990.
10. Farag Azzedin and Muthucumaru Maheswaran. “Evolving and Managing Trust in Grid Computing Systems”. In Canadian Conference on Electrical and Computer Engineering 2002, pages 1424–1429, May 2002.
11. A. Abdul-Rahman and S. Hailes, “Supporting trust in virtual communities,” *Hawaii Int’lConference on System Sciences*, Jan. 2000.