01

A SECURE MODEL TO ESTABLISH TRUST RELATIONSHIPS IN WEB SERVICES FOR VIRTUAL ORGANIZATIONS

E. R. Mello; M. S. Wangham; J. S. Fraga; R. J. Rabelo
Federal University of Santa Catarina – Department of Automation and Systems
PO Box 476-CEP 88040-900- Florianópolis(SC) Brazil
E-mail: {emerson, wangham, fraga, rabelo}@das.ufsc.br

This paper introduces a model making use of the security proposals based on Web Services architecture that aims to provide guarantees authentication and authorization transfer among different security domains. The model describes a flexible, scalable and secure way to establish trust relationships among Virtual Organization partners and to assign the access rights or roles to each partner in the VO. This model serves as a mediator for the interoperability among of security technologies that are found in a Collaborative Network.

1. INTRODUCTION

A large variety of Collaborative Networks (CNs) have emerged during the last years as a result of the challenges faced by both the business and scientific worlds, such as Virtual Enterprises (VE), Professional Virtual Community (PVC) and Virtual Laboratory (VL) (Camarinha et al., 2004). Within the CN scenario, cooperation in the form of Virtual Organizations (VO) represents a modern strategy which has been adopted by many enterprises, professionals and laboratories over the world to accomplish a given business opportunity, to take part in new markets and/or reach scientific excellence for innovative developments. Actually, a VO corresponds to a temporary set of independent organizations that share resources and skills to achieve its objective as none of them is able to attend to it alone The selection of the most suitable VO members has been often supported by partner's search and selection systems that are applied over a pre-defined group of organizations - a VO Breeding environment (as an evolution of the *cluster* concept).

However, despite this trend for collaborative works, most of organizations (companies and/or professionals) are still quite skeptic to share sensitive information when there is a need to collaborate with previously unknown partners. Actually, Collaborative network organizations demand the development of relationships with a broad range of potential partners each having a particular competency that complements the others. Therefore, the establishment of **trust relationships** among the partners is essential to the effectiveness of the VO Creation process.

The infrastructure to support the full life cycle of the VO in networked environments can be seen as a Services Oriented Architecture (SOA). A group of (web) services must attend different VO needs such as creation, operation and dissolution functionalities. It must also provide mechanisms to support coordination and collaboration functionalities, interoperable and secure information exchange, legacy systems integration, and so forth.

Collaborative Networks are usually characterized as an open, heterogeneous and large-scale system which makes a wide use of the Internet. In this way, there are some inherent advantages that make Web Services the ideal programming technology for building virtual organizations, which include: (1) it makes easy the integration and interoperability among different local systems; (2) it is based on well-accepted standards such as XML and HTTP; and (3) it provides services for discovering business partners to VOs. The Web Service's integrative feature allows existing VO applications, including legacy application, to be available and visible without any great cost being involved.

The management of distributed applications (such as VO applications) built according to the *Web Services model* is a great challenge. In a VO, since the companies' administrative boundaries get crossed, the involved applications will be under control of several security management, policies and mechanisms. Each security domain crossed by a distributed application can provide its own set of security credentials, based on its underlying security technology.

This paper presents an approach that aims at improving the trust on the infrastructure's services. It is seen as one of the necessary directions to reinforce the trust building process. The proposed model provides a flexible and secure way to establish trust relationships among VO partners as soon as it is formed as well as to assign the access rights / the roles to each partner in the VO. Its main goal is to deal with different security technologies and to allow the interaction among organizations that usually have their security services based on different technologies. This article describes an example in which three organizations are interacting, having domains based on different security technologies: X.509 PKI (ITU-T, 1993), Kerberos (Kohl, 1993), and SPKI certificates (Ellison et al., 1999), respectively. These technologies usually express identities and rights in a varied and non-interoperable way.

2. THE SECURITY MODEL

The following paragraphs illustrate a scenario where each organization in the CNO has a Web Services-based infrastructure to support the VO life cycle.

In Collaborative Networked (CNs), each organization can receive a business opportunity. Therefore, each one can become a Virtual Organization's Manager (VO Manager) and anyone can potentially be one of the VO partners. As soon as one organization is chosen to be a VO manager, it will search and select the partners. In the Web Service technology, the UDDI service (UDDI, 2002) can be used to locate these partners. UDDI has three registry types and each service (organization) can publish on it information about its functionality, capabilities and business area (e.g. molds, textile, automotive).

Once the partners have been selected, the trust relationships among them should be established. These relationships are essential to provide security guarantees such as authenticity, confidentiality and integrity of communication channels. In a CNO environment, each organization, including the VO manager, has its own security technologies and it is able to work only with them.

In order to enable a secure communication among the VO partners, a flexible solution would be to allow the VO Manager to establish trust relationships with its partners even if these partners use different technologies. Yet, the VO Manager could assign its roles in the VO by issuing a generic security token to each partner.

Figure 1 illustrates a CNO where the organizations are grouped according to security technologies. When a VO is going to be created as an answer to a certain business opportunity (BO), the involved organizations should support an interoperation among these technologies.

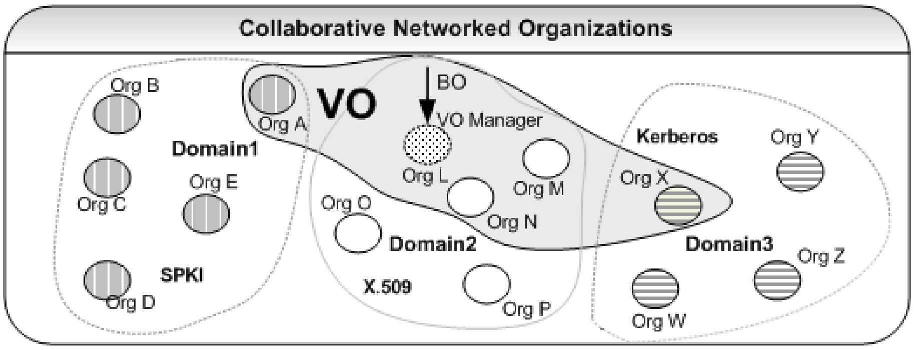


Figure 1 – A VO immersed in different security domains

In the proposed model, the infrastructure to support the VO is fully based on Web Services and its security specifications, such as WS-Trust (WS-Trust, 2004) and Security Assertions Markup Language (SAML) (OASIS, 2002). WS-Trust defines a Security Token Service (STS), which is responsible for issuing standard security tokens that should be understood by all CNO participants. In the present model, security tokens are represented by SAML assertions and used to establish the trust relationships among the VO partners. Access rights or roles to each partner in the VO are dynamically assigned by the VO Manager and expressed in SAML assertions. Therefore, it means that the security technologies present in the underlying layer is not important to the communications inside of a VO. In all communications in a VO the only security token used will be the SAML tokens issued by a VO Manager.

In the scenario depicted in Figure 1, the problem is that each partner has a different security technology. The VO Manager supports only X.509 and for all partners communicate with the VO Manager, should be necessary present tokens/certificates X.509. In addition to that, these tokens must be issued by an organization that the VO Manager trusts. The main difficulties are (1) locating the organizations that the VO Manager trusts, and (2) defining how the tokens/certificates will be issued. The next sections describe in detail the model that supports these tasks, by considering the components and services that will permit secure communication among organizations.

2.1 WS Domain in a CNO context

Security management in an environment composed of several types of organizations or professionals, each with different interests, it is hard work, mainly considering a large-scale environment. A classic way to facilitate the administration is to group individuals according to their skills and interests. An individual can belong to more than one group. In environments such as a CNO, the problem is how to organize these groups and the relationships among them.

Aiming at achieving scalability and hence being able to reach all the CN participants, groups must communicate with each other and trust relationships have to be established among themselves. These groups may be described in several ways, such as *federations*. In (Santin et al., 2003), (WS-Federation, 2003) and (Liberty, 2003), federations are proposed, whose objective is to group individuals who may have interests in common.

The trust model described in (Santin et al., 2003) is based on SPKI federations, and its objective is (1) to resolve chains of SPKI/SDSI authorization certificates (Ellison et al., 1999) and (2) the dynamic establishment of new chains of certificates. Federations must provide certificate repositories and support for certificate chain discovery. Scalability in this environment is achieved through associations among the federations (webs of federations). Such associations allow principals to carry out searches through these webs of federations, without having to join numerous federations. It is an equalitarian trust system which does not impose key hierarchy to gain in scale as those formed by X.509's PKI (Public Key Infrastructure).

The grouping of entities (services and clients) through federations, presented in the specifications (WS-Federation, 2003) and (Liberty, 2003), aims to reduce the complexity in the management of entities (names) of clients and service providers, however without requiring a central repository for storing these entities. Nevertheless, these proposals are negligent regarding the as dynamic establishment of trust relationships in heterogeneous and complex environments.

The proposed trust model is based on this concept of federation that, in this work, is called **WS Domain**. Each WS Domain is composed of a manager who groups its various affiliates according to their security attributes (credential, certificates, etc). The features of these managers depend upon the underlying security technology of the domain. For instance, if this manager is encapsulated in the SDSI/SPKI infrastructure, it becomes a simple repository of authorization certificates and names of this PKI. If this, on the other hand, corresponds to a Kerberos server, then the Ticket Granting Services of this server will be available through this manager. In other words, the manager of a WS Domain represents any PKI or security technology.

In any of these security technologies, the manager has control over the members and manages their joins and leaves, as members of the domains, as well as the queries performed by them. The WS Domain manager is a Web Service which makes possible the dynamic establishment of trust relationships. As parts of its functionalities, WS Domain manager provides the STS and XKMS (XML Key Management Service) (Ford, 2001) services.

The WS-Trust provides concepts, services and protocols which form the basis for the present trust model developed to cross management boundaries and security domains. The STS plays a fundamental role, mainly in the mediation of trust relationships involving two different security domains. The XKMS allows the localization and validation of keys, and works as an agent that makes the complexity of dealing with public key infrastructure transparent to the clients (organizations).

2.2 Trust relationships Intra-Domain and Inter Domains

After electing the most suitable VO composition, as showed in Figure 1, the VO Manager sends all participants a *challenge* aiming at mutual trust building between the VO manager and the VO members. In this model, the challenge is directly related with the security technology supported by VO managers. In the illustrated scenario, the *challenge* requires the participants present an X.509 certificate assigned by certification authorities which the VO manager trusts. In case a participant does not support the VO manager technology, the model provides means (1) to search the organizations that the VO manager trusts and (2) to negotiate the emission of security attributes required by the VO manager. Figure 2 illustrates the essential components and the steps involved in locating and negotiating security attributes.

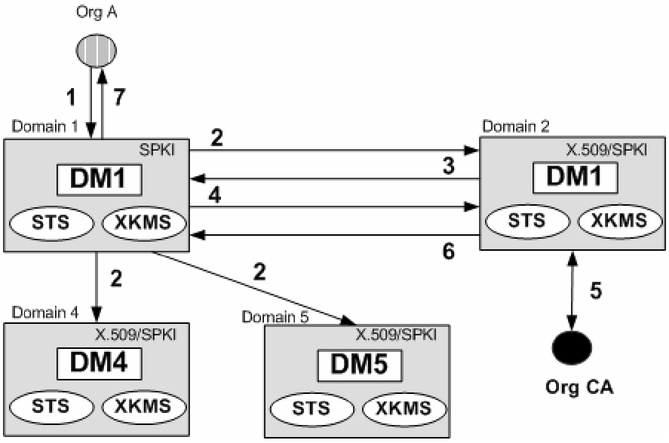


Figure 2 – Control flow for locating and negotiating security attributes

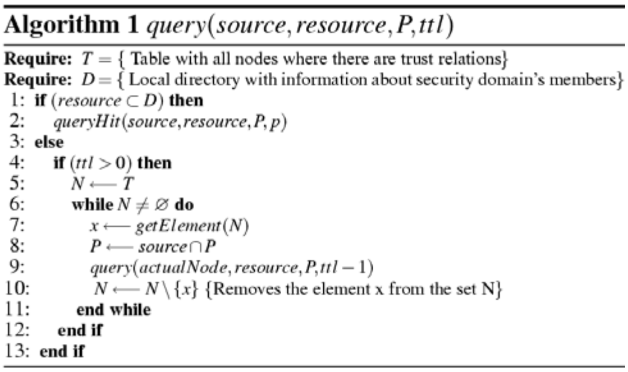
In the proposed model, the organizations have a passive role. Search and negotiation functionalities are available in its Domain Manager. Therefore, when *Org A* receives the challenge, this organization forwards it to its Domain Manager – *DM1* (**step 1**), which analyzes the challenge and verifies whether or not the requested security attribute (X.509 certificate) is supported by it. Then, *DM1* performs a search (a search heuristic as described in section 2.4) throughout the domains with which it has trust relationships, in order to find a trustworthy path which will lead it to the *Org CA* (**step 2**). *DM2* indicates, by replying to the query, that it has a trust relationship with *Org CA* (**step 3**). In **step 4**, *DM1* invokes *DM2*'s STS, by requesting an X.509 certificate (issued by *Org CA*) for *Org A*. After that, *DM2* forwards the *DM1*'s request to *Org CA* which replies a X.509 certificate (**step 5**). Hence, *DM2*'s STS issues a security token including the X.509 certificate (**step 6**). Finally, *DM1*, through its STS, provides *Org A* with all the necessary credentials so that *Org A* may respond to the challenge made by the VO Manager (**step 7**).

At this point, *Org A* did prove its identity, and then the VO Manager sends *Org A* a security token (SAML token) that will permit *Org A* to participate in VO. The steps illustrated in Figure 2, to the establishment of the trust in VO members, need to be executed to all VO members. When a VO member and a VO manager has the same security technology, this process is simplified because the interactions among Domain Managers are unnecessary.

After establishment the trust relationships with all participants, VO is fully formed. VO members' access control mechanisms are able to handle SAML tokens and implement a role-based access control (RBAC) (Sandhu and Samarati, 1994). Therefore, a VO Manager shall dynamically assign roles, expressed in SAML tokens, to each VO member and it sends all defined roles to all participants. Each VO member should map the VO Manager's roles into local roles.

2.4 Search Heuristic

In the case of the example illustrated in Figure 2, the manager of *DM1* wishes to locate, among the domains with which it has trust relationships, a trustworthy path that will lead it to *Org CA*. In the proposal in point, this search performed by the managers works similarly to the Gnutella protocol (Gnutella, 2001), which facilitates the navigation through the web of associates, in a way to achieve scale without requiring the manager to know all other likely partners in the web. The protocol which follows this model has two messages: *query*, which is used in the search for trustworthy path; and the *queryHit*, which informs that the path has been found. The algorithm shown in Figure 3 describes how the search for a path is performed, in this case the message "*query*".



```
Algorithm 1 $query(source, resource, P, ttl)$
Require: $T = \{$ Table with all nodes where there are trust relations$\}$
Require: $D = \{$ Local directory with information about security domain's members$\}$
if $(resource \subset D)$ then
    $queryHit(source, resource, P, p)$
else
    if $(ttl > 0)$ then
        $N \longleftarrow T$
        while $N \neq \varnothing$ do
            $x \longleftarrow getElement(N)$
            $P \longleftarrow source \cap P$
            $query(actualNode, resource, P, ttl - 1)$
            $N \longleftarrow N \setminus \{x\}$ {Removes the element x from the set N}
        end while
    end if
end if
```

Figure 3 – Query Protocol

The message *query* is comprised of four variables: (1) *source*, which indicates from where the request came; (2) *resource*, which describes which resource (target organization) needs to be searched; (3) *P*, which is a set containing the reverse sequence of all nodes through which the request passed; and (4) *ttl* which contains the lifetime for a search and thus limits its propagations. This prevents it from extending itself indefinitely.

A node (*p*), in this case a domain manager in the web, upon receiving a "*query*" message, verifies in its local repository (a set D of algorithm 1) if it has the "*resource*" searched and, if it does, sends a "*queryHit*" message to the node which originated the “*query*” message. Otherwise, a “*query*” message is sent to all the nodes (domains) with which it has trust relationships (set T, lines 6-11). For each new level that the “*query*” message descends, the value of “*ttl*” is decremented. With this heuristic it is possible to cover a great variety of nodes, without requiring a central repository to identify the existing trust relationships in a CNO.

3. RELATED WORK

Welch (2003) describes how to allow the dynamic creation of services as well as trust domains and has his application geared towards the Globus toolkit (a platform for grid computing architecture) (Foster and Kesselman, 1999). The security infrastructure specification for grid computing architecture assumes the integration with Web Services and benefits from the security standards, such as SAML and WS-Security. Some of the main security challenges present in grid computing architecture are shown as being the dynamics of the environment, since the service (resources) may be activated or deactivate dynamically during the life cycle of a resources-allocation session. This type of environment congregates several management and security domains, consequently different security technologies. In the proposal, security is provided as services, and is *The Credential Conversion Service* responsible for enabling different domains to communicate.

The security services described by Welch’s work are similar to the services used in our proposal. However, Wlech describes neither how trust relationships are established, nor how to locate, if necessary, possible trust relationships. In the present study, such questions are addressed and the use of the proposed in grid computing architecture could be adopted without great changes.

In (Foley et al., 2004), a security infrastructure for heterogeneous middleware is presented. To coordinate the trust relationships among the different systems, the Keynote (Blaze et al., 1999) was adopted, however the infrastructure also provides support to SPKI/SDSI. The authorization policies of each middleware are coded in Keynote certificates and vice-versa. This allows heterogeneous security domains to be crossed, serving as the basis for a decentralized support of security policies. The work details the advantages of the systems which are based on the concept of trust management (Blaze et al., 1999) on systems which use the X.509.

Foley's objective is to cross the limits imposed by technologies through Keynote certificates. The present model seeks to overcome such limits through the use of standards for Web Services, in this case WS-Trust and SAML, which seem more adequate since it is a standard defined. The crossing of limits brought problems to the localization of rights needed by each domain, which enabled the description of how to overcome such problems through the concept of federations and the navigation heuristic.

4. CONCLUSION

The integration concept represents a defined set of industry-standard technologies that work together to facilitate interoperability among heterogeneous systems. Web services hold the potential of easily integrating legacy systems with distributed applications.

This article describes a way to integrate organizations which use different security technologies in the establishment of virtual organizations. The security proposals to Web Services along with XML security standards were adopted to form the basis of the proposed model. This model then provides (1) confidentiality, (2) integrity, (3) authenticity, and also (4) a means to locate security attributes, and thus enables the dynamic creation of trust relationships.

In the context of virtual organizations the privacy of each partner's properties may be desired. Organizations would like to take part in a business opportunity, but this implies the revelation of some important information, such as production capacity, abilities, and so forth. This information can be used in a malicious form. Once the deficiencies of this organization is known, a malicious organization can focus its business on providing a competitive solution, with the same kind of services, at lower cost.

In this work the privacy of organizations issue was not addressed. Specifications such as the Liberty Alliance (2003) and the proposal WS-Federation (2003) propose pseudonymous services which guarantee anonymity. Future studies may adopt and adapt the use of pseudonyms services.

Acknowledgments

This work has been developed within the scope of the Brazilian IFM (www.ifm.org.br) and European FP6-IP ECOLEAD (www.ecolead.org) projects.

5. REFERENCES

1. Blaze M, Feigenbaum J, et al. Decentralized Trust Management. AT&T Tech. Report 96-17, 1996.
2. Blaze M, Feigenbaum J, et al. The keynote trust-management system version 2. IETF RFC 2704, 1999.
3. Camarinha, L.M and Afsarmanesh. The emerging discipline of collaborative networks. In Virtual Enterprises and Collaborative Networks, Kluwer Academic Publishers, IFIP Vol. 149, Aug 2004.
4. Ellison C. M, et al. SPKI Certificate Theory. IETF RFC 2693, September 1999.
5. Foley S. N et al. A framework for heterogeneous middleware security. 18th International Parallel and Distributed Processing Symposium (IPDPS'04), 2004.
6. Ford W, Hallam-Baker P. XML Key Management Specification (XKMS), 2001. http://www.w3.org/TR/xkms
7. Foster I, Kesselman C. The grid: blueprint for a new computing infrastructure. A Toolkit-Based Grid Architecture. Morgan Kaufmann Publishers Inc., 1999; 259-278.
8. Gnutella. The Gnutella Protocol Specification v0.4, 2001.
9. ITU-T. ITU-T Recommendation X.509, 1993. http://www.mcg.org.br/mirrors/97x509final.doc.
10. Kohl J, Neuman C. The Kerberos Network Authentication Service (v5). IETF RFC 1510, Sept. 1993.
11. Liberty. Liberty Architecture Overview v1.1, 2003.
12. OASIS. Security Assertion Markup Language (SAML), 2002. http://www.oasisopen.org/comittees/tc_home.php?wg_abbrev=security.
13. Sandhu RS, Samarati P. Access Control: Principles and Practice. IEEE Communications Magazine.
14. Santin A, Fraga J, et al. Federation WEB: A scheme to compound authorization chains on large-scale distributed systems. 22nd Symposium on Reliable Distributed Systems, Florence, Italy, 2003.
15. UDDI. UDDI Version 3 Published Specification, 2002. http://uddi.org/pubs/uddi_v3.htm
16. Wlech C, Siebenlist, et al. Security for Grid Services. 12th IEEE Int. Symp. on High Performance Distributed Computing, 2003.
17. WS-Trust. Web Services Trust Language (initial draft), 2004. http://msdn.microsoft.com/library/en-us/dnglobspec/html/WS-Trust.asp
18. WS-Federation. Web Services Federation Language (initial draft), 2003, http://msdn.microsoft.com/ws/2003/07/ws-federation.