André Miede, Tobias Ackermann, Nicolas Repp, Daniel F. Abawi, Ralf Steinmetz, Peter Buxmann: *Attacks on the Internet of Services – The Security Impact of Cross-organizational Service-based Collaboration.* In: Matthias Schumann and Kolbe, Lutz M. and Breitner, Michael H. and Arne Frerichs: Tagungsband Multikonferenz Wirtschaftsinformatik (MKWI) 2010, p. 425--426 (short) and 2151--2162 (full), Universitätsverlag Göttingen, February 2010. ISBN 978-3-941875-31-9. http://webdoc.sub.gwdg.de/univerlag/2010/mkwi/.

Attacks on the Internet of Services

The Security Impact of Cross-organizational Service-based Collaboration

André Miede[1], Tobias Ackermann[2], Nicolas Repp[1], Daniel F. Abawi[3], Ralf Steinmetz[1], Peter Buxmann[2]

[1]Multimedia Communications Lab (KOM), Technische Universität Darmstadt
[2]Chair of Information Systems, Technische Universität Darmstadt
[3]Department of Industrial Engineering and Management, Hochschule für Technik und Wirtschaft des Saarlandes

1 Introduction and Scenario

Composite, digital business processes and the increasing application of *Service-oriented Architectures (SOA)* make it possible that parts of these business processes are outsourced to third party organizations, which can be distributed all over the world. Examples are trading processes in investment banking, where market data or credit ratings are bought from external providers, or customer creation processes where data has to be checked against external watch-lists or ratings. How such a process can be mapped, e.g., on both internal and external services is shown in Figure 1.

Business processes are technically represented by *workflows* (Leymann and Roller 2000, p. 7), which – following the SOA paradigm – can be composed of services. These services deliver a defined business functionality and are clearly capsulated and loosely coupled entities (Papazoglou and van den Heuvel 2007, p. 389).

The cross-organizational collaboration allows to increase quality or to perform the processes at lower costs. The integration of third party services into service-based software systems is a value potential because it supports the services' consumers to create new functionality. The SOA paradigm and the underlying technology ease the integration and make it cheaper. (Becker et al. 2009, pp. 623-624)

The *Internet of Services* (IoS) is a business model which uses the Internet as a medium for the retrieval, combination, and utilization of interoperable services (Cardoso et al. 2008, pp. 15-16; Schroth 2007, pp. 635-642). Multiple providers may offer and sell their services, thereby leading to market places where consumers

can find third party services. The IoS provides the base for complex business networks by supporting the composition and aggregation of existing services to value-added services. An important aspect of these market places for cross-organizational collaboration is that they support flexible and dynamic intermediation between service providers and consumers through agreements on non-functional requirements like cost criteria and Quality of Service (QoS) parameters, such as performance (Braun et al. 2008, p. 227).

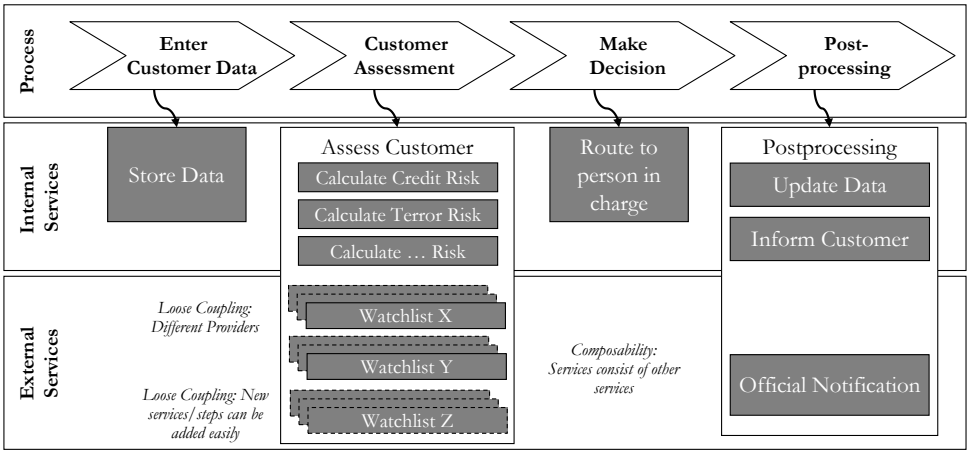

Figure 1: Example customer creation process and mapping on services

The concrete application scenario for our research is the domain of service-based collaboration between distributed service providers and consumers using market places as shown in Figure 2. In order to enable this kind of collaboration, the security of the participating systems, exchanged messages, and used communication channels has to be ensured. Achieving and guaranteeing basic IT security goals such as confidentiality, authentication, authorization, non-repudiation, integrity, and availability (Eckert 2007, pp. 6-13; Schneier 2004, pp. 59-81) is an absolute must in this context and still an active topic both in research and industry. Although security introduces additional costs and has an impact on the QoS, unsecured business transactions are not an option in most business scenarios. Existing research on outsourced services in the context of the IoS focuses on technical aspects like reference architectures and the dynamic service selection process based on QoS parameters. Security issues and attacks related to the IoS have not been researched so far. Regarding an effective risk management for the IoS, the assessment of threats and potential attacks is an important starting point for further steps such as quantifying and managing risks.

This paper focuses on attacks on cross-organizational SOAs in an Internet of Services scenario. In order to structure both technological and business-oriented attacks, an attack taxonomy is presented. The main contribution is the discussion

of IoS-specific attacks which complements the current Web service-centric view in this research area.

The remainder of this paper is structured as follows: Section 2 gives an overview of related work in the area of SOA attacks. Section 3 presents a taxonomy for attacks on the Internet of Services and discusses selected attack examples. Section 4 concludes the paper with a brief summary and an outlook on future work.

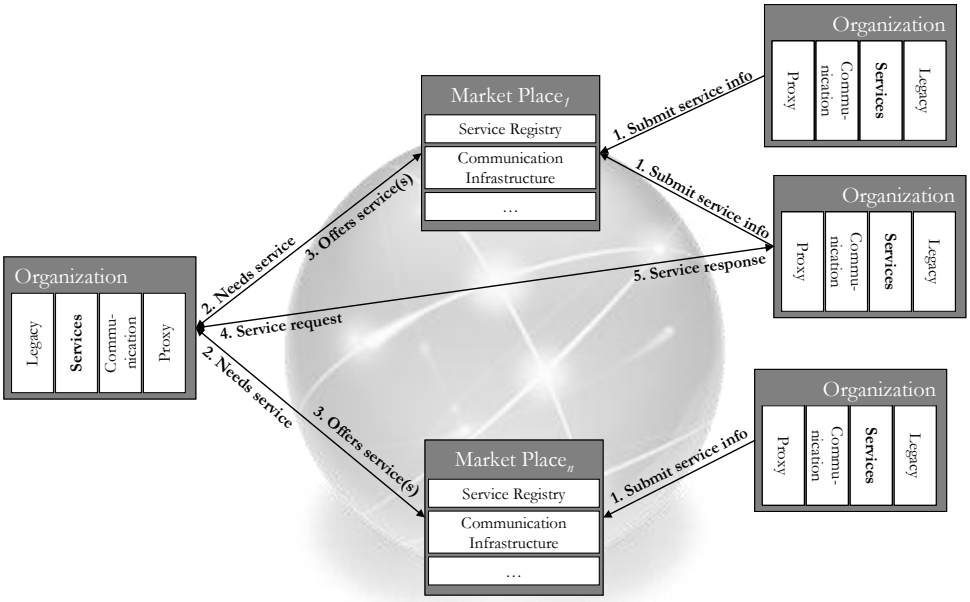

Figure 2: Generic setup for the Internet of Services

2 Related Work

Attacks on IoS scenarios have received no attention so far. However, as we consider the SOA paradigm to be an important requirement for cross-organizational collaboration in an IoS scenario, we now give a brief overview of key research dealing with attacks on SOAs.

Standard literature on SOA and SOA security such as Josuttis (2007, pp. 185-188), Bundesamt für Sicherheit in der Informationstechnik (2008, pp. 21-23), Hafner and Breu (2008, pp. 38-40), Jensen et al. (2007, pp. 35-44), Jensen and Schwenk (2009, pp. 1-10), and Kanneganti and Chodavarapu (2008, pp. 433-440), have a strong focus on Web services and related technology attacks. The most common SOA attacks discussed by the above researchers include the following:

- XML-specific attacks which are mainly targeting parser applications, i.e., XML bombs, X-Path injections, schema poisoning,

- WSDL-scanning in order to analyze services for vulnerabilities in methods and parameters,
- Message replay attacks (due to stateless Web services),
- SOAP attachments, e.g., files containing viruses.

Other technological attacks (but not as common as the above) are, for example, BPEL state deviations, workflow engine hijackings, provider instantiation floodings (directly or indirectly via intermediates), or oversized cryptography (aiming at the resources of cryptographic applications).

The Bundesamt für Sicherheit in der Informationstechnik (2008, pp. 21-23) and Hafner and Breu (2008, pp. 38-40) also give a brief outline of other, more SOA-specific attacks such as compromised services, unauthorized service usage, and the exploitation of organizational weaknesses. However, they lack more detailed discussions of related attack scenarios and their implications.

In addition to the technological focus, current discussions of SOA attacks offer little help for structuring attacks, thus, impeding the development and deployment of effective countermeasures covering as many attack scenarios as possible.

After this overview, the next section discusses means to classify attacks on SOAs and introduces new attack scenarios from a more business- and service-oriented point of view.

3 Attacks on the Internet of Services

As shown in the previous section, attacks on globally distributed value chains are at the moment mainly seen from a technical point of view, i.e., with a focus on Web services technology. Building on the attacks found in standard literature, our first step is to structure SOA attacks by providing a suitable taxonomy, which is able to capture already known attacks, the ones presented in this paper, and several additional ones not yet discovered or thought of.

Our proposed taxonomy which is based on the abstraction layers an attack targets is shown in Figure 3. The layers consist of the following (and must not be confused with the ISO/OSI model layers):

1. *Low-Level Protocols:* This layer comprises attacks on the network technology, e.g., on the Internet Protocol (IP) or the Transmission Control Protocol (TCP). Typical examples for this layer are scanning, sniffing, or spoofing.
2. *High-Level Protocols:* Here, protocols used for the message exchange in service-based scenarios are targeted, e.g., Java Message Service (JMS) or Hypertext Transfer Protocol (HTTP). The examples from the low-level protocols apply here as well.
3. *Payload:* The exchanged messages contain data which is processed by particular applications. In order to disturb these applications or to gain unauthorized access, malformed input data can be used. Examples are SQL injections executing malicious code via manipulated SQL statements or XML bombs crashing

parser applications by consisting of infinitely recursive structures. (A common technology such as SOAP is a special case, because it can be target of both protocol-specific and payload-specific attacks. SOAP uses XML for data representation and can use various protocols for the message transfer, e.g., JMS or HTTP/TCP.)

4. *Service-based Workflows:* This layer comprises attacks targeting characteristics of the SOA paradigm, e.g., loose coupling or composability. Such attacks can consist of different lower-level attack components. Examples for these attacks are given in the next sections.
5. *System Landscape:* Here, all the lower-level attacks are aggregated in order to identify attacks which occur distributed across the IT architecture of an enterprise. To achieve this, it is important to correlate different events on a large scale, to detect potential diversions, and even to anticipate certain attacks from the gathered information.
6. *Business Processes:* The top-most abstraction level deals with the business processes themselves, where an attacker's goal could be to trigger a deviation from the pre-defined target process. For example, social engineering techniques can be used in order to gain access to restricted areas or to bypass the four-eyes-principle. Other, additional layers above the process-level such as organizational structures are possible as well, but are omitted from our taxonomy for now.

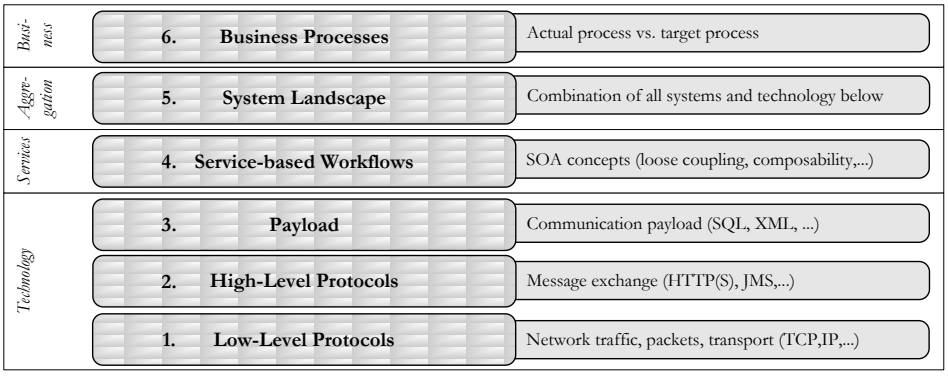

Figure 3: Attack abstraction layers and taxonomy

Layers 1-3 capture technological attacks which are executed via flaws and vulnerabilities in algorithms, protocols, or applications. Layers 5 and 6 capture the general business view and the threats it faces across the enterprise.

Layer 4, which is right between the technological and the business view, deals with attacks using the characteristics of the SOA paradigm and the IoS. So far, attacks on service-based workflows can be divided in three basic classes:

- *Service Selection Attacks* exploit characteristics of the loose coupling between a service consumer and its service providers, i.e., when an intermediary is used

to choose the best available service according to a QoS optimization model (cf. Section 3.1).

- *Consumer-Provider Communication Analysis* makes use of the general IoS scenario, where service consumers contact market places in order to get access to specific services which fulfil their business requirements. Even if detailed contents are unknown, these requests and the subsequent communication can be used by attackers to gather important information (cf. Section 3.2).
- *Loose and Malicious Compositions* focus on the aspect that workflows are composed from different loosely coupled services, which can be composed of other services themselves. Attackers can exploit this by submitting invalid service offerings or pointers to services which offer false functionality. Also either the registry or the messages themselves could be manipulated to re-route service communication to unauthorized third parties (cf. Section 3.3).

The next sections discuss selected examples for each of these classes.

3.1 Service Selection Attack: Quality of Protection Differences Exploit

One of the major advantages the SOA paradigm and the IoS offer is the flexibility to choose dynamically between different service providers, i.e., based on optimization models regarding QoS aspects and costs (Eckert et al. 2008, pp. 591-597). An attack scenario which targets the dynamic, loosely coupled service selection process is depicted in Figure 4.

Here, we assume an organization is already consuming a service from a provider who offers a high level of service protection ("1. Data exchange"). An attacker, who knows about this exchange, targets the current provider and other potential providers with similar security levels, i.e., via a Denial of Service attack ("2. Attacker disrupts service"). The service consumer's selection mechanism now detects the outage of the provider and contacts different market places in order to find a replacement for the disrupted service ("3. Find replacement"). As the attacker anticipated, one of the remaining services which is offering only low security is selected for further collaboration by the consumer ("4. Data exchange"). Exploiting this low or even non-existent security, the attacker starts the next step of the attack, e.g., targeting the badly protected communication between consumer and provider ("5. Attacker targets communication").

While in this scenario the different levels of service protection – also called "Quality of Protection" (Gollmann et al. 2006, p. vii) – were exploited, i.e., in order to eventually target the communication between consumer and provider, several variations of the attack are possible as well. For example, a service provider with bad QoS metrics could launch attacks against competitors in order to degrade their metrics and to improve his own ranking (as seen by the service selection tools).

An important implication of this attack scenario is to include the Quality of Protection as an important factor in service selection models and not only focus on classic metrics such as response time and costs. However, this requires quanti-

fying service security, i.e., finding suitable and meaningful protection metrics and defining standards for their representation.

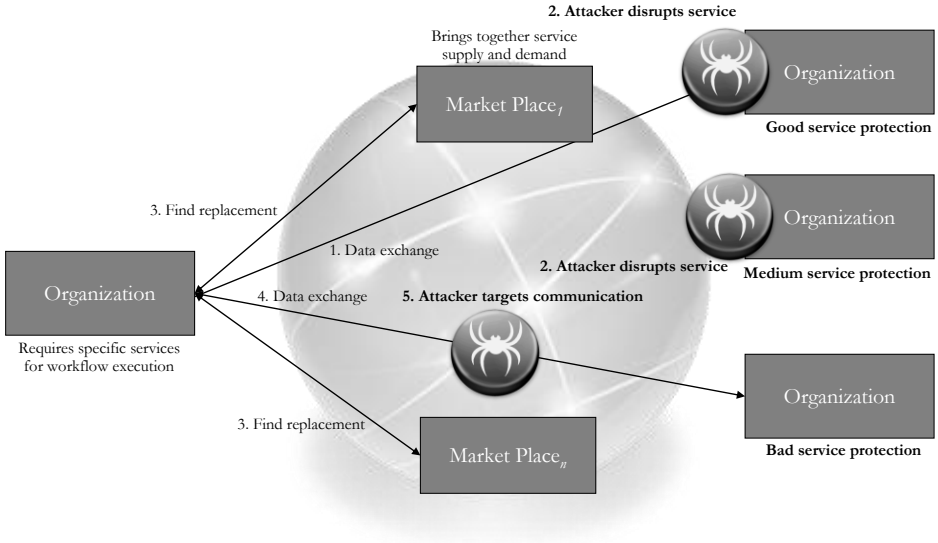

Figure 4: Schematic Quality of Protection differences attack

3.2 Consumer-Provider Communication Analysis

The IoS scenario is based on the dynamic and frequent communication between consumers, providers, and market places. However, even if basic security mechanisms such as message encryption are used, system-inherent threats remain, which are discussed in the following. An attack scenario which makes unauthorized use of the communication between all participants is depicted in Figure 5.

For this attack, we assume an organization contacts several different market places in order to find suitable services for its business processes ("1.a Find service"). Similar to other markets, we can expect market places and even service providers to specialize in particular business areas, e.g., financial services, where also sub-specializations such as capital markets or others can occur. Thus, even if the contents of the communication between the consumer and the market place are not known, e.g., due to encryption, an attacker tracking these requests can gather valuable information about the consumer's business ("1.b Gathers business information […]"), also known as *traffic analysis* (Raymond 2001, pp. 10-11) in computer security or military contexts. Important key data in this context can be which market place is contacted, when, how often, how much data is exchanged, etc. Similarly, the communication between a consumer and a particular provider can be analyzed ("2.a Data exchange" and "2.b Gathers business information

[…]"). A variation of the attack would be to analyze the customers of market places or service providers, e.g., in order to target their customer base.

Therefore, surveying the communication between the participants in the IoS, attackers can create detailed profiles of consumers, providers, and also of market places, depending on the means used maybe not even illegally. These reveal important details, e.g., consumers exploring new business opportunities, the anticipation of mergers and acquisitions, or providers changing their business models.

An important implication of these attacks is the need for a secure communication infrastructure, i.e., one that includes mechanisms for communication obfuscation by generating false or anonymous traffic.

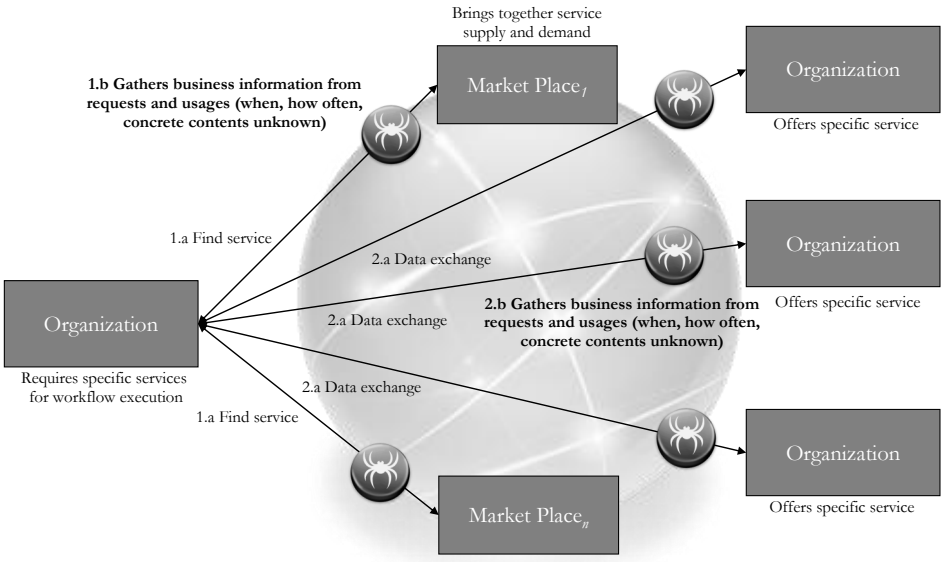

Figure 5: Schematic consumer-provider communication analysis attacks

3.3 Loose and Malicious Service Compositions: Service Encapsulation

The dynamic and loosely coupled composition of services is an important advantage of service-based workflows. However, including globally distributed services from many different providers in a flexible manner introduces the risk of using malicious services for workflow compositions. An attack scenario where a passively malicious service provider has become part of a service composition is depicted in Figure 6.

For this scenario, we assume an organization consumes a specific service from another organization, e.g., paying USD 0.50 per service call ("1. Submit service info", "2. Find service", and "3. Data exchange"). Now, an attacker buys the same service and offers it, e.g., as a mashup for USD 0.40 on one of the market places

("4. Buy service" and "5. Submit service info"). Depending on the service conditions of the service provider and the market places, this might not be illegal but even a desired effect. However, after a while service consumers start to notice the significant cost advantage and may switch to the attacker as their service provider ("6. Data exchange").

In order close the USD 0.10 gap per service call, the attacker uses the information and data received from service consumers, i.e., building user profiles of organizations, extracting sensible information, and selling both to third parties.

Different variations of this attack are possible, e.g., it can also occur with the main goal of consumer-provider analysis (cf. Section 3.2) with the difference that in this scenario even more details can be gathered due to the direct participation of the attacker in the workflow.

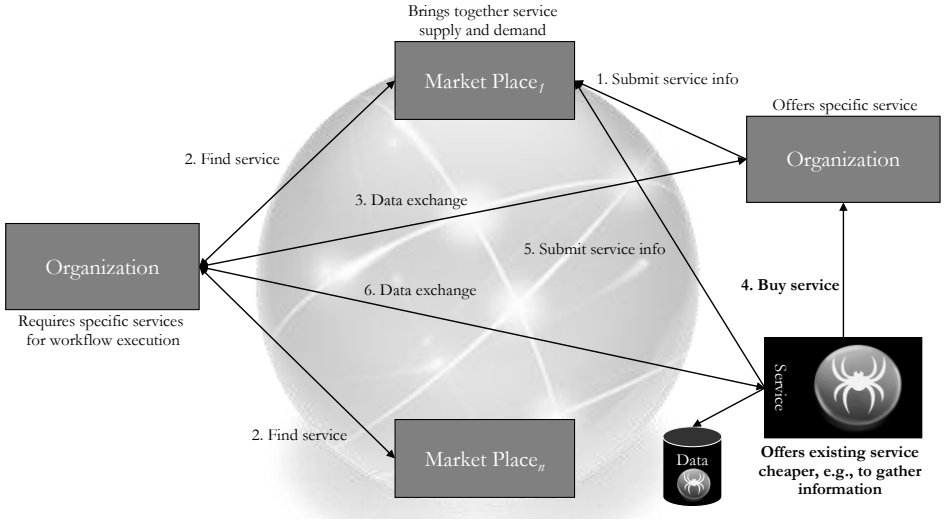

Figure 6: Schematic service encapsulation attack

The most important implication of the attack scenario is that it will be hard to detect as dynamic compositions and mashups are desired effects of service-based workflows in the IoS. As the attack is mostly passive, the attack is likely to be noticed if it is too late, i.e., if the leaked information becomes public. Detection will be even harder if the attacker is "hidden" in a complex chain or even network of workflows which are distributed over many organizational domains and countries. These cases will raise difficult legal and regulatory questions, i.e., regarding claims and liability.

4 Conclusions and Future Work

In this paper, selected security aspects of cross-organizational service-based workflow were presented, i.e., attacks on an Internet of Services scenario. As the current state-of-the-art regarding SOA attacks is focused on technological issues such as Web services, it was necessary to broaden the view towards more business-oriented and service-specific threats in this context. In a first step, an attack taxonomy was developed, which is able to capture the already known attacks, the ones presented in this paper, and also additional ones on higher levels of abstraction. Building on this taxonomy, attacks exploiting service-specific characteristics such as loose coupling and composability were presented. It was shown that these attacks have a fundamental impact on the general security of cross-organizational service-based workflows as they directly target system-imminent concepts. Thus, it is mandatory to address these challenges in order to make the Internet of Services a safe and attractive "place" to do business.

Our next steps will be to extend the attack portfolio and to formalize the attack knowledge using a generic attack metamodel (Miede et al. 2009, pp. 23-34). Furthermore, dedicated countermeasures against these types of attacks will be developed and evaluated, i.e., decentralized service provider reputation for securing service compositions, mechanisms for sender-recipient-anonymity to avoid the exposure of information about business activities in the case of traffic analysis, and service consumer profiling for detecting malicious service consumer behaviour.

Another interesting topic for further research is the support of IT risk management in the context of cross-organizational services in order to evaluate and eliminate vulnerabilities arising from outsourced services.

Acknowledgments

This work is partially supported by E-Finance Lab e.V., Frankfurt am Main, Germany (www.efinancelab.de), BearingPoint Management and Technology Consultants, and by CASED (www.cased.de).

References

Becker A, Buxmann P, Widjaja T (2009) Value potential and challenges of service-oriented architectures – A user and vendor perspective. In: Proceedings of the 17th European conference on information systems (ECIS), Verona.

Braun I, Reichert S, Spillner J, Strunk A, Schill A (2008) Zusicherung nichtfunktionaler Eigenschaften und Dienstgüte im Future Internet of Services. In: Praxis der Informationsverarbeitung und Kommunikation (PIK), 31(4):225–231.

Bundesamt für Sicherheit in der Informationstechnik (2008) SOA-Security-Kompendium: Sicherheit in Service-orientierten Architekturen. https://www.bsi.bund.de/cae/servlet/contentblob/486838/publicationFile/30662/SOA-Security-Kompendium_pdf.pdf. Last access: 2009-11-23.

Cardoso J, Voigt K, Winkler M (2008) Service Engineering for the Internet of Services. In: Enterprise Information Systems 19:15-27. Lecture notes in business information processing (LNBIP). Springer, Berlin.

Eckert C (2007) IT-Sicherheit: Konzepte – Verfahren – Protokolle. Oldenbourg, München.

Eckert J, Ertogrul D, Miede A, Repp N, Steinmetz R (2008) Resource planning heuristics for service-oriented workflows. In: Proceedings of the IEEE/ WIC/ ACM international conference on web intelligence and intelligent agent technology, Sydney.

Gollmann D, Massacci F, Yautsiukhin A (eds) (2006) Quality of protection: Security measurements and metrics. Springer, Berlin.

Hafner M, Breu, R (2008) Security engineering for service-oriented architectures. Springer, Berlin.

Jensen M, Gruschka N, Herkenhöner R, Luttenberger N (2007) SOA and Web services: New technologies, new standards - new attacks. In: Proceedings of the 5th IEEE European conference on Web services (ECOWS), Halle (Saale).

Jensen M, Schwenk J (2009) SOA security - Web Services Standards und Angriffe. In: Patrick Horster, Peter Schartner (eds) D-A-CH Security 2009. syssec, Klagenfurt.

Josuttis NM (2007) SOA in practice: The art of distributed system design. O'Reilly, Sebastopol.

Kanneganti R, Chodavarapu, P (2008) SOA security. Manning, Greenwich.

Leymann F, Roller D (2000) Production workflow: Concepts and techniques. Prentice Hall, Upper Saddle River.

Miede A, Gottron C, König A, Nedyalkov N, Repp N, Steinmetz R (2009) Cross-organizational security in distributed systems. Technical report KOM-TR-2009-01, Technische Universität Darmstadt.

Papazoglou MP, van den Heuvel W (2007) Service oriented architectures: Approaches, technologies and research issues. In: The VLDB Journal 16(3):389-415.

Raymond JF (2001) Traffic analysis: Protocols, attacks, design issues, and open problems. In: Proceedings of the international workshop on designing privacy enhancing technologies: Design issues in anonymity and unobservability, Berkeley.

Schneier B (2004) Secrets and lies: Digital security in a networked world. Wiley, New York.

Schroth C (2007) The Internet of Services: Global industrialization of information intensive services. In: Proceedings of the 2nd IEEE international conference on digital information management (ICDIM), Lyon.