EXTENDING RESOURCE ACCESS IN MULTI-PROVIDER NETWORKS USING TRUST MANAGEMENT*

Maurizio Colombo[1], Fabio Martinelli[1], Paolo Mori[1]
Barbara Martini[2]
Molka Gharbaoui[3], Piero Castoldi[3]

[1]Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy
{maurizio.colombo, paolo.mori, fabio.martinelli}@iit.cnr.it
[2]Laboratorio Nazionale di Reti Fotoniche, Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Pisa, Italy
barbara.martini@cnit.it
Scuola Superiore Sant'Anna, Pisa, Italy
{m.gharbaoui, castoldi}@sssup.it

ABSTRACT

Resource access control in a multi-provider scenario requires an authorization mechanism such that users are granted seamless access to resources (connectivity services, application services and contents) in different provider domains. This paper proposes the integration of a Role-based authorization system in a network service provisioning framework, in order to support multi-provider networks. This authorization system allows the access to provider's services by unknown users, i.e. users that have been registered in different administrative domains, provided that those domains have trust relations with the original one. By removing the user subscription as pre-condition for resource access, the proposed access model offers increasing opportunities for service delivery and resource usage with benefits for both providers and users. The paper presents the architecture of the proposed system, along with a reference implementation and the evaluation of the delay in the service delivery time introduced by the proposed security support.

KEYWORDS

Next Generation Network, Multi-provider Networks, Access Control, Trust Management

1. INTRODUCTION

Next Generation Networks (NGN) [1,2] promote the provisioning of a wide range of new services delivered from multitude of providers thus creating new market opportunities. This evolving service provisioning scenario is also fostered by advanced features presented by ever-sophisticated user terminals (e.g., PDA, laptop) in terms of processing capabilities and mobility.

Each provider relies on different expertise and assets and interwork each other to deliver services to users while addressing its own business target. Network Providers (NPs) operate a network infrastructure while offering connectivity and IP-based service, e.g., Internet access services (e.g., ADSL, Wifi, VPN). Application Service Providers (ASPs) operate a service

* This work was partially supported by the EU FP7 project "Network of Excellence on Engineering Secure Future Internet Software Services and Systems" (NESSOS), FP7-ICT-2009-5 n. 256980
DOI : 10.5121/ijcnc.2011.3309

delivery infrastructure (servers, media control systems) while providing application services, e.g., Multimedia On Demand, Video Conference. Content Providers (CPs) might support ASP in the provisioning of content-driven services by supplying contents and information they own and manage.

In this context, providers can benefit from combining respective resources for providing value-added services to a wider range of customers. For example a NP providing wired connectivity services, might enlarge connectivity offering by relying on capabilities offered by a wireless NP operating in diverse regional areas. Wired customers can benefit from empowered Internet connectivity capability by accessing, e.g., Wimax access point, while being immediately authorized. Similarly, a ASP providing, e.g., VoD service, might enlarge service offering by sharing service infrastructure with a ASP providing, e.g., e-learning services. VoD customers can benefit from empowered service portfolio by enjoying web-based training courses at home being immediately authorized. While such partnerships would be profitable and generate reciprocal benefits for all providers, access control to respective resources in this context becomes an issue [3,4].

The combination of service offerings in a multi-operator environment presents challenges for providing secure, open and flexible access to a heterogeneous and distributed set of exposed resources. On the one hand, the access control to resources exposed from several providers might involve different administrative domains, each applying its own access control policies and adopting different security mechanisms [3]. On the other hand, users might access the resources through service entities operated by a provider that did not directly subscribe to, e.g., occasional access to a WiFi hot-spot during a stop-over in a airport. In this context, a trust relationship needs to be established at the moment of a service request in a way that the adequate usage rights could be granted to the user. Since traditional access control systems require the user to be beforehand registered with the provider of each visited administrative domain [5], a flexible authorization model is desirable in multi-provider scenario in which the user credential processing is unburdened from the requirements of direct agreement with him [6].

Following the design principles presented in [7], this paper presents and evaluates an advanced authorization system, based on Trust Management techniques [8,9], to regulate the accesses to the services offered in a multi-provider network scenario. The proposed authorization system is based on the Role-based Trust Management Language (RTML) framework [10] and allows to infer derived trust relationships between user and resource provider when direct ones do not exist or are not enough to grant the requested access. Upon the service request, the authorization system exploits the user's credentials and inter-organization credentials, respectively formalizing the level of trust in the user and in the organization, to decide whether the user has the right to exploit the requested service without the need for the user to be preventively registered in the administrative domain. The trust relationship existing among the providers are expression of agreements that have been established prior and independently from the access requests. Hence, an access request received by a provider is not redirected to the provider where the user is registered in order to obtain his access right. Instead, the access rights to be granted to the user are derived from the existing trust relations among the providers, thus with a one-step decision-making process.

The rest of the paper is organized as follows. Section 2 reports an overview of the most noteworthy research works on access control in multi-provider scenario and trust management. Section 3 presents the network scenario we refer, the proposed authorization system and access rule based on the RTML framework. Section 4 describes the architecture of the proposed RTML authorization system and its integration in the network service provision platform. Section 5

describes the implementation of a prototype to validate the proposed trust model, along with some preliminary performance evaluation. Finally, Section 6 concludes the paper.

2. RELATED WORKS

The problem of regulating resource access in a multi-domain scenario has been addressed in both information and communication sectors.

While a large number of works within the communication field focus on extensions to protocol mechanisms assuring authentication and authorization features [11,12,13], the most noteworthy research works are those investigating access control and trust management issues, as outlined in the following.

In [14,15], the access control issue is tackled within the context of on-demand network resource provisioning in a multi-domain scenario for the benefit of grid applications. In this works, the focus is on per-session authorization and security context management assuring to be consistent across domains (i.e., spatial consistency) and between the resource provisioning and access phases (i.e., temporal consistency) thanks to the use of a token mechanisms. The user is allowed to consume the reserved resources spanning multiple network domains provided that the user has been previously given the token as a result of a successful authorization process. Specifically, the proposed authorization system addresses how to bind the token presented by the user to the reserved resources across domains in order to guarantee their exclusive access and consistent use. However, they do not investigate authorization process in case of non pre-registered users, that, instead, is addressed in this work as a result of one-step decision-making process prior the effective access to resource. Nevertheless, the proposed authorization mechanisms can supplement the one proposed in [14,15] for the generation and delivery of the token to verify if it can be granted to the requesting user.

In other research works, trust models have been defined to handle network resource access in distributed environments. In [5] a trust model is proposed for the propagation of trustworthiness information among service providers for sharing user profiles for the authentication and authorization of respective users. In such a model, the providers form a consortium that enable them to carry out user authorization and authentication by redirecting user access request to the provider that owns user credential, thus retrieving user credentials for non-registered users. The difference with the proposed authorization model is that in [5] a transaction (i.e., request-reply) is needed to retrieve user profile from the provider the user is registered in, while in this work such transactions are not needed thanks to the combined elaboration of user's profile and inter-organization credentials.

In [16] authors present an overview of trust management models in p2p systems, in mobile ad hoc networks and in e-commerce platforms, while in [17,18] authors present a trust models in decentralized systems, respectively collaborative intrusion detection systems and multi-agent systems, using a statistical Bayesian-based approach. Such models have the common aim to provide a dynamic rating of trustworthiness of entities cooperating in a distributed environment where the reputation estimation is the crucial issue. The rating systems are commonly based on some feedback systems that assign a weight that reflects the risk of misbehaving (i.e., reputation) of entities in the future transactions. In this work, the weights are not considered since the evaluation of trustworthiness is not aimed to evaluate the reputation, but to grant access rights to required resource based on an on/off user status information, e.g., paying/not paying user, known/unknown user identity.

The RTML authorization framework has been exploited in [19] to regulate the access to resources shared on the Grid. As a matter of fact, the Grid environment requires to establish

trust relationships between the participants that, at the same time, share and exploit Grid resources, because these participants typically are unknown each others, belong to distinct administrative domains, and direct trust relationships may not exist among them. In this case, the RTML framework was integrated with the Globus Toolkit authorization system, and the right of a Grid user to exploit a Grid service was determined taking into account the trust relationships with other Grid service providers he had collected in the past, that were represented through RTML credentials. In [20], instead, the RTML framework was extended to support also reputation management, and it was exploited in the Grid environment as well.

3. TRUST MANAGEMENT IN MULTI-DOMAIN NETWORKS

In this section the network scenario and the proposed authorization system according to Trust Management principles is presented.

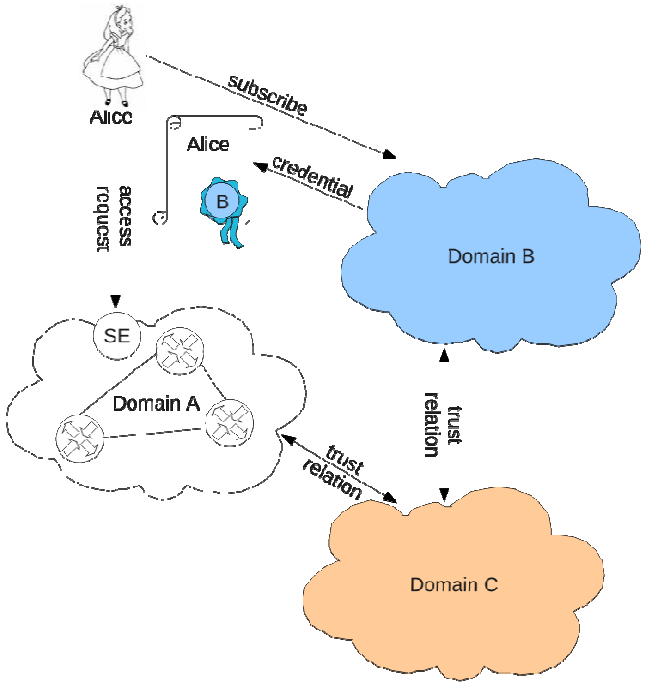


Figure 1. Multi-provider network scenario.

As shown in Figure 1, let us consider, without lacking of generality, a multi-domain scenario with three resource providers, organized in three different administrative domains, each with its own set of registered users. We consider a user, Alice, accredited in the administrative domain of the resource provider B (domain B), that requires access to resources exposed by resource provider A through the Service Element (SE) performing authorization services. If the resource provider A adopts a standard access control system, the access will be denied, because Alice is not accredited in the administrative domain A.

The features of the reference scenario do not allow the adoption of a traditional authorization system, and an advanced one is required. For example, identity-based authorization systems, that determine the set of rights to be granted to a given subject taking into account the subject's identity, cannot be adopted in this context, because this identity is unknown in the resource provider domain. Even the adoption of a simple attribute-based authorization system is not

enough, because the attributes granted to a subject by the domain he belongs to, have no meaning in the domain that the subject wants to access.

However, the user could be accredited in another administrative domain that has trust relations with the previous one. Let's suppose resource provider B has a trust relation with provider C (domain C), that in turn has a trust relationship with provider A (domain A). To overcome this limitations, we propose to use an authorization system based on Trust Management, i.e. able to infer indirect trust relations among the user and the resource provider when direct relations do not exist.

The proposed security support based on trust management is aimed at inferring the right of Alice in the administrative domain A from the attributes she holds in the domain B, provided that a trust relation between the two domains A and B can be derived. Through the security support we propose, resource provider A could exploit the attributes given to Alice by the Resource Provider B, that are valid in the administrative domain B only, to determine whether to authorize the access.

3.1. Role-based Trust Management Framework label RT

In this section a brief overview of the *Role-based Trust Management* (RT) framework is presented. A detailed description of the RT framework can be found in [10,21,22].

The RT framework provides policy language and deduction engine to manage access control in large-scale and decentralized systems. RT combines the strength of *Role-Based Access Control* (RBAC) [23] and *Trust-Management* (TM) [8] techniques. RBAC was developed to manage access control to resource in a single organization scenario in which the control of role membership and role permissions is centralized and involves a limited number of users. TM provides an approach to manage access control in distributed environment in which authorization decisions are taken on the base of *policy statements* made by multiple principals, i.e., resource providers, through the use of credentials. RT takes from RBAC the notion of role to assign permissions to users. From TM, RT takes the principles of managing distributed authorization process among multiple authorities, as well as the manipulation of trust relationships between those authorities.

The main concept in RT is the notion of *role*: each RT principal, i.e. resource provider each with own administrative domain, has its own name space for defining roles, and each role is specified by combining the principal name and a *role term*. For example, if P is a principal and r is a role term, then $P.r$ denotes the role r within the administrative domain of principal P.

The principal P has the authority to issue policy statements, i.e., access rules, assigning right depending on the the role $P.r$ presented by a subject through credentials upon the access request. In fact, each subject has a set of these credentials, representing the roles that he holds in distinct administrative domains. In turn, each principle holds RTML credentials formalizing the access rules defined as a result of trust relationships the principle has with other principles. When subject s requests to access the resource r of resource provider P, the credentials of s are properly combined with the access rules of P to determine which roles s holds in the domain of P. Each role is paired with a set of permissions, and the access request is permitted only if at least one of the roles of s grants the access to r.

3.2. RTML Credentials and Access Rules

Let us suppose that the network services provider *ProviderA* defines a set of access rules in a way that, besides granting access to its registered users, it grants access to a standard set of services (e.g., Internet access, Video On Demand) also to users of *ProviderC* and to an extended set of services (e.g., High-speed Internet, IPTV) to those users of *ProviderC* that are also

"advanced users" registered in any other provider's domain, e.g., *ProviderB*, given that this provider is accredited, for example, by the Minister of Economic Development (MED).

Hence, to access to the standard set of services delivered by *ProviderA*, Alice should supply a credential that asserts that she is a customer of *ProviderC*. To access the extended set of services delivered by *ProviderA* Alice should also provide a credential issued by *ProviderB* that gives her the role of *advancedUser*. Furthermore, another credential is required to verify that the *ProviderB* is actually a provider accredited by MED.

The credentials held by Alice are described in Table 1, while the Access Rules defined by *ProviderA* are listed in Table 2.

In Alice's credentials, the symbol '?' is used to denote a parameter whose value is not specified and in *ProviderA* access rules, the symbol '∩' denotes the conjunction (logical AND) of constraints, as explained in [13].

Table 1 – Alice's credentials

1. ProviderD.guest (id = 'M123', firstname = 'alice', lastname = 'rossi') ← Alice
2. ProviderC.user (id = 'MTR99', firstname = 'alice', lastname = 'rossi') ← Alice
3. ProviderB.advanceduser (id = 'IS137', firstname = 'alice', lastname = 'rossi') ← Alice
4. MED.resourceProvider (name = 'Provider B') ← ProviderB

Table 2 – ProviderA's access rules

1. ProviderA.resourceProvider (name = ?) ← MED
2. ProviderA.advancedUser (ProviderName = ref_{prov}, id = ?, firstname = ?, lastname = ?) ← resourceProvider (name = ref_{prov})
3. ProviderA.goldenGuest ← providerC.user(id = ?, firstname = ref_{first}, lastname = ref_{last}) ∩ providerA.advancedUser (ProviderName = ref_{prov}, id = ?, firstname = ref_{first}, lastname = ref_{last})
4. ProviderA.guest ← ProviderC.user (id = ?, firstname = ref_{first} , lastname = ref_{last})

Alice represents the Distinguished Name (DN) of the principal specified in the first three credentials for the roles issued by *ProviderD*, *ProviderC* and *ProviderB*. The forth credential is included in the set of Alice's credentials even if it represents a role of *ProviderB*, because it could be used to infer information about Alice's roles. Such credential is needed because *ProviderA* considers as resource providers the principals that are accredited as resource providers by the MED, that is the issuer of the forth credential.

The credentials provided by Alice and the access rules defined by *ProviderA* are exploited by the RTML engine to determine the roles that can be granted to Alice in the *ProviderA* domain. In this example *ProviderA* assigns the role *ProviderA.goldenGuest* to Alice. In fact, according to the third access rule, such role is granted to users that hold the role of *user* in the domain of *ProviderC*, and the role of *AdvancedUser* in the *ProviderA* domain. Indeed, Alice holds the role of *ProviderC.user* directly because of the second credential she owns, and the role *providerA.advancedUser* indirectly by combining the third and the forth credentials with the first and the second access rules. In particular, *ProviderB* holds the role *resourceProvider* in the MED domain because of the forth credential.

The first access rule claims that *ProviderA* delegates the role *resourceProvider* to the MED. By combining the previous two assertions the role *resourceProvider* is granted to *ProviderB* in the *ProviderA* domain. Furthermore, the second access rule states that *ProviderA* grants the role of *advancedUser* to any user that holds the role *advancedUser* in administrative domain which, in turn, holds the role *resourceProvider* in *ProviderA* domain. The last assertion results true in the case of Alice because *ProviderB* holds the role *ProviderA.resourceProvider* and Alice holds the role *ProviderB.advancedUser*. Hence, Alice holds the role *advancedUser* in the *ProviderA* domain and, consequently, the role *ProviderA.goldenGuest*.

Alice holds also the role *ProviderA.guest*, because of the second credential and of the forth access rule. The first credential of Alice, that grants her the role of *guest* in the domain of *ProviderD*, has not been exploited to determine Alice's role because the access rules of *ProviderA* do not define any trust relation between *ProviderA* and *ProviderD*.

4. RTML AUTHORIZATION SYSTEM ARCHITECTURE

This section describes the architecture of the prototype of RTML authorization system for multi-provider networks that we have developed, while next section presents some implementation details. In our scenario, the service provider is a Network Provider (NP), that offers connectivity to the Internet and other IP-based services (e.g. VoIP) through the Service Elements (SEs), that represent the engines for on-demand network resources provisioning. SEs expose their services through a Web Service interface, and this choice has two main advantages. The first advantage is that the interface is standard and, to interact with the SE, a client can be easily derived from the WSDL (Web Service Description Language) file that describes the service. The other advantage is that the communication channel between the user and network resource provisioning interface can rely on the Web Services security support for the data transfer across the channel. We assume that SEs perform the authentication process exploiting a standard mechanism, and we focus here on the authorization phase.

Figure 2 gives an overview of the architecture of our system, that integrates the RTML based authorization system within the SE.

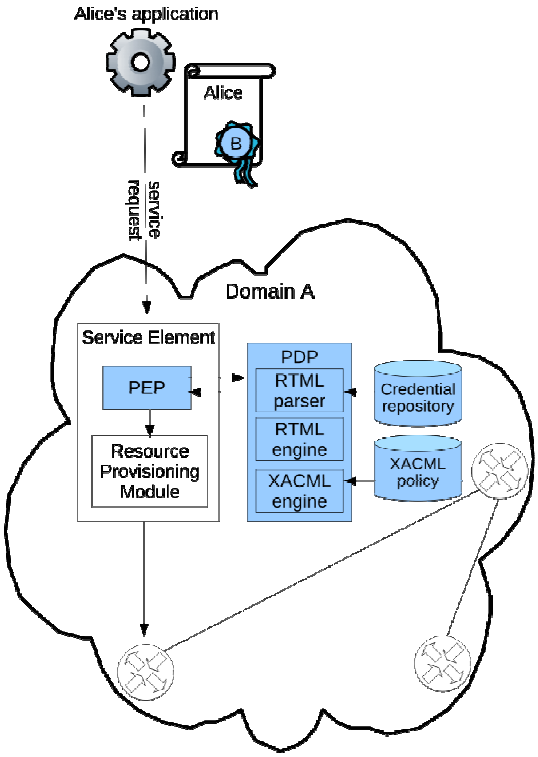


Figure 2. System architecture.

To submit the service request to the service provider, the user, Alice in Figure 2, exploits a client application, produced exploiting the SE's WSDL file. Alice requires a network service (e.g., Virtual Private Network or QoS-enabled data transfer) by issuing a request to the SE of the NP exploiting the SOAP protocol. The service request, besides the invocation of the desired service method, also includes the credentials that grant to Alice some roles in some domains. For example, Alice could include to her request the credentials represented in Table 1, that have been issued by the administrative domains of *providerD*, *ProviderC*, *ProviderB* and MED, and hence are not valid in the domain of *providerA*.

On the provider side, the SE receives Alice's request and processes it. The SE embeds the Policy Enforcement Point (PEP) of our architecture, that intercepts the incoming service requests. The PEP extracts from the service request and sends to the policy Decision Point the Distinguished Name (DN) of the user, the name of the service, the method that the user wants to execute on the service, and the role credentials submitted by the user. The Policy Decision Point (PDP) is the component which evaluates the RTML credentials submitted by the user according to the provider's access rules to determine whether the user holds specific rights on the requested service.

The decision process consists of two steps: in the first step the PDP computes all the roles that can be granted to the user in the provider's domain, while the second step checks whether these roles allow the execution of the request. In general, to retrieve the user's credentials, two different approaches are possible for the PDP: the *push model*, in which the user chooses the most suitable subset of credentials to submit, and *pull model*, in which the PDP obtains the user credentials from proper repositories. Our prototype exploits the *push model* because it preserves the user privacy, since the user decides which of her credentials are sent to the PDP, and hence could decide not to disclose all her credentials. The security policy to be enforced, instead, is read by the PDP from a local credential repository. An example of security policy for the network service provider is shown in Table 2.

The PDP at first controls the validity of the user's credentials, by checking the validity of the signatures and the expiry dates. The valid user's credentials and the provider's access rules are passed to the RTML parser that transforms them in RT statements. Then, the set of RT statements is exploited by the RTML engine to infer the roles owned by the user in the local domain. This set of roles, along with the other data extracted by the PEP from the request message, are then processed by the XACML engine. XACML [25] is an OASIS standard for expressing, combining and managing access control policies in a distributed environment. XACML was designed for attribute-based access control and it is widely used to write security policies in many environments due to its extensibility and interoperability. XACML has facilities to express traditional access control. Moreover, arbitrary attributes can be defined and exploited in the security policies to accommodate the specific requirements of the application environment. The XACML engine reads and evaluates the XACML security policy to determine whether the request can be granted. In XACML, the user's role is represented as an attribute of the user, and the services exposed by the provider are the targets of the security policy. Where necessary, the rules that regulates the access to a target could also include other conditions besides the evaluation of the user's role. If the evaluation of the security policy finds at least one role of the user that satisfies a rule that grant the required access right to the required target, than the request is granted, and the PDP returns a positive response to the PEP. Upon receiving the positive outcome of the PDP, the PEP forwards the service request to the next elements of the handler chain and, eventually, the request is sent to the Resource Provisioning Module (RPM) acting as an agent that manages network resources and configures the network node to provide the authorized service. Otherwise, if the PDP denies the request, the PEP returns an error message to the user, and the RPM is not activated.

5. PROTOTYPE IMPLEMENTATION

A prototype of the RTML-based authorization system described in the previous section has been implemented to evaluate the effectiveness of the proposed architecture and to measure the performance degradation due to the overhead introduced by the new authorization phase. The prototype consists of the client application exploited by the user, Alice, to request the services, and the Web Service that implements the SE and provides the Next Generation Network services.

The client application exploited by Alice to request the services is an application developed in Java. This client uses the stubs generated from the WSDL file exposed by the SE Web Service to set up the communication with the SE itself. However, the SE adopts a push model in which Alice is in charge of sending all and only the credentials she wants to evaluate within the request. Hence, to enable the authorization process, the client must also include in the service request the credentials released by various entities to Alice to grant her some roles in some domains. These credentials are in RTML format (that is XML based), and each of them is signed by the Issuer and represents the role of the owner within a specific domain.

On the Network Provider side, the SE is implemented as a Web Service, running within the Apache Tomcat container with AXIS2[1]. The SE Web Service embeds the RPM, that is the network resource provisioning engine designed and implemented for optical transport network presented in [14]. The WSDL file describing the methods provided by this service is exposed at a given EPR (EndPointReference) and allows possible users to develop their clients to interact with the SE, provided that they add their RTML credentials in the request.

To implement the PEP of the system, i.e., to intercept and process the incoming SOAP requests to perform the authorization phase, we adopt the SOAP message Handler mechanism, because

[1] http://ws.apache.org/axis2/

is very flexible and easily configurable. In fact, users' messages that are received by the SOAP engine that hosts the services are processed by a chain of SOAP message Handlers, called the InFlow Handler Chain, before the invocation of the methods requested in the messages. An Handler Chain consists of a sequence of SOAP message Handlers, that are executed in the order they appear in the chain. A SOAP message Handler is a software component that receives the SOAP message from the previous Handler of the chain, processes it, possibly modifies it, and returns the new message to the next Handler of the chain. In our prototype, we added to the InFlow Handler Chain the following Handlers:

- AutzHandler
- RTMLHandler
- XACMLHandler

Figure 3 shows in details the components that compose the system prototype.

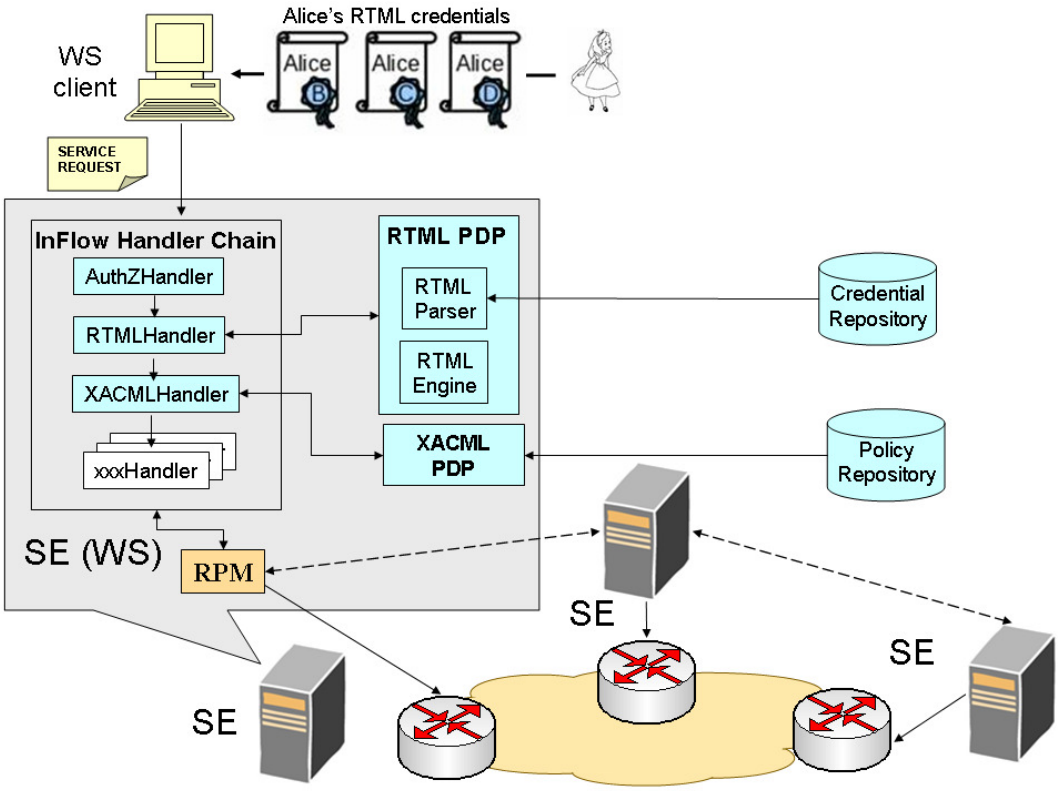


Figure 3 System prototype.

The AutzHandler is the first Handler we added to the chain, and it is in charge of evaluating the WS-Security features contained in the message. We choose to adopt Rampart[2] v1.4.2, an Axis2 module based on Apache WSS4J, because it is easy to integrate into the Handler mechanism. It can be configured to support timestamps, signature and encryption of the SOAP body. Furthermore this Handler extracts the Distinguished Name (DN) of Alice from her certificate and adds it into the MessageContext for the following handlers.

[2] http://axis.apache.org/axis2/java/rampart/

The RTMLHandler invokes the RTML parser and the RTML engine that are two Java packages that combine the credentials submitted by Alice with the local access rules in order to determine all the roles granted to her (specified by her DN) in the local domain. The RTML engine implementation is based on the language and the parser developed by N. Li et al. [8].

Finally, the XACML Handler takes as input the roles, expressed as user's attributes, that have been computed by the RTML engine, and invokes the XACML engine that verifies the role attributes owned by Alice, the resource requested and the specific action over the local XACML policy. The XACML PDP is invoked at each request and its response grants Alice the access or not to the resource. The XACML engine is based on XACML2.0 and uses the XACML framework developed by Sun[3], version 1.2. The XACML policy that regulates the access to the services is defined by the Network Provider. In general, this policy could grant different access rights on the provided services depending on the role paired with the user. If the XACML engine returns a positive answer to the XACML Handler, the SOAP message is forwarded to the next Handler of the chain, and a new Web Service instance is created to satisfy the request. Instead, if the XACML engine denies the access, a fault is created and is processed by the OutFaultFlow Handler Chain. In this case, an exception message is sent to the client, and no service instance is created.

As mentioned before, both the RTML parser, engine and the XACML engine are executed on the same machine of the SE. This choice minimizes the overhead due to information exchange among the PEP and the PDP. However, they can migrate on a distinct machine, and could be exploited to control more SEs of the same domain. In this case, the communication channels exploited for message exchange among the PDP and the SEs should be secured.

5.1. Performance Evaluation

The integration of the RTML authorization system in the Service Elements introduces a delay in the service delivery time. As a matter of fact, the time required to deliver the service includes not only the time to set up the service itself, but also the time required by the authorization system to perform the decision process. This process, as described in the previous sections, mainly consists of two phases: the computation of the user's local roles performed by the RTML engine and the evaluation of the XACML policy performed by the XACML engine. This section describes the experiments we performed to evaluate the delay introduced by the RTML authorization system. The experiments we performed simply evaluates the overhead of the authorization system by measuring the execution time on the network service provider side. The provider's access rules we used for this experiment are the ones shown in Table 2, while the credentials submitted by the user are the ones in Table 1.

The service delivery time we measured on average on the provider side is about 25 seconds, 20 of which are due to the RTML authorization system. On average, about 19 seconds of this overhead is due to the first step of the decision process, i.e. the computation of the local roles, while about 1 second is required to evaluate the XACML policy. Hence, the time required to set up the requested service is about 5 seconds [24]. The main reason for this overhead is that the RTML engine, to verify the credential submitted by the user, perform some network accesses, that introduce a considerable and unpredictable delay.

The other experiments we conducted evaluate the impact of the number of credential submitted by the user on the PDP decision time. In the previous experiments, Alice submitted 4 credentials, and the resulting overhead was about 20 seconds. In the other set of experiments we conducted, Alice submitted 6 credentials, and in this case the service delivery time was 39 seconds, and the overhead due to the RTML authorization system was 34 seconds. Finally, if Alice submits 8 credentials, the service delivery time is about 44 seconds, and the overhead is

[3] http://sunxacml.sourceforge.net/

39 seconds. Also in these cases, the overhead is mainly due to the first step of the decision process, in particular to the network accesses performed to verify the credentials, and about 1 second is required to evaluate the XACML policy.

6. CONCLUSIONS

This paper investigated security issues for Next Generation Network in multi-provider scenario, and proposed the adoption of an advanced authorization system based on trust management techniques to allow users to exploit the services of a network provider even if the are registered to another provider.

The proposed access control system is based on the Role-based Trust Management Language framework, and enables the user of a provider to be virtually a user of other providers, given that a trust relationship (represented by RTML credentials) exists between such providers. As a matter of fact, the credentials presented by the user, that represent the roles he has in the domain of his provider, are combined by the RTML framework with the credentials of the provider of the requested service, to compute the role of the user this domain. To preserve his privacy, the user could submit only a subset of his credentials, provided that he knows that the submitted credentials are enough to obtain the access right he needs. In general, a negotiation mechanism could be defined to allow the user to submit only the minimum number of credentials that grants him the required access right. This trust model has advantages both for providers and users. On the one hand, it increases the business opportunities for providers since the number of users that can be potentially served is higher. On the other hand, users are not required to stipulate contracts with all providers they encounter, even occasionally, e.g., during a wait in an airport for making just one VoIP call. Moreover, this model increases also inter-operability, and gives the opportunity for collaboration among service providers to produce composed services.

ACKNOWLEDGEMENTS

The authors would like to thank Ninghui Li for providing a beta version of the parser for RTML credentials they used in their implementation.

REFERENCES

[1] ITU-T Y.2012, *Functional requirements and architecture of the NGN release 1*, September 2006.

[2] ETSI TR 180 001 Ver. 1.1.1 (2006-03), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1.*

[3] Rensing, C.; Karsten, M.; Stiller, B., “AAA: a survey and a policy-based architecture and framework”, In *IEEE Network,* 16(6), (2002), pag. 22-27.

[4] Yan, D.; Yang, F.; , "Vulnerability Analysis of Service Architecture in NGN", *International Conference on E-Business and Information System Security 2009 (EBISS '09)*, May 2009

[5] Polito, S.G.; Schulzrinne, H., “Authentication and Authorization Method in Multi-domain, Multi-provider Networks”, In *Proceedings of the 3rd EuroNGI Conference on Next Generation Internet Networks*, (2007), pag. 174--181.

[6] Demchenko, Y.; de Laat, C.; Lopez, D.R.; Garcia-Espin, J.A., "Security Services Lifecycle Management in On-Demand Infrastructure Services Provisioning," *IEEE Second International Conference on Cloud Computing Technology and Science 2010 (CloudCom 2010)*, Dec. 2010

[7] Colombo, M.; Mori, P.; Martinelli, F.; Martini, B.;Baroncelli, F.; Castoldi, P, “Resource access in Multi-Provider Networks using Trust Management”, In *Proceeding of the 5th International Workshop on Security and Trust Management* (STM'09), (2009).

[8] Blaze, M.; Feigenbaum, J.; Lacy, J., "Decentralized Trust Management", In *Proceedings of the 17th Symposium on Security and Privacy*, (1996), pp. 164--173.

[9] De Capitani di Vimercati, S.; Jajodia, S.; Paraboschi, S.; Samarati, P., "Trust Management Services in Relational Databases", In *Proceedings of the ACM Symposium on Information, Computer and Communications Security* (ASIACCS'07), (2007), pag. 149--160

[10] Li, N.; Mitchell, J.C.; Winsborough, W.H, "Design of a role-based trust management framework", In *Proceedings of IEEE Symposium on Security and Privacy*, (2002), 114--130.

[11] Salsano, S.; Polidoro, A.; Veltri, L., "Extending SIP authentication to exploit user credentials stored in existing authentication databases," *16th International Conference on Software, Telecommunications and Computer Networks 2008 (SoftCOM 2008)*, Sept. 2008

[12] Polito, S.G.; Chamania, M.; Jukan, A.; , "Extending the Inter-Domain PCE Framework for Authentication and Authorization in GMPLS Networks," *IEEE International Conference on Communications 2009 (ICC 2009)*, June 2009

[13] Bless, R.; Rohricht, M.; , "Secure Signaling in Next Generation Networks with NSIS," *IEEE International Conference on Communications 2009 (ICC 2009)*, June 2009

[14] Demchenko, Y.; de Laat, C., Denys T., Toinard C., "Authorisation session management in on-demand resource provisioning in collaborative Applications", In *Proceeedings of International Symposium on Collaborative Technologies and Systems*, (2009), pp.201--208.

[15] Demchenko,Y., Wan, A., Cristea, M., de Laat, C., "Authorisation infrastructure for on-demand network resource provisioning" In *Proceedings of the 9th IEEE/ACM International Conference on Grid Computing*, (2008) Pages: 95-103.

[16] Huaizhi Li, Mukesh Singhal "Trust Management in Distributed Systems", In *IEEE Computer Society*, February 2007

[17] Aboulwafa, S.; Bahgat, R., "DiReCT: Dirichlet-based Reputation and Credential Trust management," *7th International Conference on Informatics and Systems (INFOS2010),* March 2010

[18] Fung, C.; Zhang, J.; Aib, I.; Boutaba, R., "Trust Management and Admission Control for Host-Based Collaborative Intrusion Detection", *Springer Journal of Network and Systems Management*, Volume: 19, Issue: 2, pp 257-277, September 2010

[19] Colombo, M.; Martinelli, F.; Mori, P.; Vaccarelli, A. "Extending the Globus architecture with Role-Based Trust Management", In *Proceeding of the Eleventh International Conference on Computer Aided Systems Theory (Eurocast 2007)* Lecture Notes in Computer Science 4739: Springer Verlag (2007) pp 448-456

[20] Colombo, M.; Martinelli, F.; Mori, P.; Petrocchi, M.; Vaccarelli, A. "Fine Grained Access Control with Trust and Reputation Management for Globus", In *Proceeding of On the Move to Meaningful Internet System 2007: CoopIS, DOA, GADA, and ODBASE*: Lecture Notes in Computer Science 4804: Springer Verlag (2007) pp 1505-1515.

[21] Li, N.; Tripunitara, M.V., "Security Analysis in Role-Based Access Control", In *Proceedings of the ninth ACM Symposium on Access Control Models and Techniques* (SACMAT 2004), (2004)

[22] Li, N.; Winsborough, W.H; Mitchell, J.C., "Distributed Credential Chain Discovery in Trust Management", In *Journal of Computer Security*, 1, (2003), pp. 35--86.

[23] Sandhu, R.S.; Coyne, E.J.; Feinstein H.L.; Youman, C.E., "Role-Based Access Control Models", In *IEEE Computer*, 29(2), (1996), pp. 38—47.

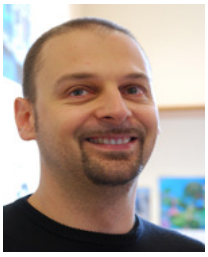
[24] Martini, B.; Martini, V.; Baroncelli, F.; Torkman, K.; Castoldi, P.; , "Application-Driven Control of Network Resources in Multiservice Optical Networks," *IEEE/OSA Journal of Optical Communications and Networking*, , vol.1, no.2, pp.A270-A283, July 2009

[25] OASIS XACML TC, eXtensible Access Control Markup Language (XACML), www.oasis-open.org/committees/xacml

Authors

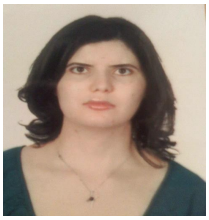
Maurizio Colombo received a Master Diploma in Internet Techologies from the University of Pisa in 2006. In 2005 he obtained an internship with IIT-CNR, from September 2006 to December 2007 he collaborated with BT (British Telecom) in UK, and since 2008 he works as software engineer in IIT-CNR, member of the information security group. His main research interests involve security in distributed systems and Service Oriented Architectures (SOA); in particular the design and implementation of mechanisms for usage control and for trust and reputation management. He is (co-)author in several papers published on international journals and conference/workshop proceedings. He has been/is involved as developer in some FP6-FP7 projects on information and communication security such as TrutCom, BeInGrid, GridTrust and Consequence.

Fabio Martinelli is a senior researcher of IIT-CNR where he leads the information security group. He is a (co-)author of more than one hundred of papers on international journals and conference/workshop proceedings. His main research interests involve security and privacy in distributed and mobile systems and foundations of security and trust. He serves as PC-chair/organizer in several international conferences/workshops and Ph.D. schools. He founded and chaired (2005-2009) the WG on security and trust management (STM) of the ERCIM consortium and He is also member of the IFIP WG on trust management. He usually manages R&D projects on information and communication security and he is/has been involved with several roles in the following FP6-FP7 projects: NESSoS, CONTRAIL, ARTIST2, BIONETS, CONNECT, Consequence, GridTrust, S3MS, Sensoria.

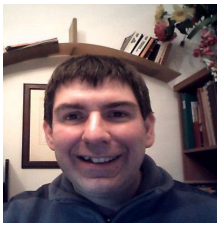


Paolo Mori received his M.Sc. in Computer Science (cum laude) from the University of Pisa in 1998, and his Ph.D. in Computer Science from the same university in 2003. He is a researcher of IIT-CNR, member of the information security group. His main research interests involve high performance computing and trust and security in mobile and distributed systems, in particular design and implementation of mechanisms for usage control and trust and reputation management in distributed environments. He is (co-)author of several papers published on international journals and conference/workshop proceedings. He has been/is involved in some projects on information and communication security, such as the European Commission funded NESSoS, CONTRAIL, GridTrust, and S3MS, and the national project InFSE.

Barbara Martini received the Laurea degree in Electronic Engineering in 1999 from the University of Florence, Italy. She joined Italtel from university working on network device drivers design for digital switching equipment. In 2000 she joined Marconi as software engineering involving in network management system design for optical networks. Since 2003 she has been a research engineer at the CNIT National Laboratory of Photonics Networks in Pisa, Italy. Her main research interests include optical network management, GMPLS optical control and service architectures for next generation networks and security in multi-domain networks. She is author of more than 40 publications in international journals and conference proceedings. Currently, she is involved in projects on advanced optical networking, such as European Commission funded BONE and STRONGEST.



Gharbaoui Molka received her National Degree of Engineer from the National School of Computer Sciences (ENSI), Tunisia, in 2007. She achieved the degree of International Master on Communication Networks Engineering (IMCNE) at Scuola Superiore SantAnna di Pisa, in 2008. She is currently a PhD student in ICT at Scuola Superiore SantAnna di Pisa. Her main research areas are the support of QoS in transport networks, the development and the implementation of service oriented architectures, access control and authorization mechanisms.



Piero Castoldi received his Master Degree from the University of Bologna, Italy, in 1991 and the PhD degree in Information technology from the University of Parma, Italy in 1996. He is currently Associate Professor at Scuola Superiore Sant'Anna, Pisa, Italy, where he is Area Leader of the "Networks and Services" area. Since January 2005 he has been also Director of the CNIT National Laboratory of Photonic Networks. His recent research interests cover reliability, switching paradigms and control for optical networks, including application-network cooperation mechanisms. He has been involved in the following European FP5-FP6-FP7 projects: Collaborator, e-photon/ONE, e-photon/ONE+, BONE, NOBEL, NOBEL2, STRONGEST. He is author of more than 200 publications in international journals and conference proceedings.