Analysis of Dynamic Service Oriented Systems for Security Related Problems Detection

Grzegorz Kołaczek
Faculty of Computer Science and Management
Wroclaw University of Science and Technology
Wroclaw, Poland
Grzegorz.Kolaczek@pwr.edu.pl

Jolanta Mizera-Pietraszko
Faculty of Mathematics, Physics and Computer Science
Opole University
Opole, Poland
jmizera@math.uni.opole.pl

***Abstract*— The paper presents an approach to solve some problems arising in the management process of IT security. Our motivation of this research is to study in every detail the context of service oriented systems, which can be defined as considerable heterogeneous, dynamic and flexible configuration of the hardware and software system resources. The fundamental difference between security management systems with traditional centralized and monolithic architecture and service oriented systems is discussed. We propose a multilayered-reference model for service-oriented systems aimed predominantly at principal objectives related to IT based systems security working in dynamic environments. Likewise, considered are some dedicated to service-oriented environments key assumptions of a multi-agent system design with the aim at security analysis. The last part of the paper presents briefly the results of our analysis of IT security aspects, performed on the comparison basis of correlation between the events observed at the low and at high layers of our reference model.**

Keywords—service oriented systems; security level; security incidents)

I. INTRODUCTION

The ability to provide security in computer systems is one of the most principal non-functional requirements in software engineering and the quality attribute discernible at the system run-time. While in the early stages of considering information systems security, the issues were marginalized [13], over the recent years, with the dramatic increase of accessibility to information owning to its ubiquitous nature, security problems have become the key element for the possibility of further development [7],[8]. Moving from monolithic architectures and centralized systems to distributed and service-oriented systems makes the yet reliable conventional methods of security assessment not sufficient and thus, while building infrastructure in the area, they need a strong support with the new aspects such as: a high level of resources heterogeneity, their diverse granularity and a high dynamic variation [6]. Service-oriented systems encounter many security problems that cannot be overcome simply by moving the patterns and solutions applicable to the systems with other architectures (eg. centralized systems, monolithic) [3]. An example illustrating the specificity of the problems in service-oriented systems may be a task of data protection to prevent security code breaches. In monolithic systems, separation of resources, is a standard architecture, as the data processed by the system remain within it and therefore an access to the particular data set implies the necessity to have an appropriate permissions granted in the context of this system and its specific resources. Consequently, in order to protect the confidentiality and integrity of the system data, it is enough to provide a full strong access control. On the other hand, data processing in service-oriented systems such as "software as a service" (SaaS) platforms, can be easily disclosed and modified in an unauthorized manner even despite a reliable massive access control. One of the reasons is that confidentiality is susceptible to loss due to some errors in the system separation mechanisms where the data is stored while the physical location of the data is shared by some other services at the same time [22].

II. IT SECURITY

A. Generic Security Problems in IT Systems

Specificity of IT security problems stems from diversity of information system architecture. Security issues of centralized systems, in which processing is performed in the highlighted central node, are a subset of problems arising in the systems with distributed architecture. Centralized systems allow for simplified processing control procedure of and unrestricted access to the resources. Naturally, the central system element is to be protected and monitored in real time. Distributed systems allow data processing and storage in different places of the system environment, quite often geographically located very far from each other. Such a quality of distributed systems implies that not only the same security level should be ensured at all the locations of the system run time environment, but the whole diversity of the local system components such as diverse computing power, different levels of interaction with the users, different requirements arising from the locally applicable legal system, etc., should comply with the central server. For distributed systems, the critical factor is also the requirement to ensure a secure communication between all the system components. Complexity level of selection of adequate methods and mechanisms for security management system grows proportionally to the number and variety of the

978-1-5090-5795-5/17/$31.00 ©2017 IEEE

distributed system components being a subject to protection [1].

Likewise, heterogeneity of the solutions in designing computer system architecture also impedes the process of providing a reliable security level evaluation. In today's systems different solutions with reference to the physical system resources and the software layer are used. This creates the need for the IT security management of the technical specifications of every system characterstic (eg. the availability of mechanisms which support hardware access control, programming errors detection, etc.) to guarantee the possibility of secure interaction between the system elements with different hardware and software type [9].

A similar complexity growth of security management process is noticable when it comes to moving from monolithic systems to the systems with service-oriented architecture (ang. Service-Oriented Architecture, SOA).

Service-oriented systems rely on the services to provide some user-defined functionalities. Service is defined as a software component that can work independently of the others with an interface to provide the implemented functionalities [19]. SOA is mainly related to the non-functional properties such as the reuse of software components, encapsulation of the system functionality, precisely defined interfaces and flexibility of applications in adopting an approach to create the framework for the service composition.

The life cycle of SOA application consists of four phases: modeling, composition, execution and management. These phases apply to all applications built with accordance to the SOA paradigm and they are specified by varying degrees of complexity and peculiar problems, including IT security. Reference model for service-oriented systems defines five layers dedicated to the fundamental system functions, ranging from low-level features associated with the provisioning of communication among the services and finishing with the description of the high-level dependencies between the services resulting from the business processes (Figure 1).

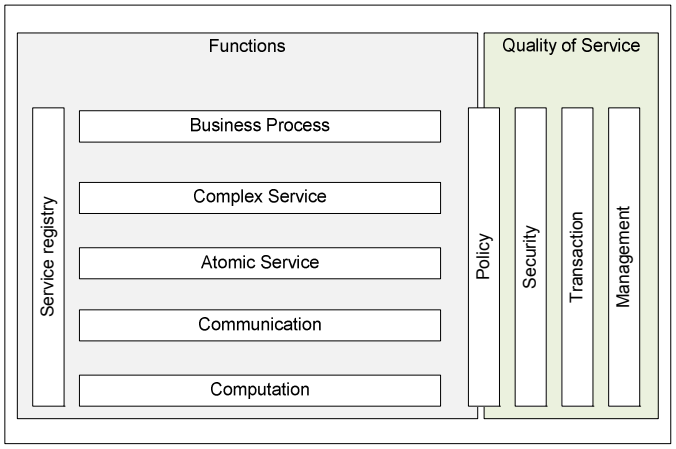

Fig. 1. SOA layered architecture

B. *Security Management in Dynamic Environments of Service-Oriented Systems*

Complexity of the security related problems in service-oriented systems is also determined by their paralel persistence; that is those related to development of distributed heterogeneous systems and confronted with some security issues like during the processes of modeling, composing, adjusting and service management. Moreover, both protection and evaluation of service-oriented systems security level considers specification of the reference model (Figure 1). Particularly, such an impact on process of security management in service-oriented systems can be described by the following requirements [23]:

- identity management - a service may be executed in different contexts and by different users' groups; the service should always be carried out with all the permissions appropriate for a given execution context (security of business processes)
- proper security controls management – it is necessary to provide all the appropriate mechanisms for security management, both at the level of individual services as well as for composite services (security services)
- security management sovereignty - it is necessary to guarantee the security management mechanisms independent of the underlying technology hardware and software (security service description)
- seamless connection to other organizations on a real-time basis - services can be offered by different service providers; the final functionality delivered to the user is supplied with the resources (services) originating from those different service providers, however, it should not be noticeable to the user (security protocols services)
- protection of data in transit and at rest - execution of composite services may be related to the data flow in systems managed by different entities and using different security mechanisms; regardless of the place where the data are processed and for what systems they are allocated, it should be possible to manage data security accurately (transport safety).

The opportunity to provide adequate solutions for evaluation of the security level and the trust level affect the following SOA system features:

- a high level of heterogeneity (in both hardware and software)
- enornous dissipation of resources.
- intensity and diversity of communication channels,
- varied granularity of tasks and resources,
- resource sharing,
- competing for resources,
- dynamics of changes and the volatility of resources,

- high-level requirements resulting directly from the specific business processes.

III. Evaluation of Security and Trust Level

The ability to determine the level of security is of a great importance thoughout the whole process of security management, hence it is monitored at every stage of the system life cycle from the design, through dimensioning, implementation, to management of the final software product. At the design stage identified are all the user's requirements also from the perspective of the expected security level. Appropriate selection and implementation of protection methods determines the extent to which these requirements will be met. At the run time the security level is constantly monitored to allow the user a rapid intervention when it comes to a security incident.

Assessment of the trust level in the service-oriented systems is equaly important as the ability to estimate the security level. Final security level in service-oriented systems is influenced by the series of security events not only those related to the direct user-system interaction, but to the interactions between the services, in particular. Consequently, evaluation of the trust level between the services and the users enables to keep control over the access to the system resources such that it minimizes the risk of fraud and security breaches. Furthermore, service-oriented systems, in which the services are offered by many far distant providers making the services implementation details unavailable for other services and the system users, considered is the inference about the security level based on the incomplete and often uncertain knowledge. In this context, evaluation of the trust level becomes the fundamental task of the security management system. The trust level is the representation of subjective beliefs about the level of security, such that its value can be estimated from the unreliable and incomplete data processed at the specific system state. The security level and the trust level in the computer system are two integral quality aspects of the security management process [2].

The level of system security is a value defined in the security metric space. A set of elements of the security metric space is defined by the characteristic system states in the context of specific security requirements.

In the process of security management, there are two separate tasks: providing the required level of security and the assessing the current level of security.

The task of providing the required level of security of a computer system is aimed to reduce the likelihood that the identified risk factors are likely to reduce the security level of the system below the predetermined value. The task of providing the required level of security is decomposed into subtasks dedicated to the process of protecting stored, processed and transmitted data by ensuring the integrity, confidentiality and accessibility [21].

The goal of assessing the security level is to estimate the current value of the risk associated with the possibility of losing the integrity, confidentiality or availability of the system resources despite the applied methods of protection.

The trust level is defined as an abstract quantity that represents the value of the trust, which is reflected in the subject's belief that the system will operate in accordance with the objectives [10]. The subject may be a standalone software component (autonomus agent) or the system's user. The trust level in the context analysis of the computer security has been introduced to enable the automation of decision-making processes relating to security, eg. in tasks of an access control, the management rights. The role of estimating the trust level is to define a function on the set of system components (trustee) with the values of the set trust levels.

The trust level allows the formal representation of the subjective beliefs about the security level of a part or the whole system. The trust level is different from the security level in the way that it is defined with the reference to the relationship between the two entities (the user - the system, the software agent - a system, a service – a service, etc.). The trust level by definition includes the subjectivity of assessment resulting from the limited knowledge or limited analytical capabilities. In contrast, the security level is calculated assuming that the knowledge about the possible threats and the strength of the protection mechanisms applied is complete and reliable.

If in the process of assessing the level of system security, only available source of knowledge is incomplete and/or uncertain, applicable are usually two possible scenarios. In the first scenario, the security level is calculated assuming that the incompleteness of knowledge, or its uncertainty, is not affected seriously enough to assess the level of security. In the second scenario, at first trust level is determined, then the security level is calculated as the value of some function which is defined over the set of trust levels and which counterdomain is a set of security levels.

In the cases of the established security level of the system and on the basis of the unique requirements of the entities, each entity has its own trust level. For example, encryption with AES algorithm with encryption key of 128 bits is objectively less secure (lower security level) than encryption using the same algorithm and 256 bits key. However, for these two different entities, depending on the data to be protected (eg. personal data, project documents, administration, private correspondence, photographs of landscapes, etc.), the trust level related to 128 bits encryption key length may be the same as for the other entity and the encryption key of 256 bits.

The current methods for the security level and the trust level - suitable for monolithic systems - focus on:

- analysis of the current system configuration based on a fixed set of requirements and metrics, including the guidelines of the applicable standards (eg. ISO / IEC 15408, ISO / IEC 27000-series, PCI DSS)
- analysis of information about the system states changes, including security related events, fraud and anomaly detection.

Analysis of the current system configuration starts from defining a set of threats and a set of security countermeasures. Then, defined is mapping of the security countermeasures to

the set of the recognized threats. The final step in the process of the security level evaluation is to conduct a formal verification of the correctness of the implementation of methods used to protect the system.

The security level evaluation based on analysis of the system states changes uses this mapping technique, which is the current state of the system is one of the predefined security levels. The final quality of the methods for the security level evaluation is dependent on the quality of matching of the selected metric space elements to the specific system states being under the assessment.

So far, the methods used to assess the security level and trust level do not allow to consider such features of service-oriented systems like:

- dynamics of dependencies between the services - the dynamics of service-oriented systems due to the SOA design principles with a loose coupling between the services, which is a fundamental difference from the traditional, predefined methods of data exchange between the systems,
- heterogeneity of runtime environment - services may be provided by different suppliers, so the final level of security and trust level results from quite different security levels of infrastructure and development environment which are used to implement and maintain a service component,
- diversity of policies - the level of security and trust level of composite service is influenced not only by the hardware and software layers, but also depends from the high level security policy of individual service providers,
- missing or incomplete knowledge about the implementation details of services - services in SOA are defined only by their interface, all the other implementation details remain generally unknown to the service recipient.

A. Security Management in Service-Oriented Systems

Synthesis of the methods dedicated to solve the problems specifically related to the above security aspects of the service-oriented systems, enabled not only the knowledge integration about the evaluation of both the current security level and the emerging threats but it also provided some substansive solutions for protecting all the system layers. The method of security management proposed explores an agent-based architecture resulting with more precise evaluation of quality and security of services that so called classical approaches. The greatest advantage of it, is an ability to analyse both security level and the trust level in the systems-oriented services also in cases of missing or incomplete knowledge about the implementation details of the services.

Methods of modeling the trust level aimed at its analysis and evaluation in the service-oriented systems based on subjective logic gives rather subjective assessment results of the security. The subjectivity of trust assessment has been modeled by subjective logic opinions of autonomous software agents. These opinions can be processed and thus the trust level is evaluated by modeling the graph structure, the communication links in the system and the standard subjective logic operators.

B. Multi-Agent System for Security Level Evaluation

The research objective of this work is to develop a detailed architecture of multi-agent system for assessing security level based on some specific elements that are characteristic for the systems with service-oriented architecture (Figure 2).

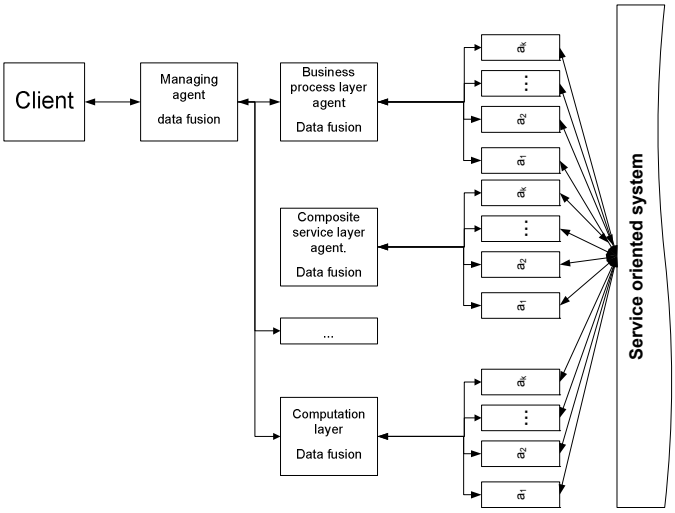

Fig. 2. Architecture of multi-agent system for evaluation of the security level in service oriented systems.

The main components of the developed architecture for service oriented systems security level evaluation are three sets of software agents. The agents at the lowest level of the architecture {a1, a2, ..., an} are responsible for data acquisition and for monitoring the execution of the services (eg. the time of the service completion, the amount of data sent and received by the service, etc.). Middleware agents {transport layer, communication protocols layer, ..., business processes layer} are responsible for aggregation and processing data sent by the agents from the lowest layer. As a result, we can assess the security level for a corresponding layer from the SOA reference model. At the highest level of the developed by us multi-agent architecture, we propose the managing agent who is responsible for providing information about the security level to the external systems working in cooperation with this one. Furthermore, this agent also provides a numerical value of the monitored system overall security level on the basis of information about each of the SOA layers security level. In addition to the architecture of multi-agent system, we propose an algorithm for the security level evaluation of the individual system layers in accordance with a multi-layered reference model for service-oriented systems. Moreover, a corresponding method for evaluation of the overall security level is proposed in [16]. The security level is represented in a form of opinions (ω) expressed in subjective logic, what is defined by three numerical values within the range [0,1] which are interpreted as a belief in the

security of the entity (belief), disbelief about the security and uncertainty (lack of knowledge) about the offered security level.

$$\omega = \langle \alpha,\beta,\gamma \rangle , \langle \alpha,\beta, \gamma \rangle \in [0,1]^3 , \alpha+\beta+\gamma=1 \quad (1)$$

The proposed approach is unique as far as it gives the advantage of formal and precise analysis of the service-oriented systems security level and also it allows to draw inferences about the changes in the security level of the composite services depending on the level of the component services security sublevels. The subjective logic, which is the basis for processing knowledge about the security levels, also it brings advantages coming from the integration of the knowledge from different resources. This type of reasoning about security level solves some conflicts arising from possible inconsistent opinions of the agents on the security level of the same entity. Contradictory information about the security level can also appear while processing data from independent information sources (e.g. software agents). Uncertainty about the value of the data acquired is an important aspect of the proposed method for assessing the security level of service-oriented systems because SOA environment usually we deals with a number of independent service providers and independent information sources about the security status that may be untrusted or imprecise [17].

Innovative features of our approach are: multi-agent system architecture for assessment of the service-oriented systems security level, the method for estimating security level in the system individual layers, the method for integration of the security level values from different agents and the method of estimating the security level of the composite services.

C. Security Analysis at Business Processes Level

We propose some methods for evaluation of the security level which considers characteristics of each SOA reference model layer [15]. One of our methods allows to evaluate the security level based on the data obtained from the lower layers (transportation, communication protocol in Figure 1) and high-level dependencies between the services, including those in the business processes layer. The data illustrating the low level characteristic of the SOA system may be reffered to a network traffic generated during communication between the services. The metadata which describe high-level dependencies define the existing links between the services – composite service structure (Figure 3).

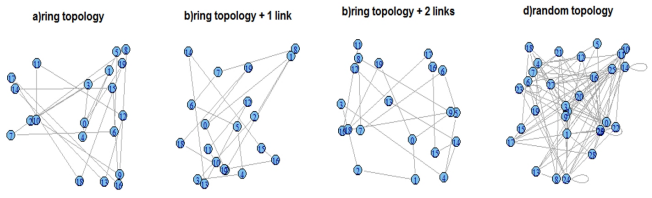

Fig. 3. Structure of the composite services. a) ring, b) ring + additional connection, c) ring + two additional connections, d) random connections.

We show that for a given composite service, there is a significant strong mutual correlation between the spatial data dependencies (incoming and outgoing data for individual service components). Also, we indicate that any disturbances in the business process or the implemention of the composite service, such as repeated calling of the selected service, disturbed sequence of the service execution, etc., singificantly impede the spatial autocorrelation parameter value (Figure 4).

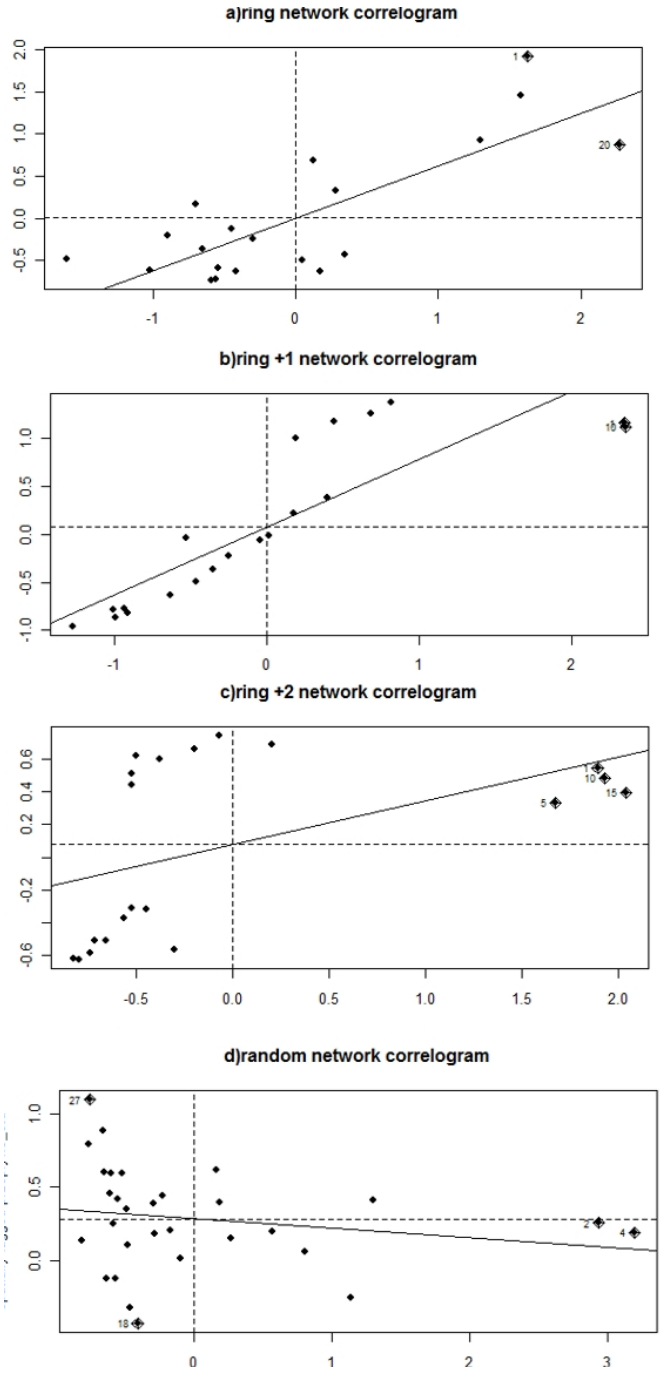

Fig. 4. Correlation of spatial data communication traffic generated for the four selected structures of complex service.

Our study highlights the importance of the measurement of spatial autocorrelation for the security level evaluation of the composite services in service-oriented systems. More generally, the spatial autocorrelation empowers the system to fraud detection by implementation of the business process logic [18].

Our original contribution to this work is development and experimental evaluation of the approach to estimation of the SOA systems security level. In order to evaluate the security level we apply statistical analysis of spatial data. In this approach we draw analogy between the services that implement a business process and any entities that have a fixed spatial structure with the specific values assigned to it, such as e.g. the distance between the selected pair of elements.

IV. Conclusions

Evaluation of the security level and the trust level in service-oriented systems require in addition to adaptation of the methods used for monolithic systems, the new methods which consider different characteristics of service-oriented systems. In particular, observed is a strong demand for the methods of analysis and identification of unexpected events, problem analysis of the traffic related to service execution and finalny the working standards for typical threats detection, such as an attack on the access to the peculiar service (called Denial of Service). These newly developed methods count on the specific nature of the risk and security requirements refered to different layers of the reference model for service-oriented systems.

These new solutions allow to carry out a comprehensive and critical evaluation of the security level and the trust level based on the information about the relations between the security events observed at a low level description of the system's state (eg. the traffic generated by the service) in relation to the events that represent high-level functions provided by the system (eg. the implementation of business processes).

References

[1] Benson, G. S., Akyildiz, I. F., & Appelbe, W. F. (1990). A formal protection model of security in centralized, parallel, and distributed systems. ACM Transactions on Computer Systems, 8(3), 183–213.

[2] Brotby, K. (2009). Information Security Governance.

[3] Chen, Y., Paxson, V., & Katz, R. H. (2010). What's New About Cloud Computing Security? University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010), 1–8.

[4] Chneider, D. (2012). The state of network security. Network Security, 2012(2), 14–20.

[5] Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719–731.

[6] Conti, M., Chong, S., Fdida, S., Jia, W., Karl, H., Lin, Y. D., … Zukerman, M. (2011). Research challenges towards the Future Internet. Computer Communications, 34(18), 2115–2134

[7] Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. Computers & Security, 28(3-4), 189–198.

[8] DRAFT Special Publication 800-160, Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems - sp800_160_draft.pdf. (n.d.). Retrieved November 6, 2015

[9] Foster, I., Kesselman, C., Tsudik, G., & Tuecke, S. (1998). A security architecture for computational grids. In Proceedings of the 5th ACM conference on Computer and communications security - CCS '98 (pp. 83–92). New York, New York, USA: ACM Press.

[10] Gambetta, D. (2000). Can We Trust Trust? In D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations (pp. 213–237). University of Oxford.

[11] Gasser, M. (1988). Building a secure computer system. Van Nostrand Reinhold Company New York, NY.

[12] Harmening, J. T. (2014). Managing Information Security. Managing Information Security. Elsevier.

[13] Harris, B., & Hunt, R. (1999). TCP/IP security threats and attack methods. Computer Communications, 22(10), 885–897.

[14] Introduction to Computer and Network Security. (2013). Network Security, 2013(11).

[15] Kolaczek, G. (2012). Spatial Analysis Based Method For Detection Of Data Traffic Problems In Computer Networks. In Uncertainty Modeling in Knowledge Engineering and Decision Making (pp. 919-924).

[16] Kołaczek, G. (2013). Multi-agent platform for security level evaluation of information and communication services. In Advanced Methods for Computational Collective Intelligence (pp. 107-116). Springer Berlin Heidelberg.

[17] Kołaczek, G., & Juszczyszyn, K. (2010). Smart security assessment of composed Web services. Cybernetics and Systems: An International Journal, 41(1), 46-61.

[18] Kołaczek, G., Juszczyszyn, K., Świątek, P., Grzech, A., Schauer, P., Stelmach, P., & Falas, Ł. (2015). Trust-based security-level evaluation method for dynamic service-oriented environments. Concurrency and Computation: Practice and Experience, 27(18), 5700-5718.

[19] Papazoglou, M. P., Traverso, P., Dustdar, S., & Leymann, F. (2007). Service-oriented computing: State of the art and research challenges. Computer, 40(11), 38–45.

[20] Pfitzmann, B., & Waidner, M. (1994). A general framework for formal notions of" secure" systems. In System, Hildesheimer Informatik-Berichte 11/94, Universitat.

[21] Pipkin, D. L. (2000). Information security: protecting the global enterprise.

[22] Rahman, N. H. A., & Choo, K.-K. R. (2014). A survey of information security incident handling in the cloud. Computers & Security, 49, 45–69.

[23] Security, S. O. A. (2008). SOA Security. Information Sciences.