A security framework for systems of systems

Trivellato, D.; Zannone, N.; Etalle, S.

Published in:
Proceedings 12th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2011, Pisa, Italy, June 6-8, 2011)

DOI:
10.1109/POLICY.2011.16

Published: 01/01/2011

Document Version
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:
• A submitted manuscript is the author’s version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher’s website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 29. Nov. 2018
A Security Framework for Systems of Systems

Daniel Trivellato, Nicola Zannone
Eindhoven University Of Technology
Email: {d.trivellato, n.zannone}@tue.nl

Sandro Etalle
Eindhoven University Of Technology
University of Twente
Email: s.etalle@tue.nl

II. SECURITY FRAMEWORK ARCHITECTURE

This section presents the security framework that is employed by each party in the SoS to protect the local resources. An overview of the security framework’s architecture 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 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 credentials, 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, they are asserted together with the authorization clauses into the authorization engine to determine 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 our framework we employ GEM [3], 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 POLIPO [1], a logic-based policy language that relies on ontologies for enabling mutual understanding among parties. In particular, POLIPO uses ontologies in two ways: (a) to obtain domain and context information relevant for an access decision or credential release 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. Ontology atoms are resolved by requesting their evaluation to the Knowledge Base (KB) component, which consists of a set of ontologies defining the concepts employed in policies as well as domain and context information. Attribute mapping requests are evaluated by the Semantic Alignment Evaluator, which implements the ontology alignment technique in [2].

### III. PROTOTYPE IMPLEMENTATION

We have deployed a prototype implementation of the security framework into an SoS in the Maritime Safety and Security (MSS) domain that has been developed within the POSEIDON project. The POSEIDON SoS consists of five types of systems: coastal AIS receivers, sea-based AIS receivers, the Internet, a Maritime Security Center (MSC), and patrol vessels. The AIS receivers capture AIS messages broadcasted by the ships transiting in their coverage area and send those messages to the MSC for further processing. The MSC collects data from the various receivers, analyzes them (e.g., for detecting anomalous behavior of ships), and integrates them with further information from the Internet; the resulting information forms the KB of the MSC. The information in the KB is used by the operators of both the MSC and patrol vessels to analyze the maritime traffic.

In this demo we show an application of the security framework to a coast surveillance scenario, where the MSC and a patrol vessel of the coast guard collaborate to prevent illicit activities off the Dutch coast. Every request to access the MSC’s KB, coming either from within the MSC or from the patrol vessel, passes through the MSC’s security framework, which checks whether the requester possesses the required credentials (possibly initiating a credential discovery process), and filters the response based on the security policy of the MSC. 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 appropriate format; this allowed us to deploy the framework without modifying the rest of the POSEIDON SoS.

We use Google Earth as visualization software; the view is updated every 30 seconds to display the new data collected by the AIS receivers. Fig. 2(a) and 2(b) show the output of the visualization for an operator of the MSC and an operator of the patrol vessel respectively. In the visualization, icons represent the current position of ships, and the color of a ship’s trajectory reflects the anomaly factor associated to that ship. In our scenario, MSC’s operators (Fig. 2(a)) are authorized to see all the maritime traffic off the Dutch coast, while patrol vessel’s operators (Fig. 2(b)) are allowed to see only ships with a high anomaly factor.

### IV. CONCLUSIONS

We have presented a security framework that provides confidentiality of information, autonomy and interoperability of parties in dynamic coalitions of heterogeneous systems. The framework consists of a set of components implemented following the service-oriented paradigm. This facilitates the deployment of the framework into existing SoS, and allows for an easy integration of additional components to support the evaluation of policies and provide additional functionalities.

**Acknowledgments.** 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.

**REFERENCES**

