André Miede:
Cross-organizational Service Security -- Solutions for Attack Modeling and Defense. In: Proceedings of the PhD Symposium of the 7th International Joint Conference on Service Oriented Computing (ICSOC/ServiceWave 2009), p. 9--12, November 2009. ISBN ISSN 1613-0073.
CEUR-WS.org/Vol-548/

Cross-organizational Service Security – Solutions for Attack Modeling and Defense

André Miede
Supervised by Ralf Steinmetz

Multimedia Communications Lab (KOM) – Technische Universität Darmstadt
Department of Electrical Engineering & Information Technology
Merckstraße 25, D-64283 Darmstadt, Germany
Andre.Miede@KOM.tu-darmstadt.de

Abstract Security is an important aspect of Service-oriented Architectures (SOAs), enabling the service-based integration of partner IT systems across organizational boundaries, i. e., in the Internet of Services. Current trends in SOA security, e. g., reducing it to Web service security, do not take into account SOA-specific threats, vulnerabilities, and attacks. In this paper, measures to support the modeling of attacks in general and in order to show the service-oriented difference regarding security are introduced. Based on this understanding, mechanisms to defend against SOA-specific attacks will be designed and evaluated.

1 Introduction

Challenging market dynamics and the rise of complex value networks require organizations to adjust their business processes rapidly in order to stay competitive. As many organizational processes are supported or even enabled by information technology (IT), a process is only as flexible as its underlying technological representation. A special integration challenge in this context are processes which span across organizational boundaries, e. g., customer creation processes, where data has to be checked against external watch lists in order to fight organized crime. Another example are trading processes in investment banking, where market data or credit ratings are bought from external providers.

The *Service-oriented Architecture* paradigm (SOA) [1] offers possibilities on both a technological and organizational level to integrate company-wide and inter-company IT systems. SOAs are based on the "service" concept, where services can be seen as black boxes representing business functionalities. These services are used to assemble business processes as service compositions and may even cross enterprise boundaries, thus, being *cross-organizational service-based workflows* [2, 3], e. g., in the *Internet of Services* scenario [4].

The rest of the paper is structured as follows: Section 2 presents the problem statement and the research questions which are at the foundation of my thesis. Section 3 structures both preliminary results and open challenges for the proposed questions. Section 4 concludes the paper and gives an outlook on next steps.

2 Problem Statement and Research Objectives

Just as any economic system requires security in order to work and to be accepted by its participants, the security of the involved systems, exchanged messages, and used communication channels has to be ensured for cross-organizational service-based collaboration. Achieving and guaranteeing basic IT security goals such as confidentiality, authentication, authorization, non-repudiation, integrity, and availability [5–7] is an absolute must in this context and still an active topic, both in research and industry. Thus, the differences SOA introduces into the field of IT security have to be analyzed and addressed.

The main tenor of current SOA security research is that conventional security measures are not sufficient in the SOA context [2, 8–10]. For example, a major argument in this context is the necessity to switch from point-to-point-security to end-to-end-security, because any used service can call an arbitrary number of different services on its own. Another argument is the need for decoupled security decision points, in SOA usually called security-as-a-service. Yet another trend is to equalize SOA security with Web service security, reducing SOA security requirements to Web service security standards and their configuration.

While these approaches are important building blocks for SOA security, they are not sufficient as they do not take into account *SOA-specific* threats, vulnerabilities, and the corresponding attacks. In order to close this gap, the following research challenges and objectives were identified:

1. Analyze SOAs regarding security challenges and specific attack scenarios, e. g., for the Internet of Services. The analysis must not be limited to particular SOA implementations, i. e., Web services, but focuses on SOA characteristics such as loose coupling, composability, etc. Based on the analysis of these security impacts, SOA-specific attacks have to be identified and modeled.
2. Develop means to understand and model attacks in general, i. e., analyze and define the elements they consist of. This objective is not service-specific, but a general IT security challenge. The results of this objective are used to model the SOA-specific attacks identified in the first objective.
3. Provide technology-independent solutions to defend against SOA-specific attacks. Based on the modeled attack scenarios, selected countermeasures have to be developed or adapted from other areas of research in order to make cross-organizational SOA scenarios safer.

The next section discusses my proposed solutions and their expected outcomes for theses challenges.

3 Proposed Solutions and Expected Outcomes

Addressing the research challenges and objectives outlined in Section 2, my research focuses on the following solution building blocks as depicted in Figure 1. In the following, for each of these solution building blocks, first results, their impact, and the progress beyond the state of the art is briefly discussed.

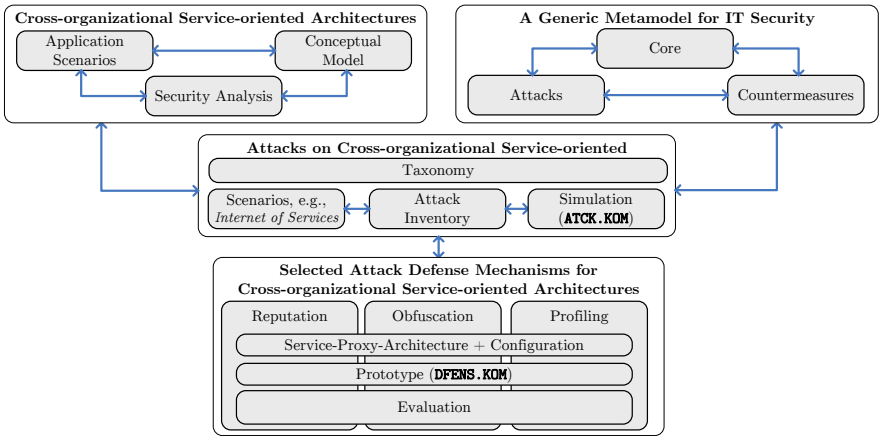

Figure 1. Research structure and approach

3.1 Cross-organizational Security – The Service-oriented Difference

Cross-organizational SOA security deals with the application of core IT security concepts such as threats, vulnerabilities etc. on the elements of cross-organizational SOA such as loose coupling, composability, etc. These elements are assembled in the form of a conceptual model which is based on SOA definitions and descriptions found in standard literature on SOA [2, 3, 11–13] (cf. Figure 2). The goal is to evaluate the security impact of single SOA elements and their relationships. While single security aspects of these elements are already well-known, i. e., for distributed systems characteristics, the combination of and relationships between the SOA elements as well as their impact makes cross-organizational SOA a special security challenge [14]. An example for such an impact is compromising an organization's legal or regulatory *compliance*, which can result in fines, the revocation of licenses, or loss of customer trust. *Composability* has also a high security impact, creating seams for exploitation, e. g., caused by the incomplete integration of different security technology, or by the possibility to introduce malicious services into the composition.

Compared to standard literature on SOA [2, 3, 11–13], which differ in their definitions, presentation, and coverage of SOA core elements, this approach offers a compact and visual inventory as a basis for communication and analysis, i. e., a dedicated SOA security analysis.

3.2 A Generic Metamodel for IT Security

The proposed generic metamodel for IT security [14] brings together the most important ideas of IT security (including their relationships) and consists of three main parts: a *Core* of basic IT security concepts, *Attacks*, and *Countermeasures*.[1] It lays the foundation for describing and understanding the different elements of attacks and countermeasures in an IT security context.

[1] `http://www.kom.tu-darmstadt.de/~miede/soasecurity/secmetamodel.pdf`

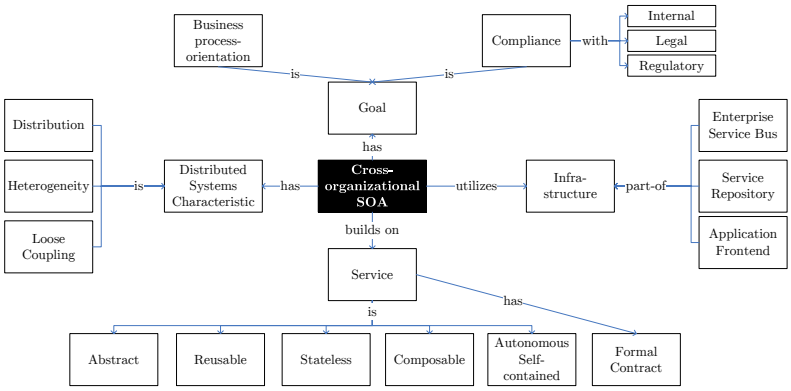

Figure 2. Conceptual model of cross-organizational SOA [14]

In order to show the applicability of the metamodel to real-life scenarios, attacks on different distributed systems were modeled, i. e., on Peer-to-Peer systems, on Mobile ad hoc Networks, and in SOA contexts. Compared to similar concepts such as attack patterns [15,16] or security patterns [17], this metamodel offers building blocks which help with actually assembling such patterns, thus, improving the means to understand and model attack knowledge.

3.3 Attacks on Cross-organizational Service-oriented Architectures

Cross-organizational SOA-specific attacks target vulnerabilities of single SOA elements and combinations thereof (cf. Figure 2). All types of attacks which are already known from classic distributed systems or which focus on specific technologies, i. e., Web services, are not considered cross-organizational SOA-specific attacks. This is due to the fact that these attacks can also occur outside SOA contexts. Examples for such attacks are *XML injections* to manipulate the structure of messages or Denial of Service attacks via *oversized payload* using a very large message [18]. However, these attacks still pose a threat for cross-organizational SOA and have to be addressed by common countermeasures such as message validation and processing mechanisms [18]. This approach is depicted in Figure 3, using abstraction layers as an attack taxonomy for SOA.

Examples are service selection attacks, where differences in the security level a provider offers are exploited. The analysis of service consumer-provider-communication can also be an attack to gather information about the business (requests, used providers, time, frequency, etc.). Loosely coupled and malicious service compositions are a likely attack as well, if "good" services are encapsulated by "bad" ones in order to manipulate data or to gather information.

Compared to other work on SOA attacks [2,8,10,18] which have a strong focus on Web service technologies, this approach adds insights on attack scenarios which target specific SOA elements such as loose coupling and composability.

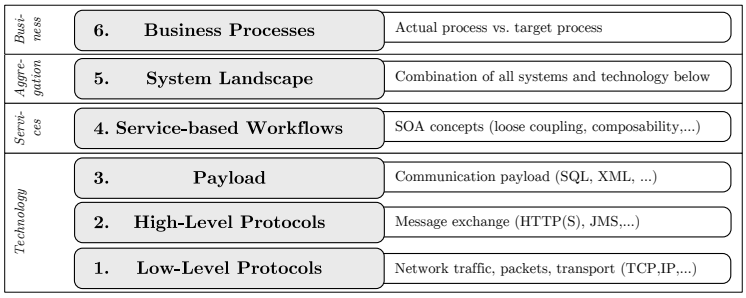

Figure 3. SOA security abstractions layers [14]

3.4 Selected Attack Defense Mechanisms

Based on the above results, several areas of interest for defense mechanisms were identified and now have to be evaluated regarding their potential for deeper research activities. These areas are the following:

1. decentralized service provider *reputation* for securing service compositions,
2. communication *obfuscation*, e. g., using Mixes [19], to avoid the exposure of information about business activities in the case of traffic analysis, and
3. service consumer *profiling* for detecting malicious service consumer behaviour.

It is planned not to pursue each of these areas in full depth, but to develop initial concepts in order to determine which area is the most fruitful for valuable contributions beyond existing approaches.

A prototype (`DFENS.KOM`) as basis for the above areas is already in development and it is based on an open-source SOA platform. There, service consumer and provider communication is relayed via a messaging system which was enhanced to forward messages to a proxy system. Via a configuration policy, this proxy is planned to trigger certain dedicated agents, e. g., for profiling consumer behaviour and checking against existing profiles, for obfuscating the communication to complicate traffic analysis, or for gathering reputation information about consumer and provider.

4 Conclusions and Future Work

As outlined above, the basic structure as well as the theoretical and conceptual foundation of the thesis is already in place (Sections 3.1–3.3) and will be further refined as follows:

- a critical revision of the conceptual SOA model elements regarding completeness, redundancies, and relationships,
- further extensions of the IT security metamodel regarding countermeasures and possibly adapting it to the Meta-Object Facility (MOF) standard,[2]
- identifying attack sub-steps from lower layers, the creation of a detailed attack model inventory, and implementing attack models for simulating attack behaviour in an Internet of Services scenario (`ATCK.KOM`).

[2] `http://www.omg.org/mof/`

However, the next major step will be to determine which of the above areas (reputation, obfuscation, profiling) to pursue further and in what direction. Basis for this will be an extensive review of related work, its applicability to the identified SOA-specific attack scenarios, and own initial solution concepts. Furthermore, appropriate evaluation techniques for such defense mechanisms have to be devised. This includes determining the evaluation basis, i. e., using a testbed based on our extensions of an open-source SOA platform or using simulation models for attacks and countermeasures in an Internet of Services scenario.

References

1. Papazoglou, M.P., Traverso, P., Dustdar, S., Leymann, F., Krämer, B.J.: Service-Oriented Computing Research Roadmap. In: Dagstuhl Seminar Proceedings on Service Oriented Computing (SOC). (2006)
2. Josuttis, N.M.: SOA in Practice: The Art of Distributed System Design (Theory in Practice). O'Reilly Media, Inc. (8 2007)
3. Newcomer, E., Lomow, G.: Understanding SOA with Web Services (Independent Technology Guides). Addison-Wesley Professional (12 2004)
4. Schroth, C.: The Internet of Services: Global Industrialization of Information Intensive Services. In: Proceeding of IEEE ICDIM 2007. (2007) 635–642
5. Eckert, C.: IT-Sicherheit: Konzepte – Verfahren – Protokolle. 5th edn. Oldenbourg (11 2007) (in German).
6. Schneier, B.: Secrets and Lies: Digital Security in a Networked World. Wiley (2004)
7. Bishop, M.: Computer Security: Art and Science. Addison-Wesley (12 2002)
8. Kanneganti, R., Chodavarapu, P.: SOA Security. Manning Publications (1 2008)
9. Hafner, M., Breu, R.: Security Engineering for Service-Oriented Architectures. Springer, Berlin (2008)
10. Bundesamt für Sicherheit in der Informationstechnik: SOA-Security-Kompendium: Sicherheit in Service-orientierten Architekturen (2008) (in German).
11. Krafzig, D., Banke, K., Slama, D.: Enterprise SOA: Service-Oriented Architecture Best Practices. Prentice Hall PTR (11 2004)
12. Melzer, I., et al.: Service-orientierte Architekturen mit Web Services. Konzepte – Standards – Praxis. 2nd edn. Spektrum Akademischer Verlag (2007) (in German).
13. Erl, T.: Service-Oriented Architecture (SOA): Concepts, Technology, and Design. Prentice Hall PTR (8 2005)
14. Miede, A., Gottron, C., König, A., Nedyalkov, N., Repp, N., Steinmetz, R.: Cross-organizational Security in Distributed Systems. Technical Report KOM-TR-2009-01, Technische Universität Darmstadt (2009)
15. Hoglund, G., McGraw, G.: Exploiting Software: How to Break Code. Addison-Wesley (2 2004)
16. Barnum, S., Sethi, A.: Attack Patterns. "Build Security In" Initiative, National Cyber Security Division of the U.S. Department of Homeland Security (2006)
17. Schumacher, M.: Security Engineering with Patterns: Origins, Theoretical Models, and New Applications. 1 edn. Springer (9 2003)
18. Jensen, M., Gruschka, N., Herkenhoner, R., Luttenberger, N.: SOA and Web Services: New Technologies, New Standards – New Attacks. In: ECOWS '07: Proceedings of the Fifth European Conference on Web Services. (2007) 35–44
19. Raymond, J.F.: Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In: Designing Privacy-enhancing Technologies Workshop. (2001) 10–29