01

TOWARD WEB SERVICES PROFILES FOR TRUST AND SECURITY IN VIRTUAL ORGANISATIONS

Alvaro E. Arenas, Ivan Djordjevic
CCLRC Rutherford Appleton Laboratory, UK {A.E.Arenas, I.Djordjevic}@rl.ac.uk
Theo Dimitrakos, Leonid Titkov
British Telecom, UK {theo.dimitrakos, leonid.titkov}@bt.com
Joris Claessens, Christian Geuer-Pollmann
European Microsoft Innovation Center, Germany {jorisc, chgeuer}@ microsoft.com
Emil C. Lupu, Nilufer Tuptuk
Imperial College, UK {e.c.lupu, nt102}@doc.ic.ac.uk
Stefan Wesner, Lutz Schubert
High Performance Computing Centre Stuttgart, Germany {wesner, schubert}@hlrs.de

The rise in practical Virtual Organisations (VOs) requires secure access to data and interactions between their partners. Ad hoc solutions to meet these requirements are possible, but Web services hold out the potential for generic security solutions whose cost can be spread across several short lived dynamic VOs. This paper identifies trust and security requirements throughout the VO lifecycle and analyse current Web Services specifications to show their suitability to meet these requirements. Although they demonstrate the potential for generic security support, there are uncertainties concerning different level of interoperability and stability of implementation for different specifications, which may slow down their exploitation for security-critical business applications. However, research in Web services developments are well timed to avoid losing first adopter advantage when they become stable.

1. INTRODUCTION

Virtual Organisations (VOs) have been the focus of business research for several years (Goldman et al, 1995; Saabeel et al, 2002; Roberts and Svirskas, 2005). In this paper, a VO is understood as a temporary or permanent coalition of geographically dispersed individuals, groups, organisational units or entire organisations that pool resources, capabilities and information to achieve common objectives (Dimitrakos et al, 2004). Enterprise Computing systems increasingly operate within VOs similar to the scientific collaborations that originally motivated Grid Computing (Foster et al, 2001). Depending on the context, dynamic ensembles of the resources, services, and people that comprise a scientific or business VO can be small or large, short- or long-lived, single- or multi-institutional, and homogeneous or heterogeneous.

Service Oriented Computing frameworks allow for the creation, maintenance, and application of the service ensembles that VOs maintain. Key business functions

are treated as services: *globally identifiable and discoverable network-enabled entities providing a capability through the exchange of messages over standardized, extensible protocols that allow data-encapsulated cross-application invocations.*

The TrustCoM[1] IST project (Dimitrakos et al, 2004) is developing a framework for enabling secure collaborative business processing in on-demand created, self-managed, scaleable and highly dynamic VOs. The project is built on the convergence of emerging technologies such as Web services and Grid. As a part of this project we have done an analysis of the Web Services Security Specifications as an enabling technology to build secure and trustworthy dynamic VOs. This paper identifies trust and security requirements throughout the VO lifecycle and analyses current Web services specifications with respect to meeting these requirements.

2. AN AGGREGATED SERVICES SCENARIO

This section introduces the example of a VO created for the purpose of offering aggregated services. It is an abstraction of the real-world scenario on aggregated services in the telecommunication domain, which is currently being developed in TrustCoM.

A *consumer* requests a complex service **S** which has been advertised by provider **SA** (Service Aggregator). The latter has a pre-defined business process describing the decomposition of **S** into a number of sub-services that interact with each other (potentially sharing resources) in order to realise **S**. From this point of view, **S** can be also understood as the enactment plan of a collaborative business process **BP** which consists of a number of tasks, some of which are outsourced to other providers and require the consumption of resources, and others which will be rented.

Figure 1 depicts the case where **BP** consists of three tasks: the first one corresponds to the first instance of an action $\mathbf{s_a}$ followed by two concurrent actions which respectively correspond to the first instances of actions $\mathbf{s_b}$ and $\mathbf{s_c}$ followed by a second instance of action $\mathbf{s_a}$. The Service Aggregator **SA** then discovers the services that match the specification of $\mathbf{s_a}$, $\mathbf{s_b}$ and $\mathbf{s_c}$. This involves locating the appropriate service providers and inspecting their reputations and the SLA template characterising their service, security and access policies they publish about their services. The **SA** (or a broker acting on its behalf) forms a collection of candidate services and assesses whether their terms of service provision collectively allow **SA** to offer satisfactory terms for the provision of service **S** to the consumer at an acceptable risk. In Figure 1, we assume that **SP1**, **SP2**, **SP3** is such a set whereas **SPx**, **SP2**, **SP3** is not.

The scenario includes a number of actors. The external actor is a *Service Consumer*, who requests a service **S** from a service provider **SA**. *Service Providers*, (**SP1**, **SP2**, etc.), offer specific services. A particular kind of service provider, which plays a significant role in this scenario, is the one that is able to *aggregate services* provided by other providers. This actor, called *Aggregator*, has the capability to act as manager of the VO, discovering the appropriate services, negotiating with service providers, setting up the VO and managing the whole operation.

Once an agreement is reached between **SP1**, **SP2**, **SP3** and **SA, the SA** confirms its agreement with the *consumer*, and prepares for the enactment of the process.

[1] http://www.eu-trustcom.com/

Preparation includes planning the formation a VO community. This can be understood as a collection of reputable services containing at each time only those services, which are active in performing a business process task and assume a specific role that is defined for this purpose. The community is managed by the federation of service providers contributing to the aggregation, and which is coordinated by the Aggregator. Notably VO community membership evolves following the progress of the business process enactment: services that are needed for performing some task enter the VO community, those that have fulfilled their role leave and those which committed terminal violations are expelled and replaced, should the business process enactment continue.

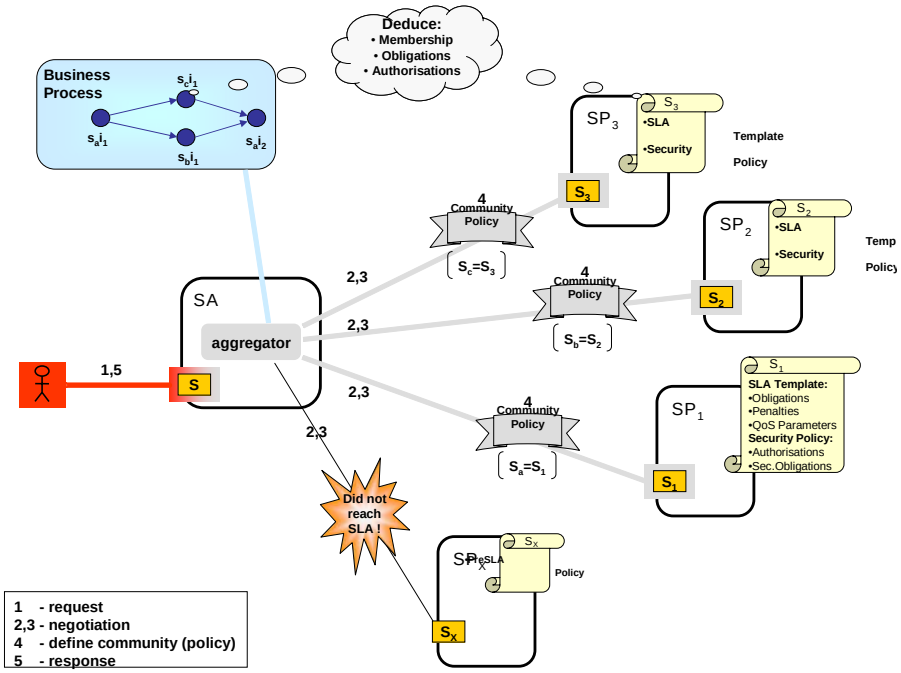

Figure 1 The Aggregated Services Scenario

Each member in the VO community is assigned to some roles which consist of a set of obligations, access permissions and prohibitions that are derived from the business process enactment plan, the service level agreements of the corresponding services and security policies of the collaborating service providers.

Furthermore, adaptation policies enable automatic updates to membership (e.g. expulsion due to violation of SLA or security obligations), to roles (e.g. an existing member also assuming a role that was previously assigned to a member that is now being expelled), to reputation (e.g. a member has just successfully completed service provision to other members of the community) or to policy (e.g. strengthening the performance thresholds so as to compensate for previous underperformance, or obligation to encrypt communication if intrusion is suspected, etc.).

Once the business process enactment is completed, all agreements are nullified and the VO community is dissolved.

Note that a VO community does not act in isolation, but rather is part of a wider system in which its members may have their credentials revoked or reputations altered as a result of actions undertaken outside the VO community. Such changes may have an impact on the VO community during its lifetime.

3. AN OVERVIEW OF WEB SERVICES

The TrustCoM project is exploiting Web services to develop frameworks to implement scenarios like the one described previously. Web services offer us an interoperable framework for stateless, message-based and loosely coupled interaction between software components. These components can be spread across different companies and organisations, can be implemented on different platforms, and can reside in different computing infrastructures.

Web services expose functionality on via XML messages, which are exchanged through the SOAP protocol. The interface of a Web service is described in detail in an XML document using the "Web Service Description Language" (WSDL). Further, a Web service is registered at a "Universal Description Discovery and Integration" registry (UDDI), and is as such discoverable.

A key element in the Web services technology is the so-called composability. Web services specifications are being created in such a way that they are mostly independent of each other, however they can be combined (composed) to achieve more powerful and complex solutions. Reliability, security, transaction capabilities and other features can be provided without adding unnecessary complexity to the specification. Moreover, the specifications are easily extended with new concepts, tools and services, by adding new layers and elements.

Section 4 summarises the main Web service specifications, when explaining the needed technology to realize the scenario of the previous section. For a more comprehensive description of the Web Services Security specifications we refer the reader to (Geuer-Pollmann and Claessens, 2005).

4. VO Lifecycle

TrustCoM is following the life-cycle model developed in the VO roadmap project (Camarinha-Matos and Afsarmanesh, 2003), including phases such as identification, formation, operation/evolution and dissolution.

The identification phase is dealing with setting up the VO; this includes selection of potential business partners by using search engines or looking up registries. VO formation deals with partnership formation, including the VO configuration by a VO Manager, who distributes information such as policies, Service Level Agreements (SLAs), etc, and the binding of the selected candidate partners into the actual VO. After the formation phase, the VO can be considered to be ready to enter the operation phase where the identified and properly configured VO members perform accordingly to their role. Membership and structure of VOs may evolve over time in response to changes of objectives or to adapt to new opportunities in the business environment. Finally, the dissolution phase is initiated when the objectives of the VO has been fulfilled.

In the rest of this section we analyse these phases for our scenario, identifying the main challenges from the trust and security perspective, and explaining how Web services specifications may help to meet those challenges.

4.1 VO Identification

The identification phase includes defining VO wide policies and VO agreement templates as well as selecting potential business partners who are both capable of providing the required services and of fulfilling the trustworthiness requirements of the VO by using search engines and or looking up registries.

In the case of our aggregated services scenario, the Aggregator first analyses the Business Process Template, identifies roles, and deduces the security requirements for the VO: obligations, permissions and prohibitions. Then, the Aggregator selects the collection of potential Service Providers for the business process tasks that it would like to outsource; this selection may include assessing the trustworthiness of the service providers. The selection of the potential providers is based on abstract service descriptions of the business process template. The Aggregator and the Service Providers will also need to negotiate further details of the agreement, including the security and access requirements. Finally, the Aggregator will need to correlate the security negotiation responses of the service providers to make sure they can collectively fulfil the requirements of the VO.

Web services technology may be useful in the realisation of this phase. In relation to the representation of the business process we can use "Business Processes Execution Language for Web Services" (BPEL4WS)[2] to specify the behaviour of both executable and abstract business processes; BPEL4WS provides a language for the specification of business processes and business interaction protocols, extending the Web services interaction model and enabling it to support business transactions. The selection of potential business partners involves looking at repositories. The usual Web service technology to be applied is WSDL/UDDI, WSDL describes messages and operations while UDDI offers a discovery mechanism. To include the provision of SLA, "Web Service Level Agreements" (WSLA)[3] has been developed, a XML language for specifying and monitoring SLA for Web Services, which is complementary to WSDL. Determining the required service providers and a proper negotiation requires secure communication. WS-Security[4], a specification defining mechanisms for integrity and confidentiality protection, and data origin authentication for SOAP messages can be used between the entities to secure the communication.

4.2 VO Formation

If the identification phase is successful, the selected set of Service Providers needs to be configured so that they can perform accordingly to their anticipated role in the VO. During the VO Formation phase the Aggregator disseminates configuration information such as VO security and adaptation policies. The VO security policies

[2] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel
[3] http://www.research.ibm.com/wsla/about.html
[4] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

include obligations –what the VO member needs to do, permissions –the access rights, and prohibitions –negative policies defining negative authorisations. These requirements are derived from the Business Process Plan and the security policies of the contributing Service Providers. Adaptation policies include rules encapsulating actions that need to be performed in case of security breaches, SLA violations and any other changes in the VO context, such as new members joining the VO. The adaptation policies are defined by analysing the collaboration agreement clauses, Business Process adaptation rules and other conditions that assist in detecting and responding to violations.

The Web Services Policy Framework (WS-Policy[5]) provides a general-purpose model to describe Web service related policies. The realisation of the VO requires the creation of federations, where two or more security domains agree to interact with each other, specifically letting users of the other security domain accessing services in the own security domain. For example, in our scenario Service Providers **SP1**, **SP2** and **SP3** may form a federation. The WS-Federation[6] specification deals with federations by providing mechanism to manage and broker trust relationships in a heterogeneous and federated environment. This includes making use of WS-Trust[7] to support for federated identities, attributes and pseudonyms. The dissemination of configuration information requires secure communication as provided by the WS-Security specification.

4.3 VO Operation

This phase can be considered as the main life-cycle phase of a VO. During this phase the identified partners contribute to the actual execution of the VO tasks by executing pre-defined business processes. Important features in this phase are the monitoring of the performance of the VO as well as the enforcement of policies.

Throughout the operation of the VO, service performance will be monitored. This will be used as evidence when constructing the reputation of the service providers. According to the predefined roles of the VO, the Aggregator or other VO members can perform monitoring. Any violation –e.g. an unauthorised access detected by the access control systems- and security threats –e.g. an event detected by an intrusion detection system- need to be notified to other members in order to take appropriate actions. Unusual behaviours may lead to both a trust re-assessment and a contract adaptation. VO members will also need to enforce security at their local site. For example, providing access to services and adapting to changes and the violations.

Monitoring can be supported by event management and notification mechanisms using the WS-Eventing[8] and WS-Notification[9] specifications. This allows the monitoring service partner to receive messages when events occur in other partners. A mechanism for registering interest is needed because the set of Web services

[5] http://msdn.microsoft.com/ws/2004/09/policy/
[6] http://msdn.microsoft.com/ws/2003/07/ws-federation/
[7] http://msdn.microsoft.com/ws/2005/02/ws-trust/
[8] http://msdn.microsoft.com/ws/2004/08/ws-eventing/
[9] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn

interested in receiving such messages is often unknown in advance or will change over time.

In addition to WS-Policy and the possibility of authorization decisions through WS-Trust, to gain access control to service resources we use constructs provided by the eXtensible Access Control Markup Language (XACML[10]). The XACML policy language is used to express access control policies written in form of XML for expressing requirements to access particular resources.

VO Evolution is part of the VO Operation phase. When a VO member fails completely or behaves inappropriately, the VO manager may need to dynamically change the VO structure and replace such partners. This evolution may involve discovering new business partners, re-negotiating terms and providing configuration information, as done in the identification and formation phases. One of the main problems involved with evolution consists in re-configuring the existing VO structure so as to seamlessly integrate a new partner, possibly even unnoticed by other participants – this involves revoking security tokens, issuing new tokens, etc.VO Evolution is close related to adaptive security. In term of specifications, currently there exists little work in this area that can be directly leveraged.

4.4 VO Dissolution

The dissolution phase is carried when the objectives of the VO has been fulfilled. During dissolution, the VO structure is dissolved and final operations are performed to annul all contractual binding of the partners. From a trust and security perspective, this involves resolving federations, revoking security credentials, invalidating VO context information, and updating reputation of all participants. According to agreement on historical information, audit trail information and provenance information may be stored.

5. CONCLUSIONS

In this paper we have presented a case study of a Virtual Organisation for aggregated services. We have analysed trust and security requirements for this kind of VO through a VO life cycle and shown how Web services specification can be used to meet such requirements, summarised in Table 1.

Trust and security aspects of a VO framework span a large number of concerns such as reputation, certification, access control, authentication and secure connection. Web Service Secure Specifications aim at producing a composable solution to these issues. Every specification aims to solve very particular problem; security solutions are created by combining the approaches from different specifications.

6. ACKNOWLEDGMENTS

The results presented here are partially funded by the European Commission under contract IST-2003-01945 through the project TrustCoM. The authors would like to thanks members of other organisations working in TrustCoM AL1: SAP, Swedish

[10] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

Institute of Computer Science, ETH Zurich, Kings College London, University of Milano, University of Salford, and IBM.

Table 1. Analysis of challenges and Web service technologies for the Aggregated Services Scenario

VO Life Cycle	Trust and Security Challenges	Technology
VO-Identification	VO interactions	SOAP/WSDL/UDDI; WS-Security to support integrity and confidentiality protection
	Defining VO and its participants	BPEL to define business process; WSLA to select potential partners based on the ability to deliver QoS
VO-Formation	Aggregator disseminates configuration information	Dissemination of information requires secure communication provided by WS-Security
	Creating federated cross-organisational realms	Use architectural paradigms of WS-Federation, combined with WS-Trust.WS-Policy to support managing security tokens/ assertions
VO-Operation / VO-Evolution	VO interactions	WS-Security to support integrity and confidentiality protection
	Authorisation and Access Control	WS-Trust, WS-Policy, XACML
	Monitoring & event management	WS-Eventing, WS-Notification
VO-Dissolution	VO interactions	WS-Security to support integrity and confidentiality protection

7. REFERENCES

1. Camarinha-Matos LM, Afsarmanesh H. A Roadmap for Strategic Research on Virtual Organizations, PRO-VE'03, Lugano, Switzerland, 2003; pp.33-46.
2. Dimitrakos T, Golby D, Kearney P. Towards a Trust and Contract Management Framework for Dynamic Virtual Organisations. In *eAdoption and the Knowledge Economy: eChallenges 2004*. Vienna, Austria, 2004.
3. Foster I, Kesselmann K, Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International Journal of Supercomputer Applications, MIT Press, 2001.
4. Geuer-Pollmann C, Claessens J. Web Services and Web Service Security Standards. Information Security Technical Report, Elsevier, 2005, 10(1)15:24.
5. Goldman SL, Nagel RN, Preiss L. Agile Competitors and Virtual Organisations: Strategies for Enriching the Customer. Van Nostrand Reinhold, 1995.
6. Roberts R, Svirskas A. Implementation Options for Virtual Organisations: A Peer-to-Peer (P2P) Approach. In *Virtual Enterprise Integration: Technological and Organisational Perspectives*, Idea Group publishers, 2005.
7. Saabeel W, Verduijn TM, Hagdorn L, Kumar K. A Model for Virtual Organisation: A Structure and Process Perspective. In *Electronic Journal of Organizational Virtualness*, volume 4, 2002.