Common Capabilities for Trust & Security in Service Oriented Infrastructures

David Brossard and Maurizio Colombo

David Brossard

BT Innovate, PP13D Orion Building, Adastral Park, IP5 3RE Martlesham Heath, England, e-mail: david.brossard@bt.com

Maurizio Colombo

Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, via G. Moruzzi, 1, 56124 Pisa, Italy, e-mail: maurizio.colombo@iit.cnr.it

Abstract In order to achieve agility of the enterprise and shorter concept-to-market timescales for new services, IT and communication providers and their customers increasingly use technologies and concepts which come together under the banner of the Service Oriented Infrastructure (SOI) approach. In this paper we focus on the challenges relating to SOI security. The solutions presented cover the following areas: i) identity federation, ii) distributed usage & access management, and iii) context-aware secure messaging, routing & transformation. We use a scenario from the collaborative engineering space to illustrate the challenges and the solutions.

1. Introduction

Today's enterprise is more pervasive with a mobile workforce, outsourced data centers, different customer engagements. This increases the need for securing end-to-end transactions between businesses and the customer. The presence of multiple authorities and complex relationships regarding the ownership of resources and information means that multiple administrators must be able to define policies about entitlements, resources, and access. Policies enforced at the same point may be defined by administrators from different organizations. We need to manage identities over enterprise domains to control them and manage information disclosure; securely exposing business services by enforcing exposure policies defining what can be invoked, by whom. This paper briefly introduces security capabilities in the context of a collaborative engineering scenario. For in-depth analysis of these capabilities and their business benefits, please refer to 1].

2. Context

This paper presents three security capabilities: (1) the identity broker (SOI-STS) – it acts as an identity broker for each enterprise, and manages the correlation of identities and security attributes within a security domain; (2) the authorization service (SOI-AuthZ-PDP) – it implements a XACML engine and enables distributed Access Control; and (3) the security gateway (SOI-SMG) – it is a security gateway which protects services, network traffic, and application data. These capabilities will be demonstrated in the following scenario: an aerospace company, Alpha Aerospace (AA), is engaged in developing fuel-efficient aircraft. AA is looking into optimizing its wing design to decrease fuel consumption. To achieve this, it will need a set of mathematical algorithms, High Performance Computing (HPC) resources, as well as secure storage sites where to maintain the results. Alpha turns to a third party collaboration manager, Epsilon, which will look up suitable partners. Eventually three partners are invited: Bêta Algorithms offers computation algorithms; Gamma Computing offers HPC; and Delta Storage offers secure storage. The high-level interaction is as follows: (1) an Alpha designer locates an algorithm at Beta to process wing data with; (2) the designer pushes the raw data with the algorithm retrieved in (1) to Gamma Computing where a job is created with the appropriate QoS and level of security; (3) the calculation job eventually terminates and sends its output to the data store at Delta Storage; (4) the Alpha Aerospace designer can now use the data stored at Delta.

3. Technical Approach

In distributed environments we cannot authenticate users or services against one single identity store. Yet there is a need to share an enterprise's users' identities with another enterprise. In order to achieve this, we can use the SOI-STS developed at BT to translate and contextualize a user's/service's internal identity into a collaboration-wide virtual identity.

The SOI-STS implementation that we will demonstrate is a WS-Trust-based web service which issues and validates security tokens that can be used to sign and/or encrypt XML messages. The STS can broker user attributes that can be used in access control decisions. Lastly, the STS is also responsible for federation establishment between each provider's STS. In our scenario, Alpha Aerospace's STS will contain the list of users at Alpha that wish to take part in the collaboration. These users can have different attributes (e.g. 'Designer') depending on their role in the collaboration. These will then be checked against a PDP for access control.

Because there is no longer a single identity store and due to the distributed nature of SOA, using access control lists or enterprise-based hierarchical decisions to control access to resources is no longer sufficient. Role-based access control is al-

so limited in an environment where we may not necessarily know a priori all the roles. There is a need for richer access control rules that can be authored by multiple administrators in different domains.
The SOI-AuthZ-PDP implements XACML: it can be used to express fine access control rules: who (subject) can do what (action) on which service (resource)?
The SOI-AuthZ-PDP responds to a request by locating a group of policies that apply to that request. Delegated policies are validated according to the XACML 3.0 administrative delegation model before use. The validation involves looking for root policies which authorize the delegated policies in accordance to the constraints defined in the administrative policies.
The SOI-SMG is a security application gateway / security appliance that securely exposes services on the basis of network traffic, message content, and application data. It acts as a message interceptor, decorator, router and enforcer. It is also the integration node in an SOA deployment (see following subsection).
The SOI-SMG is policy-based. The policies, expressed in XML, allow for rich, highly adaptive scenarios. The policies to be executed are located based on contextual information and therefore the SOI-SMG can be used in several collaborations concurrently while maintaining clear message flow segregation.
The SOI-SMG can express rules that will encrypt parts of an XML (SOAP) message e.g. with different keys if the parts are aimed at different recipients. Messages can also be signed to ensure message integrity. The key benefit is the ability to express these rules with the high-level policy language which translates into a graphical language within the SOI-SMG's management interface. The SOI-SMG is highly adaptive and can be reconfigured at runtime with zero downtime to cater for new security requirements or changes in deployment.
We have also envisioned a new policy framework model which clearly separates concerns between enforcement actions (this specifies the enforcement state, the actions that are to be enacted, their execution conditions), interceptor actions (this contains mapping between each available enforcement action and the computational entity that executes this action), and capability exposure (this is used to publish additional conditions for interacting with a protected resource). This model enables richer scenarios, as separate parts of the policies can be modified independently.

4. Innovation

The STS's key innovations lie in its modular architecture: it becomes easy to plug in new connectors e.g. identity store. Circles of trust become manageable: one can define & revoke trust relationships between providers at any time. The tokens issuance / validation can be so on the basis of a context: the STS will use a different federation definition and the issuance / validation process may be different alto-

gether. Compliance to standards eases integration with legacy applications, WSs, ESBs…
The PDP's foremost innovation is its implementation of the XACML 3.0 draft. This enables delegation and obligations. Delegation enables distributed Access Control and Authorization: policies can come from different administrative sources. The PDP also requires that the policies be signed. This ensures we can check the authenticity of the policies and run audits. Lastly, the PDP can enable contextualization and segregation of policy execution, enabling one PDP to act as separate PDPs by segregating policy sets based on contextual information.
The SOI-SMG, being an XML-driven security enforcement capability, is extremely flexible and can be used to implement a wide array of scenarios and security enforcement policies. Much like the STS and the PDP, the SOI-SMG can be contextualized: the execution of enforcement policies can be context-aware. In addition, the SOI-SMG enables security for Application networks: this means applications that are exposed as network-enabled services can securely integrate over the network. Through its content and context aware policies enforced at the enterprise boundary, the SMG enables deperimeterization: this increases the likelihood of more services being used and shared. Lastly, the SOI-SMG's key benefit is its extensible policy framework: by using XML to express policies, it lets administrators define and reuse finely granular rules.

5. Business Impact

The solution allows context-based policy differentiation enabling multiple scenarios to be run concurrently. The solution can constrain, combine, and validate policies from multiple authorities, breaking down monolithic views. The same policies can be validated in order to assess the correctness of the security enforced. The ability to audit those policies also enables compliance. This has become critical in a world teeming with laws and directives. Other benefits include the reduction of integration timescales of value-adding services. The SOI-SMG acts as an integration node: it encourages the reuse of common infrastructure thus reducing costs. Lastly, seamless service interaction within and outside corporate boundaries implies end-users will not feel the difference between home or remote services.

Acknowledgments The paper is partly the result of work from FP6 European projects TrustCoM and BEinGRID. It has also been fuelled by The SOA Architectures team at BT Innovate.

References

1. Dimitrakos T et al., Securing Business Operations in an SOA, BT Technology Journal, vol.27, no.1, April 2009