Optimizing Service Protection with Model Driven Security@run.time
Francis Wendpanga, Frédérique Biennier, Philippe Merle

To cite this version:
Francis Wendpanga, Frédérique Biennier, Philippe Merle. Optimizing Service Protection with Model Driven Security@run.time. 9th International IEEE Symposium on Service-Oriented System Engineering - IEEE SOSE 2015, Mar 2015, Redwood City, United States. pp.50-58. <hal-01109967>
Optimizing Service Protection with Model Driven Security@run.time

Wendpanga Francis Ouedraogo
Université de Lyon, CNRS INSA-Lyon, LIRIS UMR 5205,
20 avenue Albert Einstein,
69621 Villeurbanne Cedex, France
wendpanga-francis.ouedraogo@liris.cnrs.fr

Frédérique Biennier
Université de Lyon, CNRS INSA-Lyon, LIRIS UMR 5205,
20 avenue Albert Einstein,
69621 Villeurbanne Cedex, France
frederique.biennier@liris.cnrs.fr

Philippe Merle
Inria Lille - Nord Europe,
Parc Scientifique de la Haute Borne,
40 avenue Halley,
59650 Villeneuve d’Ascq, France
philippe.merle@inria.fr

Abstract—Enterprises are more and more involved in collaborative business. This leads to open and outsourcing all or part of their information system (IS) to create collaborative processes by composing business services picked in each partner IS and to take advantage of Cloud computing. Business services outsourcing and their dynamic collaboration context can bring lost of control on IS and new security risks can occur. This leads to inconsistent protection allowing competitors to access to unauthorized information. To address this issue, systematic security service invocations may be added, without paying attention to the business context leading to costly over protection. To address this issue, an adaptive security service model deployment is required to provide a business service consistent protection by taking into account the collaboration context (business service data criticality, partners involved in the collaboration, etc.), and the cloud deployment and execution environment. In this paper, we propose an adaptive security model based on MDS@run.time, the marriage of Model Driven Security (MDS) and Models@run.time approaches, allowing to select at runtime the appropriate security components to apply. The MDS approach is used to generate security policies, which are interpreted at runtime and load appropriate security mechanisms depending on the context (which takes advantage of the Models@run.time approach) ensuring business process end to end protection. A proof of concept prototype is built on top of the OW2 FraSCAti middleware, validating our proposition efficiency. Our experiments and simulations show that MDS@run.time improves the system efficiency when the over-protection risk rate increases.

I. INTRODUCTION

Today Web 2.0 development calls for a new and distributed IT infrastructure to fit the cloud models to allow an efficient and distributed execution across the Web. As data and services hosted in a cloud are let out by their owner, new security requirements emerge in order to support a long-life due usage control. This trend is reinforced due to the lack of trust on such cloud organisation [1] and the rather poor adaptability level of the current security policies are often seen as braking forces to such XaaS developments.

Unfortunately, information system security economics have mostly been designed for well-perimetrised systems. Such security strategy is based on identifying threats and vulnerabilities and implementing counter-measures to reduce these risks. Different methods and tools (EBIOS, CERT/Octave, SNA, Safe/CISCO)\(^1\) are available to implement this security strategy vision, i.e., facing identified vulnerabilities and reducing costs of security risks in a well-perimetrised and rather static environment. This static and perimetrised vision does not fit the multi-contextual execution environment involved by the service paradigm as a service can be invoked in different contexts. This may lead to inconsistent security deployment, under-protecting core information/process while running services in a new risky context or to an inefficient over-protection, locking the corporate information system access. Focusing on the service field, security has received a special attention over the last years [2]. Older works [3] focus on key technologies to support basic interoperable and standardised security services (mostly regarding transport security, message integrity and confidentiality, and even federation management to support cross authentication, etc.). The OASIS service reference model [4] takes advantage of the policy specification to trust management, authentication, authorisation and other security functions in the service model description but it does not allow to link these security features nor the security threats to the dynamic execution context of a service. This may lead to systematic and costly over protection when even useless security services are deployed or to risky under protection when useful security services are omitted.

Two other trends are interesting. Firstly, Model Driven Security (MDS) proposes to capture security policies as first-class models. MDS has already successfully applied to industrial systems [5], process-oriented systems [6], complex distributed systems [7], and multi-cloud context [8]. Nevertheless, MDS cannot take into account runtime contexts because security policy models are only considered as design/development time entities. Secondly, Security as a Service (SecaaS) [9] considers security mechanisms as reusable runtime entities. Unfortunately, the SecaaS approach is rarely implemented in a service-oriented way.

To overcome these limits, we propose a Model Driven Security@run.time approach that considers security policies as models interpreted at runtime [10] and that identifies the security requirements fitting the execution context. Plugged on the middleware used to implement the service system, our MDS@run.time component outsources the security management from the business service and provides an ad-hoc security

mediation, i.e., select, compose and orchestrate security services (SecaaS) according to the execution context. A proof of concept has been developed on the OW2 FraSCAti middleware and used to evaluate our proposal. Our experiments and simulations show that MDS@run.time improves the system efficiency when the over-protection risk rate increases.

After presenting the context and state of the art (Section II), we introduce a motivating example (Section III) before presenting our MDS@run.time architecture (Section IV) and evaluating it (Section V) before presenting further works (Section VI).

II. CONTEXT AND STATE OF THE ART

Taking advantage of both the agility provided by the service selection/composition/orchestration mechanisms and of the interoperability provided by the systematic use of Web services related standards, collaborative business processes can be designed as a composition of different business services picked from the partner’s own information system, challenging for a consistent protection fitting each partner own security requirements.

To this end, some security annotations on UML diagrams (such as the multi-purpose UMLSec [11] or the rather access control oriented SecureUML [12] domain specific languages) or BPMN diagrams [13] can be specified while designing a collaborative business process. As far as service-based business process implementation is concerned, these works have led to different frameworks such as OpenPMF [14] or SECTET [15] that take advantage of the Model Driven Security engineering [16] to generate security policies depending on the requirements associated to the business process model. Nevertheless, none of them support the full transformation process: While BPSec [17] is focused on the requirement engineering part, including CIM (Computation Independent Model) and PIM (Platform Independent Model) models, SECTET and OpenPMF provide PIM, PSM (Platform Specific Model) and code generation features. Moreover, the generation process is achieved according to a static environment vision (perimetrised process and well-known deployment platform), leading to define different policies depending on the business context. This complexifies the policy management and limits a consistent protection evolution as modifications are achieved locally.

To overcome this limit and provide a consistent protection fitting the different service invocation contexts, we believe that a service should not be duplicated and that its protection should be outsourced from the service body, i.e., defined as an associated protection policy enriched according to the different execution contexts. Such an approach involves to structure security policies depending on the protection services that must be fulfilled.

To this end, one can use the security service organisation proposed by OASIS in its service reference architecture [18] that allows to outsource security management from the business service implementation. As presented in Table I, the different protection services are split according to three implementation layers:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Network</td>
<td>secure network infrastructure</td>
<td>IPsec for VPN</td>
</tr>
<tr>
<td>Transport</td>
<td>Secure communication channel, i.e. encrypt information</td>
<td>TLS/SSL</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Secure storage and message exchanged based encryption</td>
<td>WS-Security: XML-Encryption</td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>Application</td>
<td>signed data stored and exchanged</td>
<td>WS-Security: XML-Signature</td>
</tr>
<tr>
<td>Availability</td>
<td>Network</td>
<td>DoS protection via Firewall, IDS</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Management of QoS</td>
<td>BSLA (Business Service Level Agreement)</td>
<td></td>
</tr>
</tbody>
</table>

III. MOTIVATING EXAMPLE

The reusing ability provided by Web services, that can be selected, composed, and orchestrated in different contexts, challenges a strict deployment of security services to provide the convenient level of protection. This can lead to a costly over-protection. A motivating example could be provided by a service used to check mechanical specifications of a new product, as shown in Fig. 1. As data produced and acceded by this service have a high patrimonial value for the enterprise, then different protections can be deployed:

- Strong authentication to support specification traceability, i.e., knowing who has achieved/worked on the specifications.
- Restricted access control to allow only people from the enterprise or some authenticated partners to accede to this service.
- Cryptographic algorithm to protect exchanged data.

This service can be invoked in different workflows, as shown in Fig. 1:

- The corporate Computer Aid Design CAD (CAD) modelling system can invoke this service to check the intermediate specification consistency (75% of all the invocations),
- The Product Lifecycle Management (PLM) system can invoke this service to check the product information before integrating these data in its data base (10% of all the invocations),
- Other CAD modelling systems used by partners to exchange new requirements can also invoke this service to check the ordered specifications involved in a collaborative engineering project (15% of all the invocations).

Of course, depending on the invocation context of this service, some security constraints could be relaxed:
For internal validation achieved via an invocation by the CAD modelling system, no traceability is needed.

When the validation service is invoked via the PDM system, the operation must be logged.

The corporate network is protected so data can be exchanged safely.

External access to the corporate network is provided to employees and protected via a VPN.

When a collaboration is set with a partner, this specification validation service can be invoked from the partner CAD modeller to check the requirements. In this case, the different actions must be logged. All the actions achieved via the service and restricting the access to only authorised persons.

Fig. 1: Motivating example

These protection requirements lead to identify execution contexts for the specification validation service, as shown in Fig. 1:

- Context 1: Internal checking invoked by enterprise study board, thanks to their CAD Modelling System is a safe environment, no protection is required.
- Context 2: Certified requirement checking invoked by members of the enterprise from the PLM service to store checked specification. Authentication and non repudiation are required.
- Context 3: Collaboration specification checking invoked by a partner are from its CAD system to validate the order specification. Due to business constraints, authentication, authorization, and non repudiation are necessary whereas the opened execution platform requires data encryption.

Listing 1. Security policies associated to the validateSpec resource

Listing 2. AccessControlList.xml authorization file

As this business service can be invoked dynamically by ad-hoc collaborative workflows, protection services must be deployed according to the execution context paying attention on both organisational (i.e., which partner, trusted or not, invokes the service) and technical (which kind of cloud hosts the collaborative workflow, which kind of transport service is provided, etc.) environments. The protection requirements are defined globally in the security policies attached to the different business services (see Listing 3, Line 3). These security policies are seen as security models at runtime that

```xml
<accessControlList>
  <context type="Network/IP" value="193.148.219.5, 193.148.219.25"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/>
  <context type="Network/DNS" value="www.m3.org, www.m3.org"/
```
will be used at runtime by the security mediator to select, compose and orchestrate the security services depending on the execution context.

```
1 <wsdl:binding name="mechanicalServiceSoapBinding" type="
2  http://schemas.xmlsoap.org/soap/http">
3  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http" />
4  <wsdl:operation name="validateSpec" ns="mds"/>
5  <wsdl:input name="validateSpec"/>
6  <wsdl:output name="validateSpecResponse"/>
7  <soap:body use="literal"/>
8 </wsdl:operation>
9 </wsdl:binding>
```

Listing 3. Link the security policy with the ValidateSpec operation of the Mechanical system service

In our example, the ValidateSpec service and the related information must be protected in the different contexts. The confidentiality requirement impacts both application layer, which is in charge of the access control, traceability, and transport layer (see Listing 1). The systematic composition of the authorization, traceability and confidentiality services may be costly. Table II shows a comparison of service execution time according to the context (Network Internal/External used to interact with the service, and the services attended to the collaboration). Here CADService invokes ValidateSpec without any security implementation. PLMService can invoke the ValidateSpec service with the traceability requirement. For other services, in addition to the traceability requirement, both authorization and encryption are required to invoke ValidateSpec. Testing conditions and environment are detailed in Section V.

<table>
<thead>
<tr>
<th>Context</th>
<th>Security services involved/ValidateSpec</th>
<th>Execution time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context 1</td>
<td>No security mechanism is required</td>
<td>64</td>
</tr>
<tr>
<td>Context 2</td>
<td>Authentication and Non Repudiation</td>
<td>80</td>
</tr>
<tr>
<td>Context 3</td>
<td>Context 2 security services + Authorization and Confidentiality</td>
<td>86</td>
</tr>
</tbody>
</table>

To avoid this costly over protection or risky under protection depending on the runtime environment vulnerability, we propose to turn these security policies as Models@run.time so that they can be analysed to select, compose and orchestrate the most convenient security services depending on the exact runtime environment. This requires a new architecture to outsource the security management as a new high-level service that can be plugged on the hosting middleware.

IV. MODEL DRIVEN SECURITY@RUN.TIME

Context-aware security management has lead to different works for more than the decade from the early adaptation of access control rules [19] to SLA and policy orchestration integration in cloud [20]. Nevertheless, these works do not fit the service dynamic reusing abilities and different policies are attached to each execution context. To overcome this limit, we propose to extend the Model Driven Security approach to a MDS@run.time strategy in order to capture the execution context while deploying the security services. This execution context integrates the business process related context defined by OASIS and information related to the execution platform. By this way, a single security policy gathers all the protection requirements and deployment can be outsourced from the business service and managed in a context-aware security strategy. We first present our context model before detailing our architecture.

A. Execution context specification

The execution context is defined as a set of functional, organisational and technological specifications, which determine the choice of security measures to perform. The functional specification allows knowing the types of information (strategic, personal, financial, etc.) used or handled by each service and the information sensitive level (top secret, secret, confidential, restricted, unclassified). This specification aims to know which protection and level of protection are required in terms of confidentiality and/or integrity. Organizational specification focused on access control and other security criteria such as availability and non-repudiation. It allows to answer to the questions: Who can access and interact with process resources? By using which means, such as networks, devices, etc.? From which locality and at which time? Moreover this organization specification allows defining both obligation and restriction constraints in terms of access control. Based on these risk-analysis specification, a consistent security policy can be defined for each service gathering the different protection services. As show in TABLE II, this can be rather costly. As a consequence, we integrate contextual information to motivate the use of the different security assertions depending of the context. To this end, our formal context model is defined by different parameters:

- **Who**: Refer to the business service invoking the protected service.
- **For who**: Specify the user for whom the service is invoked.
- **From where**: Specify the network specification.
- **When**: Define time depending of the protection management.

Thanks to this extended context specification, one can select the security assertion to be composed and deployed at runtime.

B. MDS@run.time architecture

To deploy our adaptive security model [21], we take advantages of the SOA distributed implementation. Here an SOA middleware plays an intermediary role between the client and the service provider. It is a software component, which is located between the operating system and business applications, and offers a high level abstraction for building distributed applications. It allows business service integration and management, and provides access to various external services. It is an integration solution, which implements a fully distributed architecture deployed on multiple nodes, providing services such as data processing or Content Based Routing (CBR), and a higher level of interoperability by systematically using standards such as XML, WS-* specifications [3].

Our outsourced context-aware security architecture [22] is plugged on the middleware capturing the service invocation (see Fig. 2). A middleware specific interceptor intercepts the service invocation (Step 1) and routes this request to the MDS@run.time component (Step 2). Based on the request, the
MDS@run.time component retrieves all the policies associated to the invoked business service. Thanks to the environment characteristics (cloud platform, devices and network used, etc.) (Steps 3 and 4), only the security policies matching the current context are selected and composed to implement the required protection. Then the MDS@run.time component orchestrates the security service invocations (Steps 5 and 6) by using the security as a service component, which implements the security mechanisms defined in each policy (Steps 5 and 6). If succeeded, the invoker is granted and security mechanisms are applied, the MDS@run.time component routes back the business service/middleware (Steps 7 and 8). But in unsuccessful case, the business service is not invoked and an error message is returned to the invoker.

Fig. 2. MDS@run.time architecture

The MDS@run.time architecture is composed of three components as illustrated in Fig. 3: Interceptor, MDS@run.time, and Security as a Service. This design allows us to clearly separate concerns: specific middleware interception, MDS@run.time mediation, and security services. Moreover, this design provides portability of both MDS@run.time and Security as a Service components across different middleware platforms.

The specific middleware interceptor is defined to capture and route the interactions between the business service and the middleware to our MDS@run.time component. But as how request interception is done is specific to each middleware, this component must be specifically implemented for each middleware, see Section V-A for details on how this component is implemented for the OW2 FraSCAti middleware.

Fig. 3. MDS@run.time components

The MDS@run.time component is the core element of our context-aware architecture [22] and is in charge of identifying the assertion to implement, composing and orchestrating the security services accordingly. It includes three components as illustrated in Fig. 3:

- The security mediator is the entry point of this component. It analyses the interaction received from the interceptor that defines the invoked service and the execution environment context information identifying some context parameters as:
  - Who, i.e., the service invoking the business service.
  - When, i.e., capture the invocation time.
  - From where, i.e., capture the geographic location of the calling service.

Then, it invokes the policy manager to extract the policy associated to the invoked service and the context manager, which will compose and deploy the security services depending on the context.

- The PolicyManager component manages the security policies. It receives from the Mediator the resource or service reference requested and the link to the policy file. It returns to the Mediator the list of security policies to apply.

- The ContextManager component analyses security policies associated to services and identifies the different policies to be applied according to the user context, the execution environment and security policies associated to the client and service provider. It also provides to the Mediator component information such as policies and policy rules related to the execution context. These policy rules are used by the Mediator component to call the technical security services.

To support a fully outsourced security strategy, this architecture is enriched with a Security as a Service (SecaaS) component, which gathers implementations of the different security services based on standards such as:

- The Authentication component is used to prove the user identity (of human or other service). This component receives from the SecaaS component the policy rule to apply, extracts information about the security pattern and invokes the security mechanism to be applied. It can be a weak authentication mechanism such as login/password or strong authentication such as One Time Password (OTP) or two factors authentication. This Authentication component includes subcomponents such as the SSORegistry (Single Sign On Registry) component used to store information about authentication of sessions and to allow to retrieve user information without restarting authentication.

- The Authorization component manages access to resources and services, and allows grant or deny the user access to them. As the Authentication component, it receives the security policy rule and invokes the authorization mechanism to be applied. This mechanism can be based on an authorization by role
(RBAC) implemented by the XACML authorization protocol or a simple Access Control List (ACL).

- The Encryption component provides data and messages encryption/decryption mechanisms. It also provides secure protocols using secure communication (SSL).
- The Integrity component ensures the integrity of exchanged data and messages by using message signatures or hash functions.
- The NonRepudiation component is responsible for recording user actions (authentication, access to data or service, data modification/destruction, etc.). This information can then be used for auditing and monitoring.
- The Availability component is responsible for the services’ availability providing access to the service or a clone (redundant service) thereof if the original target service is unavailable. This component also provides backup mechanism to restore system data and services after disaster.

The Encryption, Integrity and NonRepudiation components can use security protocols such as WS-Security XML Encryption and XML Signature, which provide encryption and signing exchanged message mechanisms.

V. Evaluation

Our MDS@run.time architecture is designed to support an outsourced security deployment. As presented in Fig. 2, it is designed in a non intrusive way for both services and middleware. To evaluate our proposal, we present in the following sub-sections a Proof of Concept prototype plugged on the OW2 FraSCAti middleware before evaluating its performance level on the motivating example presented in Section III, and comparing the results with other approaches to manage security in collaborative processes.

A. Organisation of the Proof of Concept prototype

FraSCAti\(^2\) [23] is an open source middleware framework to build, develop, deploy, execute, and manage adaptable service-oriented business applications. FraSCAti is based on the OASIS Service Component Architecture (SCA) standard\(^3\). FraSCAti applications can be deployed in different clouds such as Amazon EC2, Appfog, CloudBees, DELL KACE, dotCloud, Eucalyptus, Jelastic, Heroku, OpenShift, Windows Azure, as discussed in [24], [25], [26]. The adaptability at design time is based on the fact that the FraSCAti platform was designed as a plugin-based architecture to adapt it to different execution environments and to select on demand the required application functionalities composing a FraSCAti instance [27]. The adaptability at execution time is based on the FraSCAti reflective features, which encompass introspection and reconfiguration of applications at runtime [28]. For dealing with web services and REST, FraSCAti embeds Apache CXF\(^4\), a well-known open source services framework. To ensure the business process security deployed on cloud infrastructures, we propose a MDS@run.time framework based on SCA components, which can be plugged to the FraSCAti platform. Our prototype takes advantage of Aspect Oriented Programming (AOP [29]) features and of the SCA model, both provided by FraSCAti, to deploy the three Interceptor, MDS@run.time and Security as a Service components shown in Fig. 3.

SCA provides the notion of intent, which is an abstraction for designating a non-functional property such as security, transaction, logging, etc. With FraSCAti, SCA intents are implemented as SCA components, then both business and non-functional concerns are designed then implemented in the same framework, aka SCA.

The Intent component is responsible for detecting and intercepting business services invoked by clients. This component uses AOP techniques provided by FraSCAti to perform actions before, during and after each business service invocation. These techniques use the Apache CXF interception mechanism. The Intent component creates a Request object, which plays the intermediary role between the FraSCAti middleware and security services. This object provides a bidirectional interface that allows the Intent component to formalize the interaction messages received from Apache CXF and also to specify orders towards Apache CXF. The Request object ensures a total independence between our MDS@run.time component and the underlying service-oriented middleware, allowing on one hand the security services to be able to deploy and run on any other middleware and on another hand to deploy on a specific platform just the required security services.

In our MDS@run.time prototype, we reused and enhanced the Enterprise Java XACML framework\(^5\). The data encryption function is AES 128-bit. Authentication by login/pwd and non-repudiation by logs are implemented in an ad hoc way. For authentication, unique tokens are generated to avoid to manually re-authentifying when accessing other services (SSO). As the thread model of Apache CXF is to affect a thread to each incoming request, then potentially concurrent threads can execute our security services. The MDS@run.time security services must then be protected against concurrent accesses via critical sections like Java monitors.

B. Performance evaluation

Our performance evaluation is based on the use case presented in Section III, focusing on the mechanical system ValidationSpec operation. This operation is implemented thanks to a service associated to a security policy including non repudiation (see Listing 1, Lines 2-9), access control (Lines 10-17) using ACL (Lines 23-25) and confidentiality (Lines 28-38). As far as the collaborative service is concerned, the business service is encapsulated in a MechanicalService, which is associated to the convenient security policy and refers to the MDS@run.time composite (Listing 4, Line 4). By this way, the business service can be intercepted and MDS@run.time is invoked before invoking the business service itself.

---

\(^1\) <composite name="Mechanical" >
\(^2\) <service name="Mechanical" promote="MechanicalComponent/Converter" >
\(^3\) <interface java interface="mechanical.api.mechanicalService" />
\(^4\) <http://frascati.ow2.org>
\(^5\) <http://cxf.apache.org>
\(^6\) <http://www.oasis-open.ca/sca>
\(^7\) <http://cxf.apache.org>
\(^8\) <https://code.google.com/p/enterprise-java-xacml/>
To evaluate the impact of our MDS\textregistered run.time with FraSCAti prototype on the service execution time, we set a benchmarking environment using FraSCAti version 1.6 with Oracle Java Virtual Machine 1.7.0_51 on Microsoft Windows 7 Professional (32 bit) using a 2.54GHz processor Intel(R) Core(TM)2 Duo CPU with 4Go of memory.

Firstly, we measured the execution time of each component: The business service without invoking our security architecture (Measure 1 in Table III), the FraSCAti service interception (Measure 2), the mediator component (Measure 3), the authentication service (Measure 4), the non-repudiation service (Measure 5), the authorization service (Measure 6), and the confidentiality service (Measure 7). We manage a benchmark loop to compute an average execution time on 1000 client requests, so that extra factor impacts, such as bootstrapping effects, Just-In-Time compilation, etc., can be smoothed.

\textbf{TABLE III. EXECUTION TIME OF MDS\textregistered run.time COMPONENTS}

<table>
<thead>
<tr>
<th>No</th>
<th>Component</th>
<th>Average execution time (ms)</th>
<th>Systematic protection</th>
<th>Context 1</th>
<th>Context 2</th>
<th>Context 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FraSCAti + Apache CXF + Business service</td>
<td>58</td>
<td>58</td>
<td>58</td>
<td>58</td>
<td>58</td>
</tr>
<tr>
<td>2</td>
<td>FraSCAti Interceptor</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td><a href="mailto:MDS@run.time">MDS@run.time</a></td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>Authentication</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>NonReputation</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>Authorization</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Confidentiality</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>80</td>
<td>64</td>
<td>80</td>
<td>86</td>
<td>86</td>
</tr>
</tbody>
</table>

The execution meantime for a systematic protection, i.e., all security services are invoked but without our MDS\textregistered run.time components, is 80 milliseconds (Column 4 in Table III). The execution meantime for Context 1, involving our MDS\textregistered run.time components but no security services, is 64 milliseconds, i.e., the business service execution time plus the MDS\textregistered run.time overhead. The execution meantime for Context 2, involving MDS\textregistered run.time plus authentication and non-repudiation services, is 80 milliseconds. The execution time of Context 3, involving all security services, is 86 milliseconds.

So, the first result is that the interception and mediation process (Measure 2 plus 3 in Table III) represents only 6 milliseconds, i.e., around 7\% of the total execution time of Context 3. This overhead could certainly reduced within an industrial implementation of MDS\textregistered run.time by for instance merging/moving the implementation code of both MDS\textregistered run.time and Security as a Service components into the interceptor. But then we will lose the portability of these components on different middleware platforms. Then this is an implementation trade-off between performance and portability. However this demonstrates that our MDS\textregistered run.time approach, i.e., interpretation of security policies at runtime, introduces a small overhead compared to a systematic deployment of the different security services.

Table IV reports the unitary execution time and the total execution time split according to the three contexts paying attention of the occurrence rate of each context (see Section II). It shows that our security adjustment allows to reduce the total execution time for about 14\% compared to the systematic protection (over-protection) scenario.

\textbf{TABLE IV. EXECUTION TIMES EVALUATION}

<table>
<thead>
<tr>
<th></th>
<th>With our approach</th>
<th>Systematic protection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Context 1</td>
<td>Context 2</td>
</tr>
<tr>
<td>Execution time for one invocation (ms)</td>
<td>64</td>
<td>80</td>
</tr>
<tr>
<td>Rate of 1000 invocations</td>
<td>75%</td>
<td>10%</td>
</tr>
<tr>
<td>Total execution of each context</td>
<td>48 000</td>
<td>8 000</td>
</tr>
<tr>
<td>Total of execution time for 1000 invocation (ms)</td>
<td>68 900</td>
<td>80 000</td>
</tr>
</tbody>
</table>

We extend this benchmark to integrate business services that request longer or smaller computation times (see Table V) to compare the cost of context analysis and of the dynamic security composition and orchestration at runtime. Our simulation uses several business services whose execution times vary from 10 ms to 100 ms. We set 2 reference execution contexts, one required no security deployment (Context 1) whereas the other requires the maximum protection (i.e systematic protection required in Context 3 associated to our motivating example). Measures are achieved using different rates for Context 1 (from 10\% to 100\%). The results show that the MDS\textregistered run.time maximum cost varies from 18.75\% of the smaller service execution time to 4.9\% for the bigger one when a systematic protection is required. On the opposite, MDS\textregistered run.time exhibits a benefit of 13\% to 50\% of the execution time when no protection is required. These results show that the overhead involved by our MDS\textregistered run.time architecture can be rather neglected compared to the large overhead introduced by the systematic invocation of (often) useless security services provided that the no protection rate is greater than 30\% as shown in Fig. 4.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig4.png}
\caption{Variation of MDS\textregistered run.time execution cost according to three business services}
\end{figure}

\textbf{C. Comparison with other related works}

As stated in Section II, different works on Model Driven Security [16] have been conducted to integrate security annota-
TABLE V. EXECUTION TIMES FOR A PANEL OF 1000 INVOCATIONS OF BUSINESS SERVICES WHERE THE NO PROTECTION RATE EVOLVES FROM 0% TO 100%

<table>
<thead>
<tr>
<th>Systematic protection</th>
<th>0%</th>
<th>10%</th>
<th>20%</th>
<th>30%</th>
<th>40%</th>
<th>50%</th>
<th>60%</th>
<th>70%</th>
<th>80%</th>
<th>90%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1 (10ms)</td>
<td>32000</td>
<td>32000</td>
<td>32000</td>
<td>31400</td>
<td>29200</td>
<td>27000</td>
<td>24800</td>
<td>22600</td>
<td>20400</td>
<td>18200</td>
<td>16000</td>
</tr>
<tr>
<td>S2 (20ms)</td>
<td>42000</td>
<td>42000</td>
<td>41400</td>
<td>41400</td>
<td>39200</td>
<td>37000</td>
<td>34800</td>
<td>32600</td>
<td>30400</td>
<td>28200</td>
<td>26000</td>
</tr>
<tr>
<td>S3 (30ms)</td>
<td>52000</td>
<td>52000</td>
<td>51400</td>
<td>51400</td>
<td>49200</td>
<td>47000</td>
<td>44800</td>
<td>42600</td>
<td>40400</td>
<td>38200</td>
<td>36000</td>
</tr>
<tr>
<td>S4 (40ms)</td>
<td>62000</td>
<td>62000</td>
<td>61400</td>
<td>61400</td>
<td>59200</td>
<td>57000</td>
<td>54800</td>
<td>52600</td>
<td>50400</td>
<td>48200</td>
<td>46000</td>
</tr>
<tr>
<td>S5 (50ms)</td>
<td>72000</td>
<td>72000</td>
<td>71400</td>
<td>71400</td>
<td>69200</td>
<td>67000</td>
<td>64800</td>
<td>62600</td>
<td>60400</td>
<td>58200</td>
<td>56000</td>
</tr>
<tr>
<td>S6 (60ms)</td>
<td>82000</td>
<td>82000</td>
<td>81400</td>
<td>81400</td>
<td>79200</td>
<td>77000</td>
<td>74800</td>
<td>72600</td>
<td>70400</td>
<td>68200</td>
<td>66000</td>
</tr>
<tr>
<td>S7 (70ms)</td>
<td>92000</td>
<td>92000</td>
<td>91400</td>
<td>91400</td>
<td>89200</td>
<td>87000</td>
<td>84800</td>
<td>82600</td>
<td>80400</td>
<td>78200</td>
<td>76000</td>
</tr>
<tr>
<td>S8 (80ms)</td>
<td>102000</td>
<td>102000</td>
<td>101400</td>
<td>101400</td>
<td>99200</td>
<td>97000</td>
<td>94800</td>
<td>92600</td>
<td>90400</td>
<td>88200</td>
<td>86000</td>
</tr>
<tr>
<td>S9 (90ms)</td>
<td>112000</td>
<td>112000</td>
<td>111400</td>
<td>111400</td>
<td>109200</td>
<td>107000</td>
<td>104800</td>
<td>102600</td>
<td>100400</td>
<td>98200</td>
<td>96000</td>
</tr>
<tr>
<td>S10(100ms)</td>
<td>122000</td>
<td>122000</td>
<td>121400</td>
<td>121400</td>
<td>119200</td>
<td>117000</td>
<td>114800</td>
<td>112600</td>
<td>110400</td>
<td>108200</td>
<td>106000</td>
</tr>
</tbody>
</table>

TABLE VI. VARIATION OF MDS@RUN.TIME EXECUTION COST COMPARED TO BUSINESS SERVICES EXECUTION TIMES DEPENDING ON "THE NO PROTECTION" CONTEXT RATE

<table>
<thead>
<tr>
<th>Business services</th>
<th>0%</th>
<th>10%</th>
<th>20%</th>
<th>30%</th>
<th>40%</th>
<th>50%</th>
<th>60%</th>
<th>70%</th>
<th>80%</th>
<th>90%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1 (10ms)</td>
<td>-18,75%</td>
<td>-11,88%</td>
<td>-5,00%</td>
<td>1,88%</td>
<td>8,75%</td>
<td>15,63%</td>
<td>22,50%</td>
<td>29,38%</td>
<td>36,25%</td>
<td>43,13%</td>
<td>50,00%</td>
</tr>
<tr>
<td>S2 (20ms)</td>
<td>-14,29%</td>
<td>-9,05%</td>
<td>-3,81%</td>
<td>1,43%</td>
<td>6,67%</td>
<td>11,90%</td>
<td>17,14%</td>
<td>22,38%</td>
<td>27,62%</td>
<td>32,86%</td>
<td>38,10%</td>
</tr>
<tr>
<td>S3 (30ms)</td>
<td>-11,54%</td>
<td>-7,31%</td>
<td>-3,08%</td>
<td>1,15%</td>
<td>5,38%</td>
<td>9,62%</td>
<td>13,85%</td>
<td>18,08%</td>
<td>22,31%</td>
<td>26,54%</td>
<td>30,77%</td>
</tr>
<tr>
<td>S4 (40ms)</td>
<td>-9,68%</td>
<td>-6,13%</td>
<td>-2,58%</td>
<td>0,97%</td>
<td>4,52%</td>
<td>8,06%</td>
<td>11,61%</td>
<td>15,16%</td>
<td>18,71%</td>
<td>22,26%</td>
<td>25,81%</td>
</tr>
<tr>
<td>S5 (50ms)</td>
<td>-8,33%</td>
<td>-5,28%</td>
<td>-2,22%</td>
<td>0,83%</td>
<td>3,89%</td>
<td>6,94%</td>
<td>10,00%</td>
<td>13,06%</td>
<td>16,11%</td>
<td>19,17%</td>
<td>22,22%</td>
</tr>
<tr>
<td>S6 (60ms)</td>
<td>-7,32%</td>
<td>-4,63%</td>
<td>-1,95%</td>
<td>0,73%</td>
<td>3,41%</td>
<td>6,10%</td>
<td>8,78%</td>
<td>11,46%</td>
<td>14,15%</td>
<td>16,83%</td>
<td>19,51%</td>
</tr>
<tr>
<td>S7 (70ms)</td>
<td>-6,52%</td>
<td>-4,13%</td>
<td>-1,74%</td>
<td>0,65%</td>
<td>3,04%</td>
<td>5,43%</td>
<td>7,83%</td>
<td>10,22%</td>
<td>12,61%</td>
<td>15,00%</td>
<td>17,39%</td>
</tr>
<tr>
<td>S8 (80ms)</td>
<td>-5,88%</td>
<td>-3,73%</td>
<td>-1,57%</td>
<td>0,59%</td>
<td>2,75%</td>
<td>4,90%</td>
<td>7,06%</td>
<td>9,22%</td>
<td>11,37%</td>
<td>13,53%</td>
<td>15,69%</td>
</tr>
<tr>
<td>S9 (90ms)</td>
<td>-5,36%</td>
<td>-3,39%</td>
<td>-1,43%</td>
<td>0,54%</td>
<td>2,50%</td>
<td>4,46%</td>
<td>6,43%</td>
<td>8,39%</td>
<td>10,36%</td>
<td>12,32%</td>
<td>14,29%</td>
</tr>
<tr>
<td>S10(100ms)</td>
<td>-4,92%</td>
<td>-3,11%</td>
<td>-1,31%</td>
<td>0,49%</td>
<td>2,30%</td>
<td>4,10%</td>
<td>5,90%</td>
<td>7,79%</td>
<td>9,51%</td>
<td>11,31%</td>
<td>13,11%</td>
</tr>
</tbody>
</table>

Our MDS@run.time vision overcomes these limits as:

- All requirements are gathered in a single protection policy attached to the business service, which policy is generated thanks to a fully automated generation process.
- Security deployment is outsourced from the business process orchestration process as the security policy is analysed dynamically according to the technological and organisational execution context.
- The security architecture is designed in a non-intrusive way and can fit multi-cloud deployment as it is plugged on the service middleware.

Moreover, our context definition enriches the context model proposed in the OASIS reference architecture with technical context information picked from the different cloud security models. So services can be secured on the fly. Thanks to the execution platform information, collected by the mediator component, security services are selected, composed and orchestrated in a transparent and consistent way, avoiding the costly over-protection and the risky under protection.

VI. CONCLUSION

Securing collaborative business processes deployed on cloud systems require paying attention on both organisational and platform-related vulnerabilities. Taking advantage of the intrinsic flexibility provided by the association of security policies to services, we propose to use them as Models@run.time to select, compose and orchestrate security services depending on the required protection and on the execution context. To this end, a MDS@run.time component is plugged on the middleware, intercepting service invocation and capturing context information. The experiment reported in this paper shows how our MDS@run.time architecture can be plugged on the OW2 FraSCAti middleware and reduce the execution time compared to a systematic over-protection approach. Further works will focus on the integration of more detailed platform models and on vulnerability monitoring loops so that our coarse-grained vision of the execution context will be refined to increase the protection efficiency.

REFERENCES


