Multiagent Security Evaluation Framework for Service Oriented Architecture Systems*

Grzegorz Kołaczek

Institute of Informatics
Wroclaw University of Technology, Wroclaw, Poland
Grzegorz.Kolaczek@pwr.wroc.pl

Abstract. As more and more organizations use the Service Oriented Architecture (SOA) to design and implement their information systems also the systems' architects need the more intelligent and reliable tools. The complexity, modularity and heterogeneity of the information systems make the security evaluation process difficult. The proposed method uses multiagent approach as the most promising direction of the research. As the security evaluation requires the precise definition of the set of evaluation criteria the basic criteria for each functional layer of SOA have been presented. Also, the paper presents two algorithms where the first can be used separately for each of the particular layer of SOA and the second serves for the calculation of the generalized SOA system security level.

1 Introduction

Most organizations deliver their business processes using information technology (IT) applications. Many different software tools are used to capture, transform or report business data. Their role may be for example to structure, define and transform data or to enable or simplify communication. Each such interaction with an IT asset can be defined a service. The set of delivered from the business processes services provide the incremental building blocks around which business flexibility revolves. In this context, Service Oriented Architecture (SOA) is the application framework that enables organizations to build, deploy and integrate these services independent of the technology systems on which they run.[8] In SOA, applications and infrastructure can be managed as a set of reusable assets and services. The main idea about this architecture was that businesses that use SOA can respond faster to market opportunities and get more value from their existing technology assets.[9]

The final success of the SOA concept can be obtained if many groups, both internal and external to the organization, contribute to the execution of a business process. Because in most cases the most valuable and also sensible part of each organization is information, a business partner is much more willing to share information and data assets, if it knows that these assets will be protected and their integrity maintained. Business partners will also be more likely to use a service or process from another group if it has assurance of that asset's integrity and security, as well as reliability and

* The research presented in this paper has been partially supported by the European Union within the European Regional Development Fund program no. POIG.01.03.01-00-008/08.

J.D. Velásquez et al. (Eds.): KES 2009, Part I, LNAI 5711, pp. 30–37, 2009.

performance. Therefore ensuring security is a one of the most crucial elements while putting SOA approach into practice.

The paper is structured as follows. The second section presents the general motivation and related work to the problems of security level evaluation and service oriented architecture. Next section describes a few basic notions in a security governance and after that the some examples of basic requirements for security evaluation in SOA. The forth section brings the main contribution – the description of multiagent framework for security evaluation in SOA systems. The last section consists of the conclusion and the direction of future research.

2 Motivation and Related Work

A mobile agent is a composition of computer software and data which is able to move from one host to another autonomously and continue its execution on the destination host. Mobile agent technology can reduce the bandwidth requirement and tolerate the network faults - able to operate without an active connection between clients and server. As the security evaluation process must be accurate and efficient, these basic features relevant to agent and multiagent systems are the main motivation for many researchers to apply multiagent approach to the tasks related to system security. The second premise in this case is the correspondence of the multiagent environment to SOA systems. Multiagent systems are composed from the number of autonomous and mobile entities that are able to act both cooperatively and separately. The fundamental concept for SOA system is service – entity that could be evoked individually as well as in cooperation with other services. And at last, both multiagent and SOA systems tend to act in heterogenic and highly distributed environment.

As the number of SOA implementation grows the concerns about SOA systems security also increases. The literature related to the security of SOA focuses on problems with threat assessment, techniques and functions for authentication, encryption, or verification of services.[1],[2],[6] Some other works focus on high level modeling processes for engineering secure SOA [4],[9] with trust modeling [7], identity management and access control [12][10]. Many studies focus on secure software design practices for SOA, with special interest in architectural or engineering methodologies as the means to create secure services. [3],[5]

To the author best knowledge, the proposed in this paper framework is the first that introduces the multiagent approach to the SOA security level evaluation. The other important and novel issues addressed in this work are the personalization of the security level evaluation process, multilevel security evaluation, support for continuous and automate security evaluation.

3 SOA Security Governance

There are several standards and mechanisms that have been elaborated to provide and to maintain the high security level of SOA systems. The basic solutions address the problems of confidentiality and integrity of data processed by SOA system. Because of the network context of SOA and the multilevel security risk related to the layers of

ISO/OSI network model, there are several solutions that offer data protection mechanisms at the corresponding level to each network layer.

The most commonly used and described are standards and protocols from the application layer that are maintained by OASIS consortium. These solutions have been worked out to support the development of web services and so also SOA systems. The other type of the protection methods, mechanisms and protocols like for example IPv6 are common for all network applications and can be used in SOA systems as well in any other type of software.

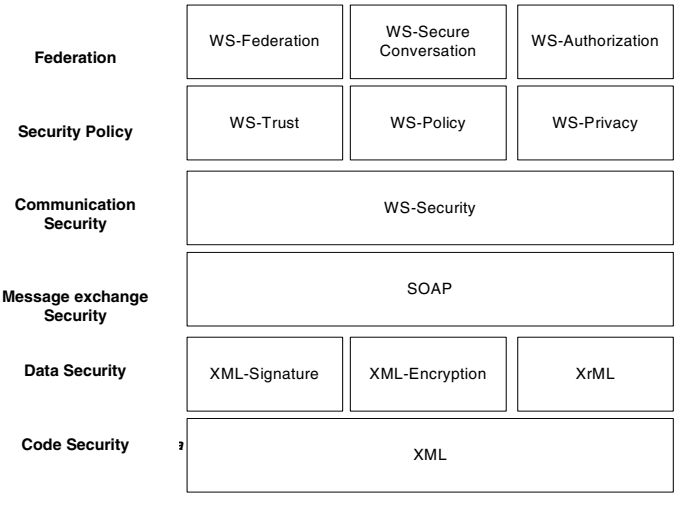

Fig. 1. SOA application layer related security protocols

3.1 Evaluation of SOA Security

The security evaluation process should be based on some formal prerequisites. This means that the security evaluation must be objective to guarantee the repeatability and universality of the evaluation results. So, there must be defined notion of the security

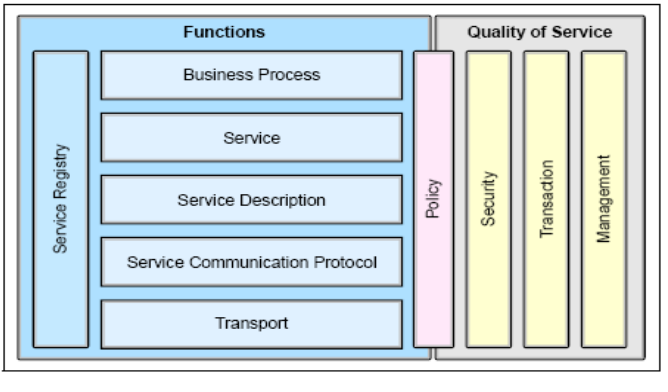

Fig. 2. The layered model of Service Oriented Architecture

measure. There are some confusion about this notion. The first problem is that the security measure does not have any specific unit. The other difficulties are: security level has no objective grounding but it only in some way reflects the degree in which our expectation about security agree with reality, security level evaluation is not fully empirical process, etc.

As the SOA system can be defied by its five functional layers (fig.2.) the correspondent definition of SOA security requirements for security evaluation process should address the specific security problems within each layer. Some elements from a set defining security requirements for the SOA layers has been presented in Table 1.The complete list can be found in [5].

Table 1. The functional and non-functional security evaluation requirements for each of the SOA functional layers (selection)

SOA Layer	Evaluate/verify/test
Policy and Business Processes	– Policy consistency – Policy completeness – Trust management – Identity management
Service	– Identification of the services – Authentication of the services – Management of security of the complex services
Service Description	– Description completeness – Availability – Protection from attacks
Service Communication Protocol	– Confidentiality – Authentication – Norms compliance
Transport	– Availability – Protection from attacks – Integrity

4 Multiagent Framework for SOA Security Evaluation

There are several different problems considering the SOA security level evaluation process. The most crucial, as it has been stated in the earlier sections are: the complexity of the architecture, multilevel relationships between the system components and heterogenic environment. Each security level evaluation method and tool must take into account all these factors and apply appropriate solutions for them to provide the accurate final results of the security evaluation process.

4.1 The Architecture of Multiagent System for SOA Security Level Evaluation

This section presents the main assumptions about SOA systems security evaluation framework. The main idea about this framework is the application of multiagent architecture. As systems implementing Service Oriented Architecture are often geographically

and logically dispersed the appropriate tool for monitoring and controlling all components is necessary. The multiagent approach offer all relevant mechanisms and concepts so it seams to be the best solution in the described situation.

The main element of the multiagent system architecture for SOA security evaluation is definition of the agents classes. The following agents classes have been considered:

1. AMOL – SOA functional layer monitoring agents
2. ASL – SOA functional layer superior agents
3. AM – SOA managing agents
4. AC – the agents of consumers of SOA system services

Table 2. The characteristic of the agent classes

AMOL_1= $\{amol1_1, amol1_1,\ldots, amol1_n\}$	- set of autonomous agents which perform the security level evaluation related tasks defined in Table 1. For the first functional layer of SOA – transport; - for example $amol1_1$ may be an agent that evaluates the confidentiality of the transport layer, $amol1_2$ may be an agent that evaluates data integrity at the transport layer level, etc.
AMOL_2= $\{amol2_1, \ldots, amol2_m\}$ AMOL_3= $\{amol3_1, \ldots, amol3_l\}$ AMOL_4= $\{amol4_1, \ldots, amol4_o\}$ AMOL_5= $\{amol5_1, \ldots, amol5_p\}$	- sets of autonomous agents for corresponding four SOA layers (communication protocols, …, business processes) that perform specific security evaluation tasks related to the particular layer as described in Table 1.
ASL={*asl1, asl2, …, asl5*}	- for each SOA functional layer there is defined one *superior agent*; - the *superior agents* range of responsibility is to coordinate all the tasks related to the security evaluation process for the particular SOA functional level, to collect the results provided by *amol* agents, to interpret the results provided by *amol* agents and finally to present the results of the security level to *managing* agent and to *client* agents
AM={*am*}	- the *managing agent* is responsible for the most top-level security evaluation; it coordinate the activity of *asl* agents, collect the results of the SOA layer evaluation, combine all security level related information and produce the general SOA security level value, serves the *consumer* agents requests
AC={ac_1, ac_2,…, ac_q}	- SOA *services consumers* agents collect the information about security level of provided by SOA systems services and evaluates the security level of composite services

The fundamental relations among agents, agent classes and SOA architecture are presented in fig. 3.

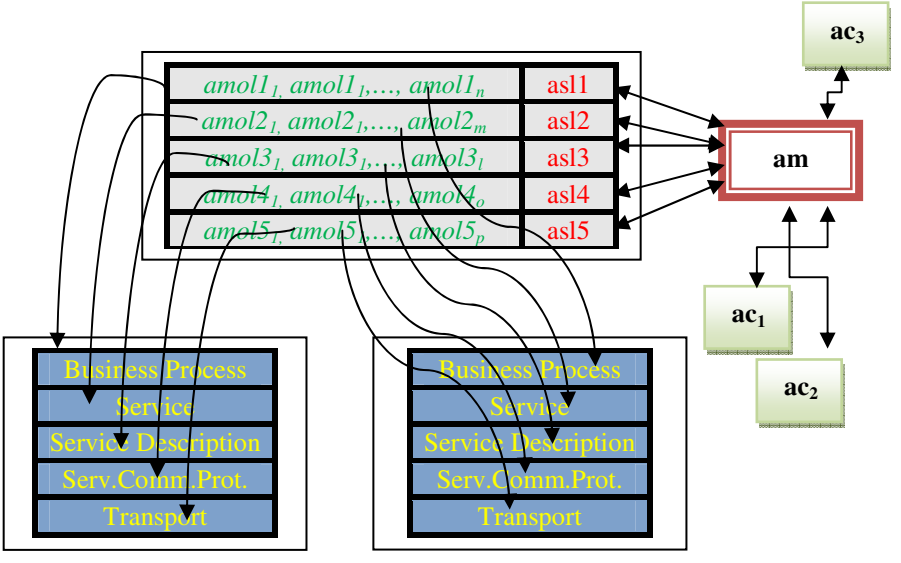

Fig. 3. The architecture of the multiagent system for SOA security level evaluation

4.2 A General Idea about SOA Security Level Evaluation

The most important functionality related to the SOA security level evaluation architecture is description of the all components, mechanisms and relations that are necessary to precisely evaluate the security level of the particular SOA system. As it was described in section 3 the problem of security evaluation is very complex and there exist more than one solution that could be acceptable within a context of a particular system and its environment. This part of the paper describes some general ideas about SOA security level evaluation in a relation to requirements listed in the table 1 and multiagent architecture presented in the fig. 3

Algorithm 1. Security level evaluation for a separate SOA functional layer.

Given:
- N – number of SOA layer
- ac_k – consumer of the service
- $p_1, p_2,..., p_l$ – details or preferences related to ac_k request
- am – managing agent
- $amolN_1, ..., amolN_m$ – set of specialized agents that perform security evaluation using appropriate tests, mechanisms, etc. related to the N-th SOA layer

Result:
- L_n – security level value for N-th layer

BEGIN
1. ac_k prepare and send to *am* a request concerning the security level of the *N-th* layer of the SOA system
2. *am* find all the monitoring agents related to *N-th* layer ($amolN_1$, ..., $amolN_m$), prepare and send the appropriate requests to them
3. Monitoring agents ($amolN_1$, ..., $amolN_m$) perform the security evaluation tasks using all tools, methods, algorithms, etc. available to them
4. *am* collects the results obtained by all monitoring agents and using the specific algorithm (data fusion, consensus operator, etc.) and taking into account the list p_1, p_2,..., p_l of ac_k preferences evaluates the final security level value of the *N-th* layer of this SOA system
5. *am* returns L_n to the ac_k

END

Algorithm 2. SOA security level evaluation.

Given:
- ac_k – consumer of the service
- *am* – managing agent
- p_1, p_2,..., p_l – details or preferences related to ac_k request

Result:
- L_{soa} – SOA system security level

BEGIN
1. ac_k prepare and send to *am* a request concerning the security level of the SOA system
2. Using *algorithm 1* managing agent *am* evaluate L_1,..., L_n – security levels for all SOA system's layers
3. Managing agent *am* evaluate L_{soa} the final security level value of the SOA system using selected data fusion methods and taking into account the list p_1, p_2,..., p_l of ac_k preferences
4. *am* returns L_{soa} to the ac_k

END

Discussion. In both algorithms there is no explicit definition of the method used for evaluation of the security level for a separate SOA layer and for the whole SOA system. The definition and the validation of the methods, algorithms used in these steps is one of the most challenging task of the security evaluation process. But as it was stated before, there is more than one acceptable approaches. The final decision concerning selection of the method used to combine the data provided by monitoring agents may depend on the context of the SOA system or/and the context of the consumer request.

5 Conclusion

The paper presents a novel framework of multiagent system for SOA security level evaluation. Also some general discussion about security level evaluation and Service Oriented Architecture have been presented. The multiagent architecture is composed of three types of agents: monitoring agents that tests the various security parameters

related to particular SOA layer, superior agents that manage the activity of monitoring agents, manging agents that are responsible for all superior agents and for communication with service consumer agents. Two algorithms used by monitoring agents and managing agents have been discussed.

The most important future work related to the problems described in the paper is proposition of the exact calculation method for assessment of the corresponding security level. After that, the selected method should be validated in the environment of the production SOA systems.

References

[1] CERT (2009), http://www.cert.org (retrieved March 20, 2009)
[2] Department of Homeland Security. National Vulnerability Database of the National Cybersecurity Division (2009), http://nvd.nist.gov (retrieved March 20, 2009)
[3] Epstein, J., Matsumoto, S., McGraw, G.: Software security and SOA. IEEE Security and Privacy 4(1), 80–83 (2006)
[4] Fernandez, E.B., Delessy, N.: Using patterns to understand and compare web services security products and standards (2006)
[5] Kolaczek, G.: Opracowanie koncepcji specyfikacji metod i modeli szacowania poziomu bezpieczeństwa systemów SOA i SOKU, WUT (2009) (in polish)
[6] Nakamura, Y., Tatsubori, M., Imamura, T., Ono, K.: Model-driven security based on web services security architecture. In: IEEE International Conference on Services Computing, vol. 1, pp. 7–15 (2005)
[7] SANS Institute (2006), http://www.sans.org (retrieved March 20, 2009)
[8] Skalka, C., Wang, X.: Trust by verify: Authorization for web services. Paper presented in ACM Workshop on Secure Web Services, pp. 47–55 (2004)
[9] SOA Reference Model Technical Committee. A Reference Model for Service Oriented Architecture, OASIS (2006)
[10] Steel, C., Nagappan, R., Lai, R.: Core security patterns: Best practices and strategies for J2EE, web services, and identity management. Pearson, Upper Saddle River (2006)
[11] Tari, Z., Bertok, P., Simic, D.: A dynamic label checking approach for information flow control in web services. International Journal of Web Services Research 3(1), 1–28 (2006)
[12] WS-security policy 1.2, OASIS (2009)
[13] Yuan, E., Tong, J.: Attributed based access control (ABAC) for web services. In: IEEE International Conference on Web Services, pp. 561–569 (2005)