POSTER: Protecting Information in Systems of Systems

Daniel Trivellato
Eindhoven University of Technology
The Netherlands
d.trivellato@tue.nl

Nicola Zannone
Eindhoven University of Technology
The Netherlands
n.zannone@tue.nl

Sandro Etalle
Eindhoven University of Technology & University of Twente
The Netherlands
s.etalle@tue.nl

ABSTRACT

Systems of Systems (SoS) are dynamic, distributed coalitions of autonomous and heterogeneous systems that collaborate to achieve a common goal. While offering several advantages in terms of scalability and flexibility, the SoS paradigm has a strong impact on system interoperability and on the security requirements of collaborating parties. In this demo we present a prototype implementation of POLIPO, a security framework that combines context-aware access control with trust management and ontology-based services to protect information in SoS.

Categories and Subject Descriptors

H.2.7 [**Information Systems**]: Database Management—*Security, integrity, and protection*

General Terms

Design, Security

Keywords

Systems of systems, security framework, protection of information, system interoperability

1. INTRODUCTION

Systems of systems (SoS) are coalitions of autonomous systems and services that collaborate to achieve a common goal. These coalitions are often dynamic, with systems joining and leaving, and involve parties employing different vocabularies, data models and organizational structures. Examples of SoS include Web Services, Mobile Ad-hoc Networks, air traffic control systems, etc. For the success of a coalition, parties may need to share sensitive information with the other parties in the SoS; nevertheless, this information should be accessed exclusively by authorized parties, which may vary depending on the context (e.g., in emergency situations, or based on the location of the requester).

Several security frameworks for SoS have been proposed. These frameworks can be divided into two categories: semantic frameworks [2, 9] and trust management (TM) frameworks [3, 4, 5]. Semantic frameworks rely on ontologies for the specification of access control policies and the definition of domain knowledge and context information. This enables interoperability among parties at the cost of limiting the expressive power of the policy language, which does not allow the specification of several types of security constraints (e.g., separation of duty). On the other hand, TM frameworks rely on an attribute-based approach to access control where access decision are based on digital certificates, called credentials. TM frameworks employ expressive policy specification languages to ensure data confidentiality and integrity; however, they either require all parties in an SoS to use the same vocabulary [4, 5], or do not provide a mechanism to align different vocabularies [3]. Thus, none of the existing frameworks satisfies all the requirements imposed by SoS.

In this demo we present POLIPO, the security framework for SoS that we have developed within the POSEIDON project, a joint project involving a number of industrial (Thales Nederland and Noldus) and academic partners. POLIPO combines context-aware access control with TM and ontology-based services [6, 7] to guarantee the protection of information (both data and security policies), autonomy and interoperability among the parties in an SoS. We show an application of the framework to a scenario in the Maritime Safety and Security (MSS) domain.

Copyright is held by the author/owner(s).
CCS'11, October 17–21, 2011, Chicago, Illinois, USA.
ACM 978-1-4503-0948-6/11/10.

2. THE POLIPO FRAMEWORK

In this section we introduce the POLIPO security framework and present its prototype implementation.

2.1 Framework Ingredients

As a first step towards the design of POLIPO, we identify the characteristic features of SoS to be the following:

- *Dynamicity*: SoS are constantly evolving. Systems may leave an SoS at any time while new systems may join the coalition, depending on the context or the progress towards the goal. Similarly, the information that systems need to exchange may be context-dependent.
- *Distribution*: each system in an SoS is an independent, complex system which belongs to a (possibly) different security domain and is governed by a different authority. Furthermore, parties may not know each other before joining the SoS.
- *Heterogeneity*: each system may adopt different data and organizational structures, and a different vocabulary to define the concepts and relationships in an application domain.

To address these challenges, the POLIPO framework combines techniques from the fields of computer security and knowledge representation. In particular, it relies on:

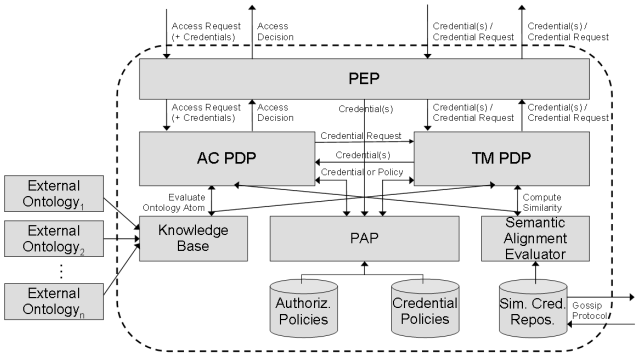


Figure 1: POLIPO Framework Architecture

- *Context-aware access control and TM to protect the confidentiality and integrity of information.* Context-aware access control is used to tackle the dynamicity of SoS: by incorporating context information (e.g., the location of the requester, the criticality of the situation) in access decisions, parties can specify flexible policies which adapt to different situations. TM, on the other hand, deals with the distributed nature of SoS. In TM, in fact, access decisions are based on the attributes of a requester, which are certified by means of digital credentials. Contrarily to identity-based approaches, grounding an access decision on the attributes of a requester allows parties to exchange information with (previously) unknown entities.
- *Ontology-based services to enable autonomy and interoperability among the parties in an SoS.* More precisely, parties refer to ontology concepts, relationships, and instances to assign a semantics to the terms used in their policies. In addition, ontologies are used to define the data and organizational structures of each party. This, combined with the use of semantic alignment techniques to map concepts and relationships from different ontologies, allows parties to use the vocabulary and structures they consider more appropriate within their system (thus accommodating parties' heterogeneity), while preserving mutual understanding with the rest of the coalition.

The context-aware ontology-based policy language and the semantic alignment technique employed in POLIPO are introduced in [6] and [7] respectively. In the next section we present the architecture of POLIPO and show how these techniques are combined into a unified framework.

2.2 Framework Architecture

The architecture of the POLIPO framework is shown in Fig. 1; the dashed line separates the local components (i.e., the trusted environment of a party) from the external world. The framework's architecture, inspired by XACML, consists of a set of core security components complemented by an ontology repository and the semantic alignment component. To facilitate the integration of the framework into existing systems, all the components have been designed as services, following the service-oriented architecture paradigm.

The *policy enforcement point* (PEP) is the interface of a party with the external world, and has three main tasks: (1) intercepting incoming requests for local resources, (2) contacting the appropriate *policy decision point* (PDP) to evaluate those requests, and (3) enforcing the decision of the PDP. Two types of requests are allowed: *access requests* and *credential requests*. Access requests are processed by the *access control PDP* (AC PDP), while credential requests by the *trust management PDP* (TM PDP).

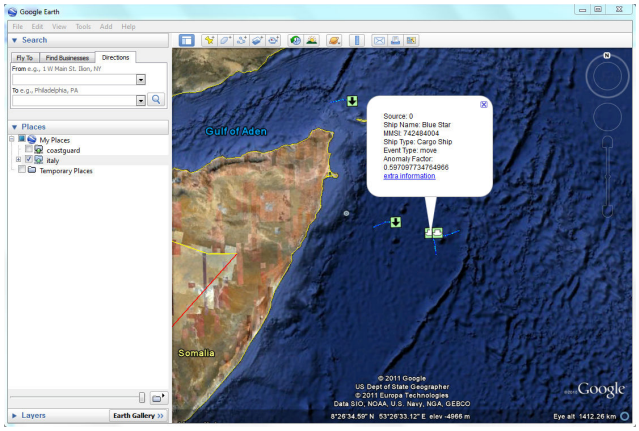
When it receives an access request, the AC PDP fetches the relevant authorization clauses through the *policy administration point* (PAP). If the clauses depend on some credential, the AC PDP requests them to the TM PDP, which takes over the responsibility of retrieving them. Once all the necessary credentials have been collected, the AC PDP determines the access decision. Similarly to the AC PDP, upon receiving a request the TM PDP fetches the applicable credential clauses and the locally available credentials through the PAP. The policy evaluation algorithm within the TM PDP defines the procedure to compute the answers to a credential request. In POLIPO we employ GEM [8], a policy evaluation algorithm that evaluates credential requests in a completely distributed way without disclosing the policies of parties, thereby preserving their confidentiality.

Both authorization and credential clauses are expressed in the logic-based policy language introduced in [6], which relies on ontologies for enabling mutual understanding among parties. In particular, the language uses ontologies in two ways: (a) to obtain domain and context information relevant for an access decision or credential release (e.g., the current location of the requester), by means of ontology atoms in the body of clauses; (b) to provide a semantics to the attributes certified by credentials, which enables the use of semantic alignment techniques to map attributes defined in different ontologies (i.e., to map an unknown attribute to a known one). Ontology atoms are resolved by requesting their evaluation to the *Knowledge Base* (KB) component, which consists of a set of ontologies defining the concepts and relationships employed in the party's policies and all the domain and context information. Attribute mapping requests are evaluated by the *Semantic Alignment Evaluator*, which implements the ontology alignment technique in [7].

2.3 Prototype Implementation

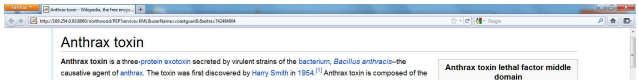
We have deployed a prototype implementation of POLIPO into an SoS in the MSS domain that has been developed within the POSEIDON project. The SoS consists of three main systems: a patrol vessel of the Italian navy (IT-1), a frigate of the Danish navy (DK-1), and an Operation Control Center (OCC), which collaborate in the context of EU NAVFOR, an anti-piracy operation taking place off the coast of Somalia. Each of these systems employs sensors to gather information from its surroundings. Sensors data are then integrated with further information from the Internet and intelligence gathered by the parties in the SoS to obtain more comprehensive information and derive new knowledge about the current situation. These information is then presented to the vessels' operators, which monitor the maritime traffic to accomplish their task in the mission.

In this demo we show how the attributes of a requester and the current context influence access decisions. In particular, we present a scenario divided into two parts. In the first part, an operator of IT-1, which is patrolling an area south-east of the Horn of Africa, observes on his display that two ships are suspiciously approaching each other at a nearby location (Figure 2(a)). The operator requests to DK-1 (which is in command of operations in that area) whether



(a) Visualization for the Operator of IT-1

(b) Extra Information Returned the Operator of IT-1



(c) Extra Information Returned the Operator of CG-1

Figure 2: Information Displayed to the Operators of the Italian navy and of the Dutch coastguard

more information about those two ships is available. One of the two ships (called Blue Star) is already under investigation by the Danish navy and police because it is heading to Copenhagen and is suspected of being involved in terrorist activities. Even though IT-1 is part of the EU NAVFOR, DK-1 does not provide to the Italian operator the extra information gathered about Blue Star (Figure 2(b)), because IT-1 is not assigned to the prevention of terrorist activities.

In the proximity of the Dutch coast, Blue Star gets into troubles due to a storm and starts drifting. A vessel of the Dutch coastguard (CG-1) is nearby and prepares to intervene to give assistance to Blue Star's crew. In order to prepare the intervention, CG-1 needs to have information about the cargo transported by Blue Star. Since Blue Star has transited off the Somali coast, CG-1 sends a request for extra information about the ship also to the OCC of the EU NAVFOR. Due to the emergency situation, and since CG-1 is a vessel certified for SAR operations by the Dutch navy, CG-1 becomes temporarily part of the SoS and the OCC provides extra information about Blue Star's cargo to CG-1. Through this information CG-1's operators find out that Blue Star's cargo may contain Anthrax that is meant to be distributed to terroristic cells in Europe (Figure 2(c)).

Every request to access the local resources of each party in the SoS is intercepted by its instance of the POLIPO framework, which checks whether the requester possesses the required credentials (possibly initiating a credential discovery process), and returns a response based on the local security policy. Notice that the evaluation of a policy might require the alignment of the vocabulary of the local party with that of the other coalition members.

In the POSEIDON SoS, communication among parties is via HTTP. Accordingly, we developed the PEP of the security framework as a web proxy that intercepts all the HTTP requests and returns an HTTP response in the expected format. This allowed us to deploy POLIPO without modifying the other components of the POSEIDON SoS.

3. CONCLUSIONS

We have presented POLIPO, a security framework that guarantees protection of information, autonomy and interoperability among the parties in an SoS by combining context-aware access control with TM and ontology-based services. The framework components have been implemented following the service-oriented paradigm; this facilitates the deployment of the framewoan SoSo existing SoS, and allows for an easy integration of additional components to support the evaluation of policies and provide additional functionalities. Besides the MSS domain, we have also deployed the framework in an SoS in the employability domain [1].

4. ACKNOWLEDGEMENTS

This work has been carried out as part of the POSEIDON project under the responsibility of the Embedded Systems Institute (ESI). This project is partially supported by the Dutch Ministry of Economic Affairs under the BSIK03021 program.

5. REFERENCES

[1] K. Böhm, S. Etalle, J. den Hartog, C. Hütter, S. Trabelsi, D. Trivellato, and N. Zannone. Flexible Architecture for Privacy-Aware Trust Management. *JTAER*, 5(2):77–96, 2010.

[2] L. Kagal, M. Paolucci, N. Srinivasan, G. Denker, T. Finin, and K. Sycara. Authorization and Privacy for Semantic Web Services. *IEEE Intelligent Systems*, 19(4):50–56, 2004.

[3] A. J. Lee, M. Winslett, and K. J. Perano. TrustBuilder2: A Reconfigurable Framework for Trust Negotiation. In *Proc. of IFIPTM'09*. Springer, 2009.

[4] N. Li, J. C. Mitchell, and W. H. Winsborough. Design of a Role-Based Trust-Management Framework. In *Proc. of S&P'02*, pages 114–130. IEEE Computer Society, 2002.

[5] W. Nejdl, D. Olmedilla, and M. Winslett. PeerTrust: Automated Trust Negotiation for Peers on the Semantic Web. In *Proc. of SDM'04*, LNCS 3178, pages 118–132. Springer, 2004.

[6] D. Trivellato, F. Spiessens, N. Zannone, and S. Etalle. POLIPO: Policies & OntoLogies for Interoperability, Portability, and autOnomy. In *Proc. of POLICY'09*, pages 110–113. IEEE Computer Society, 2009.

[7] D. Trivellato, F. Spiessens, N. Zannone, and S. Etalle. Reputation-Based Ontology Alignment for Autonomy and Interoperability in Distributed Access Control. In *Proc. of CSE '09*, vol. 3, pages 252–258. IEEE, 2009.

[8] D. Trivellato, N. Zannone, and S. Etalle. GEM: a Distributed Goal Evaluation Algorithm for Trust Management. Technical Report CS 10-15, Eindhoven University of Technology, 2010.

[9] A. Uszok, J. M. Bradshaw, M. Johnson, R. Jeffers, A. Tate, J. Dalton, and S. Aitken. KAoS Policy Management for Semantic Web Services. *IEEE Intelligent Systems*, 19(4):32–41, 2004.