Security and Business Situational Awareness

Roland Rieke[1][2], Maria Zhdanova[1], Jürgen Repp[1]

[1] Fraunhofer Institute SIT, Darmstadt, Germany
[2] Philipps-Universität Marburg, Germany
{roland.rieke,maria.zhdanova,juergen.repp}@sit.fraunhofer.de

Abstract. "Security needs to be aligned with business". Business situational awareness is the ability to continually monitor ongoing actions and events related to business operations and estimate the immediate and close-future impact of the new information. This ability is crucial for business continuity and should encompass all associated aspects. Considering the growing dependability of businesses on IT on the one hand, and ever increasing threats on the other, IT security aspects should get adequate attention in the awareness system. We present an approach to raise business situational awareness using an advanced method of predictive security analysis at runtime. It continually observes a system's event stream to find deviations from specified behavior and violations of security compliance rules. Operational models of the key processes are utilized to predict critical security states, evaluate possible countermeasures, and trigger corrective actions. A security information model maintains the security strategy and explains possible deviations from the originating goal. The approach is demonstrated on an industrial scenario from a European research project.

Keywords: predictive security analysis, process behavior analysis, security modeling and simulation, security monitoring, security strategy, security information and event management, governance and compliance

1 Introduction

Business processes are the most important asset of enterprises, since they provide the basis of the value chain and, thus, define the underlying business model. The Internet today provides an ecosystem, where frequent changes to *business process* models have to be applied, to address changing business needs [31]. This evolving environment, however, also enables new threats and scales up the risks of financial and also physical impact. Thus, business processes must not only be secure, they must be demonstrably so. Situational Awareness (SA) can be viewed as three increasing levels: perception of the elements in the environment, comprehension of the current situation, and projection of future status, that altogether form the basis for decision making [7]. The perception level gives necessary information on the environment recognizing the status and behavior of relevant objects. The comprehension level analyzes and interprets the perceived information in order to identify critical objects and events and determine the current state. The projection level predicts a (close-) future state based on the obtained knowledge to adequately respond to potential problems. All three levels of SA depend on decision maker's goals and context.

In this paper we introduce a flexible and comprehensive modeling approach for business SA that allows us to align business systems with supporting IT and to encompass IT security aspects. This work mainly builds on the Security Strategy Meta Model (SSMM) [28,24] and the Predictive Security Analysis at Runtime (PSA@R) approach [25,6,23], and uses the notion of Enterprise Architecture (EA) as a structured enterprise modeling approach [18]. The SSMM spans all stages of the security monitoring and decision support process, namely: (i) detecting threatening events; (ii) putting them into context of the system state; (iii) explaining their potential impact with respect to the security compliance model; (iv) taking appropriate actions. More specifically, we aim to show that utilizing a model of the prescribed process behavior and the respective compliance rules supports an intelligent security management life-cycle over the whole value creation cycle. The process owners can: (1) assess the achievement of the process objectives better, (2) determine and predict deviations from the planned (prescribed) behavior, (3) monitor and audit the executing process regarding the security policies, (4) assess the treatment of incidents better, (5) identify weak points in the process flow and so better plan corrections of the process flow.

Our contributions: We extended the SSMM with the asset dimension to align the architecture of the managed system and the security directives related to the critical assets. We describe an implementation of security strategy management based on the SSMM using Security Strategy Processing Components (SSPCs) provided by a prototypical implementation of PSA@R. Moreover, we present new results from the application of PSA@R implemented in the Predictive Security Analyzer (PSA) tool to industrial scenarios. These results demonstrate the integration of security status information into the PSA@R security directives and the co-action of Complex Event Processing (CEP) and PSA for attack detection.

This paper is structured as follows: Section 2 explains the background and section 3 presents our systemic approach for business SA and the extended SSMM. Section 4 describes the architecture and functionality of the PSA providing its implementation. Section 5 describes the adaptation of the PSA to industrial scenarios, followed by concluding remarks in Section 6.

2 Background

An EA meta model describes the organization of an enterprise encompassing multiple views (structural layers), equally focused on business-related elements, such as business goals and processes, and on application systems and IT infrastructure [18]. A variety of EA frameworks were established in practice and research [13]. From the most cited ones, the Zachman Framework [30], The Open Group Architectural Framework (TOGAF) [32], and Sherwood Applied Business Security Architecture (SABSA) [29] were evaluated for security engineering. While operational risk management is an important aspect of EA, IT security –

being one of the most critical operational risks faced by IT-enabled enterprises – is not considered by the majority of EA frameworks [34]. Thus, though EA helps to reveal sensitive assets and identify (multi-level) dependencies between them, this information needs to be enriched with security concepts.

Modeling concepts for combined views of business, application, physical, and technical information are given in [10], while [27] introduces the use of event-triggered rules for sensing and responding to business situations. A formalized approach to security risk modeling for electronic business processes in [33] comprises simulation aspects, but not the utilization of runtime models. A classification of approaches in the field of Business Process Management (BPM) is given in [1]. According to this classification, the work presented here supports the "check conformance using event data" approach, where information from the process model and the event data is used to identify deviations of runtime behavior from expected behavior. The work on runtime compliance verification for business processes in [15] is complementary to the work presented here.

3 Systemic Approach for Business Situational Security Awareness

A systemic approach for business SA consists of three interrelated parts (see Fig. 1): a *business context* part defined by an EA meta model, a *security information* part given by the Security Information Meta Model (SIMM), and an *operational aspects* part expressed with the SSMM. These models are linked together through model artifacts.

In order to provide a flexible and comprehensive concept for business SA that considers security aspects we adopt a modeling approach introduced in [28,24]. This approach enables a multi-level and cross-domain analysis of security issues and builds upon two interlinked semantic concepts: the SIMM and the SSMM. The SIMM [24] defines a top-down security design process consisting in consecutive definition of four interrelated model parts: (i) high-level (security) goals, (ii) security requirements, (iii) measurement requirements, and (iv) objects of measurement. The SIMM can be viewed as a hierarchy, each level of which refines concepts of higher levels depending on the associated environment. A similar approach - but with a different focus - has been proposed by the project PoSecCo, where a traceable chain of connected policies bridges three different abstraction levels: business policies, IT security policies, and security configurations [2]. In order to obtain system security requirements that convey targeted security goals one would need to employ some procedure for security requirement elicitation [17,8]. Measurement requirements specify how security status of the system, i.e., conformance to given security requirements can be verified (measured). Note that the measurement requirements part of the SIMM is a new structure extending the definition of the Information Security Measurement Model (ISMM) given in the ISO/IEC 27004 standard [11], which is introduced to link the information need to a relevant object of measurement. Operational aspects of the SIMM are covered by the SSMM [28].

The SSMM provides a way for users to define at an abstract level detection rules for security incidents that can be automatically compiled into tool-specific rules, e.g., event correlation rules of a CEP engine. The SSMM has four parts, namely : *on*, : *if*, : *do*, and : *why*, which are derived from the measurement requirements on one hand, and which refer back to the SIMM on the other hand (cf. Fig. 1). The : *on* part specifies *event stream property* or event patterns that indicate a security incident. This part describes anomalies and misuse signatures using parameters extracted from an event stream (channel) together with detection criteria evaluating extracted parameters. The event stream property can be used to express both horizontal event correlation, as steps in a work-flow, and vertical correlation across multiple abstraction levels, e.g., correlation of alerts received from an intrusion detection system with violated security requirement. The : *if* part of the model provides *context information* specifying system state conditions to be validated whenever a (malicious) event pattern is matched. Context information increases the probability to discover targeted attacks and is essential for stateful incident detection, such as practiced in process security analysis. Moreover, the SSMM supports the whole cycle of security incident management including incident response. Its : *do* part models executable *response actions* to be performed when an incident is detected, ranging from notification to autonomous re-configuration of the IT system, e.g., blocking a malicious IP address on a firewall. In order to close the traditional *plan-do-check/study-act* cycle [5], incident detection needs to be linked to the high-level security requirement. This is achieved by the : *why* part of the SSMM, represented by the dotted arrow in Fig. 1. It defines *security pertinence* of an incident and should contain a reference to security concepts specified by the SIMM. The : *why* part helps to estimate the impact of the incident and explains why certain countermeasures are taken. A concrete instance of the SSMM is called Security Strategy Model (SSM) and is made of specific rules, Security Directives (SDs).

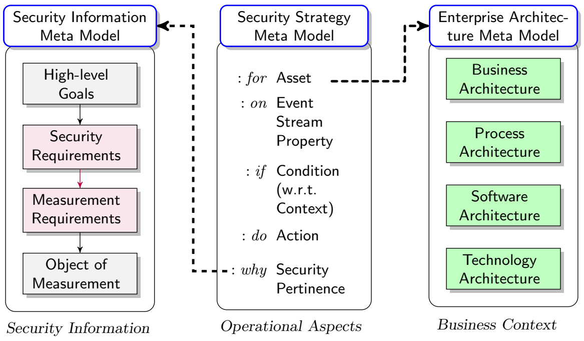

Fig. 1. Modeling approach for business situational awareness

In order to connect the enterprise assets represented by an EA model and the security strategy, we extend the SSMM structure with the : *for* part that provides an explicit *asset reference.* It enables propagation of security requirements as well as systematic tracing of security incidents through the abstraction layers of EA and evaluation of their impact in regard to business goals and processes. This extension can also facilitate operational aspects of creation and management of SDs in the following ways. First, the : *for* part enables easy identification of dependent SDs. Then, an activation of one of the dependent SDs can cause a cascade triggering of others even if it is not explicitly defined in the : *do* part. The latter means that an incident can be detected even if some sensors implementing the : *on* part in dependent SDs are compromised. Moreover, the link between EA and the SSMM allows completeness analysis of SDs in order to reveal missing or redundant SDs and ensure that all critical security properties are covered. It also aids in detection of conflicting response actions which can block operations within the enterprise if realized. Finally, an explicit asset reference in an SD helps to identify optimal measurement points, including domain-specific sensors and physical sensors, formulate context conditions related only to a particular asset and to update this information if the underlying EA changes, e.g. new sensors appear or security systems are deployed. Thus, the extension to the SSMM allows an enterprise to increase overall SA and to respond to security incidents in a more robust and adequate way due to closer semantic relations and mutual information exchange between security concepts and enterprise structures. In the following we use the term SSMM to refer to the extended SSMM.

4 Security Strategy Processing

Conceptually, the implementation of SSMM processing is composed of SSPCs [24]. One specific component called PSA [25,6,23] has been developed by the authors of this paper. At runtime, the PSA *observes* the operation of a managed system by analyzing events received from this system. A novel capability in this approach is that it utilizes an operational process specification to compute the pre-planned process behavior depending on the actual state of an observed system. Deviations from the expected behavior trigger *uncertainty management* and possibly alerts. Formally, the behavior of the operational process model is described by a Reachability Graph (RG) [19], also referred to as Labelled Transition System (LTS) [20]. PSA@R uses the RG to *predict the close-future behavior of the process instance.* A subgraph of the RG starting with the current state of the process instance can always be computed on-the-fly based on the formal process model. The *prediction depth* is the depth of this subgraph starting from the current state.

The PSA supports the specification and on-the-fly check of security compliance rules as well as visualization of the current security status. Possible close-future process actions can be predicted based on the operational process specification and the current process state as reflected in the model. This knowledge about the expected behavior is used to predict upcoming critical states regarding given security compliance rules. This *judgment* whether the observed system behaves according to the given rules enables proactive reactions for risk mitigation. Figure 2 shows the architecture of the PSA and its interaction with the observed system as well as other systems in the environment that can play the role of SSPCs. The *PSA modeler* provides the user interface for model management and visualization of the current system state, and the *PSA core* performs process security analysis at runtime. For the applications presented in this paper, the PSA was deployed in the next-generation Security Information Event Management (SIEM) architecture MASSIF [35] to perform (high-level) security event processing and anomaly detection on the business application (service) layer.

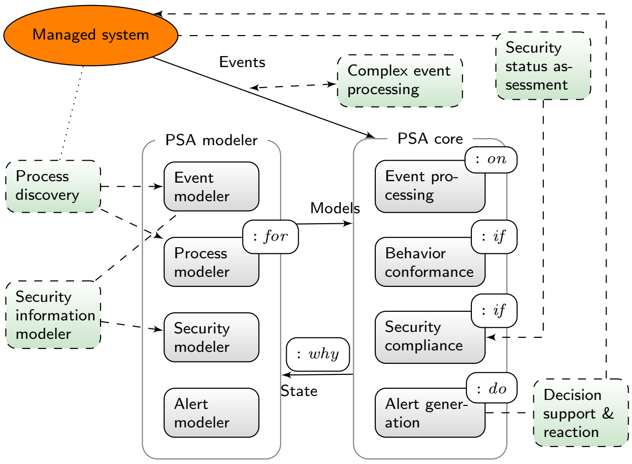

Fig. 2. Architecture and environment of the predictive security analyzer

The *event processing component* of the PSA core processes the : *on* part of the SSMM. It maps the events to the corresponding process instance, and creates abstract events containing only information that is relevant for security processing. This component can optionally be supported by external CEP. In the MASSIF framework, the coaction of CEP and PSA for attack patterns detection was realized by two components, namely Generic Event Translation (GET) [4] for distributed collection and preliminary correlation of raw events and a high-performance CEP [3] for correlation. The PSA *behavior conformance component* and the *security compliance component* process the : *if* part of the SSMM. The abstract events are used by the *behavior conformance component* to update the respective state of process instance models reflecting the actual state of the running processes and behavior anomalies are identified. By executing the security model the *security compliance component* identifies process states critical from the security perspective. The security compliance component can optionally be supported by external components for *security status assessment*.

In MASSIF this was realized by the Attack Modelling and Security Evaluation Component (AMSEC) [12]. If a process anomaly or a security critical state is detected or predicted, the PSA *alert generation component*, which implements the : *do* part of the SSMM, triggers a security event using the mapping configured in the alert model. In MASSIF, these alerts were forwarded to the Decision Support and Reaction (DSR) component [9] for countermeasure selection and response. Backward references within the process and security models allow to visualize the current process state with the PSA *process modeler component* which is related to the : *for* part of the SSMM and the security state within the *security modeler component* of the PSA. The PSA modeler manages reference to the originating goal with the help of a project description. This provides basic functionality for the : *why* part of the SSMM.

5 Industrial Setups: Lessons Learned

Based on experiences with application of an early prototype in a logistics scenario [6], we have applied the PSA tool in several use cases, each of which allowed us to examine a particular aspect of PSA@R in a realistic industrial setup [16]. The application scenarios related to four industrial domains: (i) managed enterprise service infrastructures for outsourced IT services [22]; (ii) mobile money transfer services provided by a mobile network operator [26]; (iii) the Olympic Games IT infrastructure management [21]; (iv) critical infrastructure process control (on the example of a storage dam in a hydroelectric power plant) [4]. (Mis)use cases made available for each domain by scenario providers covered one or several steps of the proposed security analysis cycle, from behavior conformance monitoring to detection of security violations and prediction of security-critical situations in the near future. In the range of the applications presented in this section, the PSA was deployed as a model management component of the next-generation SIEM architecture MASSIF to perform (high-level) security event processing and anomaly detection on the business application (service) layer [35]. Collection and preliminary correlation of raw events were carried out by other MASSIF components, such as GET [4] and CEP [3]. Alerts produced by the PSA were forwarded to the DSR system which implemented countermeasure selection and response mechanisms [9]. In this section we exemplarily summarize our experience using an industrial scenario from the MASSIF project.

5.1 Olympic Games

In today's media society, the Olympic Games have become one of the most profitable global media events. Olympics media diffusion, international dimension, and symbolic value constitutes a lucrative target for attackers. As a consequence, security has become a top priority [21]. In the MASSIF project, we have investigated security provisioning for Olympic Games services accessible over the Internet, such as the accreditation and sport entries applications. Considering high security risks, it is reasonable to assume that extensive efforts are made to protect the IT infrastructure of the Olympic Games from both persistent and emerging threats. In particular, we considered a misuse case, which involved a targeted "low-and-slow" (persistent) attack on a web application server providing the accreditation service for participants [14,22]. The adversary is aware that the IT infrastructure is under continuous security monitoring, therefore, she executes multiple low profile actions distributed over longer period of time. In our trial setup, the adversary first compromises a sports entries web server in order to brute-force a local administrative account. When this attempt fails, she performs port scanning to discover an open LDAP port on a back-end authentication server. The adversary launches a command injection attack to obtain root access on the authentication server. She retrieves a list of user credentials and resorts to exhaustive search on the accreditation web server to find some user account with sufficient privileges for the accreditation application.

Assets (: ***for*****).** The accreditation application processing accreditation data is the critical asset targeted. In order to gain access to the accreditation data other entities in the IT infrastructure – the sport entries server and authentication server – get compromised to provide a launch site for the final attack step.

Event Stream (: ***on*****).** Security events were generated using a testbed that reproduced the Olympic Games IT infrastructure with deployed security controls. These events were sent to the CEP component of the MASSIF SIEM where they were correlated over different time intervals to reveal adversarial behavior patterns. If malicious activity was detected, the CEP produced an alarm with a specific identifier (e.g., *data_tampering*, *privilege_escalation*) which was forwarded to the PSA for further correlation. The following alarm identifiers referring to particular attack steps were used:

Condition (: ***if*****).** The PSA aggregates alarms generated by different security controls in the observed infrastructure evaluates the security state in regard to the specified "low-and-slow" attack and predicts near future security-critical states and potential security violations by means of the security monitor presented in Fig. 3. The monitor automaton has two critical states – *crashes_edirectory* and *unusual_activity* – in which the PSA generates a security alert.

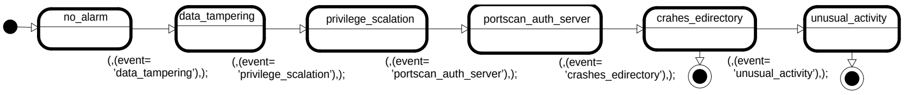
no_alarm
data_tampering
privilege_scalation
portscan_auth_server
crahes_edirectory
unusual_activity
(,(event= 'data_tampering'),);
(,(event= 'privilege_scalation'),);
(,(event= 'portscan_auth_server'),);
(,(event= 'crashes_edirectory'),);
(,(event= 'unusual_activity'),);

Fig. 3. Security monitor for the Olympic Games scenario

Action (: ***do*****).** If a critical state of the monitor automaton (see Figure 3) is reached, the PSA generates a corresponding security alert that was forwarded to the DSR system, which blocked the IP address of the adversary.

Security Pertinence (: ***why*****).** In this case, the goal is to "prevent unauthorized access to the accreditation data".

5.2 Lessons Learned

The main problem we faced during the adaptation to the use case scenarios is that none of them a priori involved either process-aware information systems or process specifications. Another problem concerns synchronization and ordering of events coming from different systems with different time bases. Thus, a point of particular interest regarding these industrial setups is exploitation of process-aware security controls similar to the PSA in “process-unaware” environments that can often be seen in the wild. In the Olympic Games scenario, it was not possible to relate the events from different event sources to the respective process instance because the needed event attributes were missing. As in this case, the application provider could not modify the involved systems, the modeled process behavior thus did not reflect the business process but rather an attack process (cf. Fig. 4). The scenario provider reported that once the models are completed, the regular use is fairly simple [16].

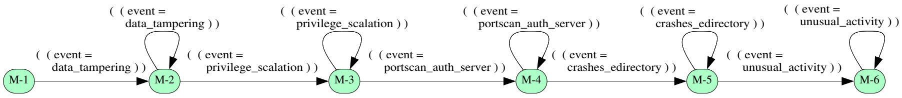
((event = data_tampering))
((event = data_tampering))
((event = privilege_scalation))
((event = privilege_scalation))
((event = portscan_auth_server))
((event = portscan_auth_server))
((event = crashes_edirectory))
((event = crashes_edirectory))
((event = unusual_activity))
((event = unusual_activity))
M-1
M-2
M-3
M-4
M-5
M-6

Fig. 4. Reachability graph of the attack process in the Olympic Games scenario

A general finding of our work on runtime security assessment is that the traditional *plan-do-check/study-act* cycle [5] needs to be extended, when applied to information security measurement. In the *plan* phase, it should not only establish the objectives, identify security requirements, and analyse the design of the system, but also *plan runtime measurements*. In the *do* phase, it should not only analyse the configuration of the implemented plan, and verify that the goals are met, but also *provide data for runtime analysis*. In the *check/study* phase, it should *identify and study deviations of measured from expected results*, *check for compliance*, and *forecast critical behavior*. Finally, in the *act* phase, it should analyse security consequences, determine their root causes, and trigger corrective actions.

6 Conclusion and Research Directions

We have argued that business goals and compliance requirements, which create obligations for security management, need a meta model - such as SSMM - that consolidates the necessary security strategy information. Therefore, we extended the SSMM, which has been introduced in [28,24], with an EA model to link the architecture of the managed system and the security directives defined for the critical assets. We have exemplarily shown, how to implement the systemic approach for security strategy management based on the SSMM, by means of a mapping of components of our PSA prototype to SSPCs.

The PSA provides early awareness about deviations of a running process from expected behavior - as specified by the model - and generates triggers for decision support and reaction. As security relies on the compliance of actual behavior with the given specifications, this early detection of changes and reaction elevates security of the process in question. In combination with other novel applications, the PSA enables anticipatory impact analysis, decision support, and impact mitigation by adaptive configuration of countermeasures.

In particular, we have demonstrated on an industrial scenario, how the SSMM can be used in a framework of SSPCs, to observe system and process behavior, detect anomalies, and provide situational awareness not only on an infrastructure but also up to business process level. This scenario also demonstrates the coaction of CEP and PSA and the integration of security status information into PSA security monitoring for attack process detection. The external security status information from AMSEC enriches the context awareness. It is used by the PSA to improve the assessment of the security status of the observed process and thus facilitates the prediction of security policy violations in close future.

Results published in [23] confirm that model-based analysis as implemented in the PSA prototype is applicable and fast enough for security analysis of important real-world applications at runtime. However, in order to apply our PSA@R method easily, systems, applications, and processes should be *designed for security assessment at runtime*. The approach has been validated specifically with respect to security concerns but is also applicable to on-the-fly analysis of generic compliance and dependability requirements. Further results published in [36], where we compared PSA@R with classical fraud detection approaches, indicate that we can achieve better recognition performance.

For future work, we plan to investigate the adaptability of our security strategy management approach to decentralized Internet of things ecosystems, where traditional centralized security management concepts will not be applicable and - from the privacy perspective - not even desirable.

Acknowledgments. This research was supported by the European Commission in the context of the project MASSIF (ID 257475) and the German Federal Ministry of Education and Research in the project ACCEPT (ID 01BY1206D).

References

1. van der Aalst, W.M.P.: Business process management: A comprehensive survey. ISRN Software Engineering p. 37 (2013)
2. Arsac, W., Laube, A., Plate, H.: Policy chain for securing service oriented architectures. In: Pietro, R.D., Herranz, J., Damiani, E., State, R. (eds.) DPM/SETOP. Lecture Notes in Computer Science, vol. 7731, pp. 303–317. Springer (2012)
3. Callau-Zori, M., Jiménez-Peris, R., Gulisano, V., Papatriantafilou, M., Fu, Z., Patiño Martínez, M.: STONE: A Stream-based DDoS Defense Framework. In: Proceedings of the 28th Annual ACM Symposium on Applied Computing. pp. 807–812. SAC'13, ACM, New York, NY, USA (2013)

4. Coppolino, L., D'Antonio, S., Formicola, V., Romano, L.: Enhancing SIEM Technology to Protect Critical Infrastructures. In: Hämmerli, B.M., Kalstad Svendsen, N., Lopez, J. (eds.) Critical Information Infrastructures Security, Lecture Notes in Computer Science, vol. 7722, pp. 10–21. Springer Berlin Heidelberg (2013)
5. Deming, W.E.: The new economics for industry, government, education / W. Edwards Deming. Massachusetts Institute of Technology, Center for Advanced Engineering Study, Cambridge, MA : (1993)
6. Eichler, J., Rieke, R.: Model-based Situational Security Analysis. In: Proceedings of the 6th International Workshop on Models@run.time at the ACM/IEEE 14th International Conference on Model Driven Engineering Languages and Systems (MODELS 2011), CEUR Workshop Proceedings, vol. 794, pp. 25–36. RWTH Aachen (2011)
7. Endsley, M.: Toward a theory of situation awareness in dynamic systems. Human factors 37(1), 32–64 (1995)
8. Fuchs, A., Rieke, R.: Identification of Security Requirements in Systems of Systems by Functional Security Analysis. In: Casimiro, A., de Lemos, R., Gacek, C. (eds.) Architecting Dependable Systems VII, LNCS, vol. 6420, pp. 74–96. Springer (2010)
9. Granadillo, G., Jacob, G., Debar, H., Coppolino, L.: Combination approach to select optimal countermeasures based on the rori index. In: Innovative Computing Technology (INTECH), 2012 Second International Conference on. pp. 38–45 (2012)
10. Innerhofer-Oberperfler, F., Breu, R.: Using an enterprise architecture for it risk management. In: Eloff, J.H.P., Labuschagne, L., Eloff, M.M., Venter, H.S. (eds.) ISSA. pp. 1–12. ISSA, Pretoria, South Africa (2006)
11. Iso Iec: ISO/IEC 27004:2009 - Information technology - Security techniques - Information security management - Measurement (2009)
12. Kotenko, I., Chechulin, A.: Attack modeling and security evaluation in SIEM systems. In: International Transactions on Systems Science and Applications, vol. 8. SIWN Press (December 2012)
13. Lange, M., Mendling, J.: An experts' perspective on enterprise architecture goals, framework adoption and benefit assessment. In: Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2011 15th IEEE International. pp. 304–313 (Aug 2011)
14. Llanes, M., Prieto, E., Diaz, R., , Coppolino, L., Sergio, A., Cristaldi, R., Achemlal, M., Gharout, S., Gaber, C., Hutchison, A., Dennie, K.: Scenario requirements (public version). Tech. rep., FP7-257475 MASSIF European project (April 2011)
15. Maggi, F.M., Montali, M., Westergaard, M., van der Aalst, W.M.P.: Monitoring business constraints with linear temporal logic: An approach based on colored automata. In: Business Process Management (BPM 2011). LNCS, vol. 6896, pp. 132–147. Springer (2011)
16. MASSIF project consortium: Acquisition and evaluation of the results. Deliverable D2.3.3, FP7-257475 MASSIF European project (September 2013)
17. Mellado, D., Blanco, C., Sánchez, L.E., Fernández-Medina, E.: A systematic review of security requirements engineering. Computer Standards & Interfaces 32(4), 153–165 (2010)
18. Nightingale, D.J., Rhodes, D.H.: Enterprise systems architecting: emerging art and science within engineering systems. In: MIT Engineering Systems Symposium (March 2004)
19. Ochsenschläger, P., Rieke, R.: Abstraction based verification of a parameterised policy controlled system. In: Gorodetsky, V., Kotenko, I., Skormin, V.A. (eds.) Computer Network Security, Communications in Computer and Information Science, vol. 1, pp. 228–241. Springer (2007)

20. Peled, D.A.: Software Reliability Methods. Springer, 1 edn. (2001)
21. Prieto, E., Diaz, R., Romano, L., Rieke, R., Achemlal, M.: MASSIF: A Promising Solution to Enhance Olympic Games IT Security. In: International Conference on Global Security, Safety and Sustainability (ICGS3 2011) (2011)
22. Rieke, R., Coppolino, L., Hutchison, A., Prieto, E., Gaber, C.: Security and reliability requirements for advanced security event management. In: Kotenko, I., Skormin, V. (eds.) Computer Network Security, LNCS, vol. 7531, pp. 171–180. Springer (2012)
23. Rieke, R., Repp, J., Zhdanova, M., Eichler, J.: Monitoring security compliance of critical processes. In: Parallel, Distributed and Network-Based Processing (PDP), 2014 22th Euromicro International Conference on. pp. 525–560. IEEE Computer Society (Feb 2014)
24. Rieke, R., Schütte, J., Hutchison, A.: Architecting a security strategy measurement and management system. In: Proceedings of the Workshop on Model-Driven Security. pp. 2:1–2:6. MDsec '12, ACM, New York, NY, USA (2012)
25. Rieke, R., Stoynova, Z.: Predictive security analysis for event-driven processes. In: Computer Network Security, LNCS, vol. 6258, pp. 321–328. Springer (2010)
26. Rieke, R., Zhdanova, M., Repp, J., Giot, R., Gaber, C.: Fraud detection in mobile payment utilizing process behavior analysis. In: Availability, Reliability and Security (ARES), 2013 Eighth International Conference on. pp. 662–669. IEEE Computer Society (2013)
27. Schiefer, J., Rozsnyai, S., Rauscher, C., Saurer, G.: Event-driven rules for sensing and responding to business situations. In: Jacobsen, H.A., Mühl, G., Jaeger, M.A. (eds.) DEBS. ACM International Conference Proceeding Series, vol. 233, pp. 198–205. ACM (2007)
28. Schütte, J., Rieke, R., Winkelvos, T.: Model-based security event management. In: Kotenko, I., Skormin, V. (eds.) Computer Network Security, Lecture Notes in Computer Science, vol. 7531, pp. 181–190. Springer (2012)
29. Sherwood, J., Clark, A., Lynas, D.: Enterprise Security Architecture: A Business-Driven Approach. CMP Books (2005)
30. Sowa, J.F., Zachman, J.A.: Extending and formalizing the framework for information systems architecture. IBM Syst. J. 31(3), 590–616 (Jun 1992)
31. Tallon, P.: Inside the adaptive enterprise: an information technology capabilities perspective on business process agility. Information Technology and Management 9(1), 21–36 (2008)
32. The Open Group: TOGAF Standard Version 9.1 (2012), `http://pubs.opengroup.org/architecture/togaf9-doc/arch/`, [Online; accessed 24-May-2015]
33. Tjoa, S., Jakoubi, S., Goluch, G., Kitzler, G., Goluch, S., Quirchmayr, G.: A formal approach enabling risk-aware business process modeling and simulation. IEEE Transactions on Services Computing 4(2), 153–166 (2011)
34. TOGAF-SABSA Integration WG: TOGAF and SABSA Integration. Whitepaper. The Open Group, The SABSA Institute (October 2011)
35. Verissimo, P., et al.: Massif architecture document. Tech. rep., FP7-257475 MASSIF European project (April 2012), `http://www.massif-project.eu/sites/default/files/deliverables/MASSIF_Architecturedocument_v15_final.zip`, [Online; accessed 24-May-2015]
36. Zhdanova, M., Repp, J., Rieke, R., Gaber, C., Hemery, B.: No smurfs: Revealing fraud chains in mobile money transfers. In: Proceedings of 2014 International Conference on Availability, Reliability and Security, ARES 2014, pp. 11–20. IEEE Computer Society (2014)