Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2019, Volume 51, Number 2(192), Pages 321-334
DOI: 10.5604/01.3001.0013.2607

**Original article**

# Solving problems relating to ICT security management systems including various characteristics of the environment and system

**Dominika Dudziak-Gajowiak**[1]*, **Grzegorz Kolaczek**[2], **Krzysztof Juszczyszyn**[2]

[1] Faculty of Management,
General Tadeusz Kosciuszko Military University of Land Forces, Wroclaw, Poland,
e-mail: d.dudziak@wso.wroc.pl

[2] Department of Computer Science, Faculty of Computer Science and Management,
Wroclaw University of Technology, Poland,
e-mail: Grzegorz.Kolaczek@pwr.edu.pl; Krzysztof.Juszczyszyn@pwr.edu.pl

INFORMATIONS

**Article history:**

Submited: 14 January 2019

Accepted: 27 March 2019

Published: 17 June 2019

**ABSTRACT**

The work presents the essence of problems appearing in the ICT security management process in the context of systems characterized by significant dynamics of configuration and heterogeneity of resources both in the hardware and software layer. Basic differences in security management in systems with traditional centralized and monolithic architecture as well as in systems with service-oriented architecture have been presented. A layered reference model for service-oriented systems taking account of the basic goals of ICT security for dynamic information systems has been discussed. The basic assumptions of the multi-agent ICT security analysis system in service-oriented systems as well as the results of the safety analysis, including the correlation between events observed in low and high layers of the reference model have been discussed.

**KEYWORDS**

ICT security, threat detection, service-oriented systems, security level

* Corresponding author

## Introduction

The possibility of ensuring security is one of the basic non-functional requirements for IT systems. While security issues were marginalized in the early phase of IT systems development [1], with the increasing availability and widespread use of IT systems, security issues have become a key element for the possibility of further development [2; 3]. Moving from monolithic architectures and centralized systems to distributed and service-oriented systems means that the available methods of guaranteeing and assessing safety are not sufficient and must be supplemented with elements that include, among others, high level of heterogeneity of resources, diverse granularity of resources along with high dynamics of the variability of resources in the IT system [4].

In service-oriented systems, there are security problems that cannot be solved by simply transferring patterns and solutions applicable to systems with other architects (e.g., centralized, monolithic systems). In particular, there is no possibility of simple transfer of previously used methods to analyze and guarantee security in environments with high levels of heterogeneity, intensive and different communication, diversified tasks and resources, as well as high dynamics of resource variability [5]. An example illustrating the specificity of problems in service-oriented systems may be a situation involving a data protection task. In monolithic systems, the separation of resources is naturally ensured, since the data processed by the system remain within it, and access to them is associated with the need to have appropriate rights granted in the context of this system and specific resources. Consequently, in order to protect confidentiality and data integrity, a monolithic system should be adequately suited to ensure access control. In a service-oriented system, where data processing is performed e.g., in the "Software as a Service" (SaaS) model, despite the provision of reliable access control mechanisms, data can be disclosed or modified in an unauthorized way, for example as a result of errors in the mechanisms ensuring the separation of resources, when the data is stored in a shared location also by other services [6].

## 1. IT security

The concept of IT (computer) security is defined as the condition of a system in which protection of elements of technical infrastructure, software and data processed, collected and transmitted by the system is guaranteed [5; 7; 8]. Given the fact that data is a key element in every system, also in the context of security research, the issues dedicated to data security representing information processed in the system (data and information security) play a special role.

The aim of research in the field of data security is to provide methods and solutions that enable the implementation of mechanisms to protect against unauthorized access, disclosure, destruction, use and modification of data [9]. The increase in the role of communication between systems, which often determines the possibility of achieving the desired functionality by the system, has made the importance of mainstream work aimed at seeking solutions to problems related to remote access to the system and distributed data processing. Research problems dedicated to communication issues belong to the field of network security [10]. Important research issues in the field of network security include: policy and access management to system resources, monitoring access to system resources, preventing, detecting and responding to abuse related to unauthorized access, and modification and use of system resources [12].

### 1.1. Problems with IT security management

The specificity of IT security problems arises from the diversity of architectures of IT systems. Security problems relating to centralized systems, in which data processing is carried out in a distinguished central node, are a subset of problems that arise in the case of distributed architecture systems. Centralized systems enable easier control of the processing and access to resources, since the central point of the system, which is the main element subject to protection and monitoring, is naturally distinguished in them. Distributed systems allow the possibility of processing and storing data in various places of the system, often also those that are geographically distant. Such specificity of distributed systems is associated with the need to simultaneously ensure security in various places, taking into account the diversity of the local specificity of system components, including the diversified computing power, diversified level of interaction with system users, various requirements resulting from a locally applicable legal system, etc. For distributed systems, the critical factor is also the need to ensure secure communication between all system components. The complexity of the process of selecting adequate security management methods and mechanisms for an IT system, considering the full scope of its specificity, increases with the number and diversity of elements subject to protection [12].

Another feature of the IT system architecture that affects the complexity of the assurance and estimation of ICT security is the heterogeneity of the solutions used. Modern information systems take advantage of a variety of solutions both in the layer of physical system resources and in the software layer. This means that it is necessary to include in the security management both the specificity of a given element of the system (e.g., availability of hardware for memory access control mechanisms, detection capabilities of critical – in relation to security – programming errors, etc.) as well as guaranteeing the possibility of safe interaction between system components with different hardware and program specificity [13].

A similar increase in the complexity of the security management process causes the transition from systems with monolithic architecture to systems with service-oriented architecture (SOA).

Systems with a service-oriented architecture are constructed using services that provide user-defined functionality. A service is described as a software element that can operate independently of others and has a defined interface through which it provides the functions implemented [14]. The SOA is an architecture for creating dynamic connections of service interfaces, implementation of their functionality and execution of calls to their operations. The SOA is primarily associated with such nonfunctional characteristics as the reuse of software components, encapsulation of functionality, precise definition of interfaces and flexibility of applications created by means of composition. The life cycle of SOA applications includes four phases: modeling, composition, startup, and management. These phases concern all applications built in accordance with the SOA paradigm and are characterized by a varied level of complexity and specific problems, including those in the field of IT security. The reference model for service-oriented systems defines five layers dedicated to the basic functions of the system, starting from the low-level functions related to providing communication capabilities with services, and ending with the description of high-level dependencies between services resulting from business processes supported by the system (Fig. 1).

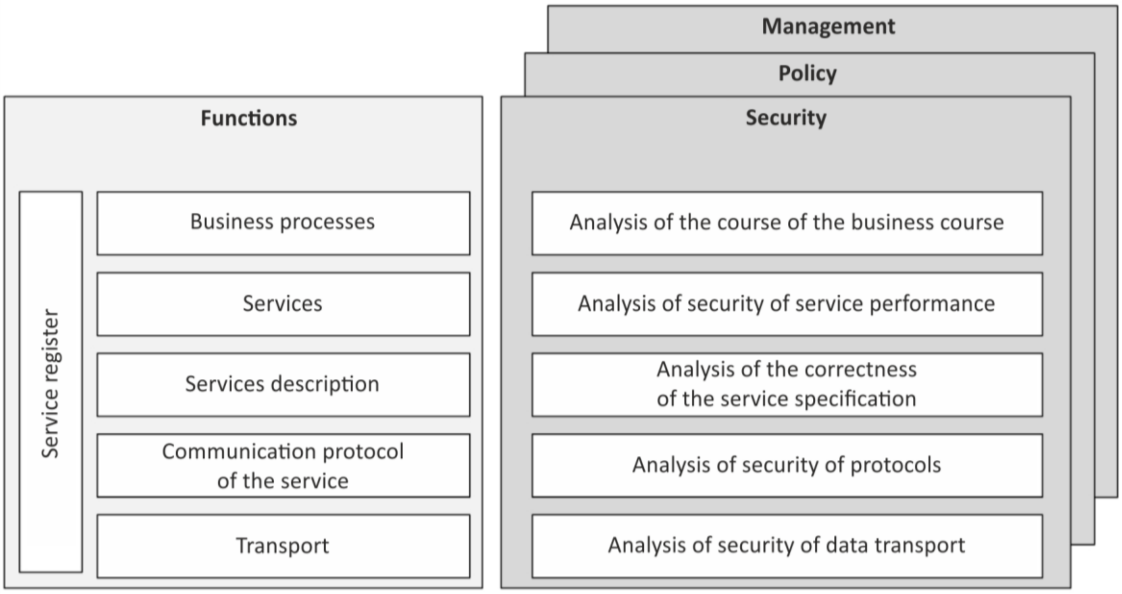
Management
Policy
Functions
Security
Service register
Business processes
Services
Services description
Communication protocol of the service
Transport
Analysis of the course of the business course
Analysis of security of service performance
Analysis of the correctness of the service specification
Analysis of security of protocols
Analysis of security of data transport

**Fig. 1.** A layered reference model for service-oriented systems.
*Source: Own elaboration.*

### 1.2. Security management in dynamic environments of service-oriented systems

The complexity of security issues in service-oriented systems results from the fact that in this type of systems there are simultaneously problems characteristic for distributed and heterogeneous systems, as well as specific security problems related to modeling, composition, startup and service management processes. The process of providing and assessing security for service-oriented systems requires consideration of the specificity associated with the elements distinguished in the reference model (Fig. 1). The following issues have a significant impact on the security management process in service-oriented systems [15]:

– identity management – a service can be run in different contexts by different users; the service should be carried out each time with a set of rights appropriate for a given execution context (security of business processes),
– proper security controls management – it is necessary to provide appropriate security management mechanisms both at the level of a single service and for complex services (security of services),
– security management sovereignty – it is necessary to guarantee security management mechanisms independent of the used hardware and programming technologies (safety of service description),
– seamless connection to other organizations on a real-time basis – services can be provided by various service providers; when the final functionality supplied to the user is provided using resources (services) from different service providers, this fact should not be noticeable to the user (security of the communication protocols of the services),
– protection of data in transit and at rest – performance of complex services may involve the necessity of data flow through systems managed by various entities

and using various security mechanisms; irrespective of the place where the data is processed and by which systems are transferred, it should be possible to pre-select data security management (transport safety).

The following characteristics of systems with service-oriented architecture influence the possibility of providing adequate solutions for the assessment of the level of security and the level of trust:

- high level of heterogeneity (both in the hardware and software layer),
- scattering of resources,
- intensity and diversity of communication,
- varied granurality of tasks and resources,
- sharing resources,
- competing for access to resources,
- dynamics of resource volatility,
- high-level requirements resulting directly from the specifics of realized business processes.

## 2. Estimation of the security and trust levels as a significant element of ICT security management

The ability to determine the level of security is important in the entire safety management process, and thus it is also essential at every stage of the system life cycle, from the design phase, through dimensioning, introduction, implementation, to the operation of a ready IT product. When designing a system, it is necessary to identify the user's requirements as to the expected level of security, then these requirements must be met by the appropriate selection and implementation of protection methods. During the operation of the system, however, it is necessary to constantly monitor the current level of security in order to enable the user to take a quick response in the event of a security incident.

The possibility to assess the level of trust in service-oriented systems is as important as the possibility to estimate the level of trust. In service-oriented systems, a special role for security is played by events not only related to the direct interaction between the user and the system, but the interactions between services are equally important. Therefore, only the determination of the level of trust between the services and system users makes it possible to control access to system resources in a manner that minimizes the risk of fraud. In addition, in service-oriented systems, where services are provided by many service providers, and service implementation details are not available to other services and system users, we are dealing with drawing conclusions concerning security using incomplete and often uncertain knowledge. In such situations, the assessment of the level of trust becomes the basic possibility of managing security in the IT system. The level of trust gives the opportunity to represent a subjective belief about the level of security, and the value of the level of trust can be estimated using uncertain and incomplete data about the state of the system. The level of security and the level of trust of the IT system are important elements in the process of IT security management [16].

The level of information system security is the value of a metric defined as part of the adopted metric space of security. The set of elements for the metric space of the IT system security is defined by the system states defined in the context of detailed security requirements.

In the process of managing the security of the IT system, two separate tasks are distinguished: the first one related to ensuring the required level of security and the other one – to assessing the existing level of security.

The task of ensuring the required level of security of the IT system or its part consists in limiting the probability that the identified risk factors will lower the level of system security below the assumed value. The task of ensuring the required level of security is decomposed to subtasks dedicated to the protection process of stored, processed and transmitted by the system data by providing integrity, confidentiality and accessibility [18].

The task of assessing the level of security allows for the estimation of the current value of the risk associated with the possibility of loss of integrity, confidentiality or access to resources, despite the methods of protection used.

The level of trust is understood as the abstract size representing the value of trust, which is reflected in the belief of the subject that the information system will operate in accordance with the applicable assumptions [19]. The subject may be a certain autonomous software component or a system user. The level of trust in the context of IT security analysis has been introduced to enable automation of decision-making processes related to security, e.g., in the tasks regarding access control or rights management. The task of estimating the level of trust consists in defining a trust function defined on a set of assessed system elements (trustee) with values in the set of trust levels.

The level of trust enables a formal representation of the subjective conviction of the entities about the level of security of the part or the entire system. The level of trust differs from the level of security since it is defined for the relationship between two entities (user–system, program agent–service, system–system, etc.) and is, by definition, to consider a certain level of subjectivity of the assessment, resulting from the limited knowledge or limited analytical capabilities. Whereas the level of security is calculated assuming that the assessor's knowledge about possible threats and the protection mechanisms used in the system is complete and reliable.

If only sources of incomplete and/or uncertain knowledge are at disposal during the process of assessing the level of IT system security, two scenarios are acceptable. In the first scenario, the level of security is calculated assuming that the incompleteness of knowledge or its uncertainty does not significantly affect the assessment of the level of security. In the second scenario, confidence levels are first determined, and then the level of security is calculated as the value of a function the domain of which comprises the set of values of trust levels, and the counter-domain constitutes a set of security levels.

Situations in which the level of system security is known and on this basis entities calculate their own levels of trust in relation to the system are also considered. For example, ensuring confidentiality by encrypting data with the AES algorithm with the 128 bit – long key is objectively less secure (the lower security level) than encryption using the same algorithm and key with the length of 256 bits. However, for two different entities, depending on the data they want to protect (e.g., personal data, project documents, applications, private correspondence, landscape photos, etc.), the value of the level of trust in the encryption method with the 128 bit – long key may differ.

The currently used methods for estimating the level of security and the level of trust – appropriate for monolithic information systems – focus on:

- the analysis of the current system configuration using a set of requirements and metrics, including the use of guidelines from applicable standards (e.g., ISO/IEC 15408, ISO/IEC 27000-series, PCI DSS),
- the analysis of information about system state changes, including the use of methods for detecting fraud and identification of atypical states.

The analysis of the current system configuration starts with defining the set of threats and the set of security measures. Next, the mapping of elements of the set of securities to the identified elements from the set of threats is defined. The final stage of the process of assessing the level of security is to perform a formal verification of the correctness of the implementation of security methods in the system.

Estimating the level of security using the description of system state changes employs techniques that map the current state of the system to one of the distinguished security levels. The quality of a given method for estimating the level of security depends in this case on the degree of matching the selected metric space to the specifics of the system under evaluation.

The methods applied to date for assessing the level of security and the level of trust do not allow taking into account such features of service-oriented systems as:

- dynamics of links between services – the dynamics of service-oriented systems results from the SOA project assumption of a loose connection between services, which is a fundamental difference to the traditional, predetermined methods of data exchange between IT systems,
- heterogeneity of the runtime environment – services can be provided by different providers, so the final level of security and the level of trust is influenced by the varied level of security of the infrastructure as well as the programming environment responsible for the implementation of all component services,
- diversity of service provider policies – the level of security and the level of trust of complex service is affected not only by the hardware and software layer of the runtime, but also by the high-level security policy of individual service providers,
- the lack or incompleteness of knowledge regarding the implementation details of services – services in the SOA architecture are defined only by their interface, all implementation details are usually unknown to the recipient of the service.

## 2.1. Security management in dynamic environments of service-oriented systems

The synthesis of solutions dedicated to individual aspects of the problem of security of service-oriented systems enabled the integration of knowledge regarding the assessment of the current level of security and emerging threats for all layers of the system. The proposed method of integration of knowledge about security uses the proprietary architecture of the agent system for the evaluation of quality and safety of services, with individual layers of the reference model taken into consideration. The proposed approach makes it possible to analyze the level of security and the level of trust in service-oriented systems also in cases of the lack or incompleteness of knowledge regarding the implementation details of services.

For the purpose of analyzing and estimating the level of trust in service-oriented systems as an element of the subjective safety assessment, a method of trust modeling with the use of subjective logic has been developed. The aspect of the subjective assessment of the security level has been used in the proposed agent system architecture, for which the method of estimating the level of trust has been presented, including the knowledge of the position of the selected agent in the graph structure representing the current communication links in the system and the level of trust of other agents towards the selected one.

## 2.2. The multi-agent system for assessing the security of dynamic IT systems

The aim of the work was to develop a detailed architecture of the multi-agent system that allows for the assessment of the level of security including elements specific to systems with service-oriented architecture (Fig. 2).

Three sets of program agents are elements of the developed system for assessing the level of security. The lowest level agents $\{a_1, a_2, ..., a_n\}$ are responsible for the acquisition of data from monitoring the execution of services (e.g., service delivery time, the number of data sent and received by the service, etc.). Intermediate agents {transport layer agent, communication protocol layer agent, ..., business process layer agent} are dedicated to aggregation and data processing tasks sent by the lowest layer agents, and the result of processing the obtained data is the safety level assessment for a given reference model layer for systems with a service-oriented architecture. The managing agent that is responsible for providing information about the security level to external systems is at the highest level of the proposed architecture. The managing agent also calculates the total security level of the monitored system based on information on the level of security for individual layers. In addition to the multi-agent system architecture, an algorithm for assessing the level of security for individual system layers that complies with the layered reference model for service-oriented systems and the method for estimating the resulting safety level, including all system layers have been proposed [19]. The level of security of the constituent elements is represented in the form of subjective logic $\omega$, which is expressed by three values in the range [0-1] and which are interpreted as a belief about the security of the examined element, a disbelief about the security, uncertainty (lack of knowledge) as to the security offered by a given element.

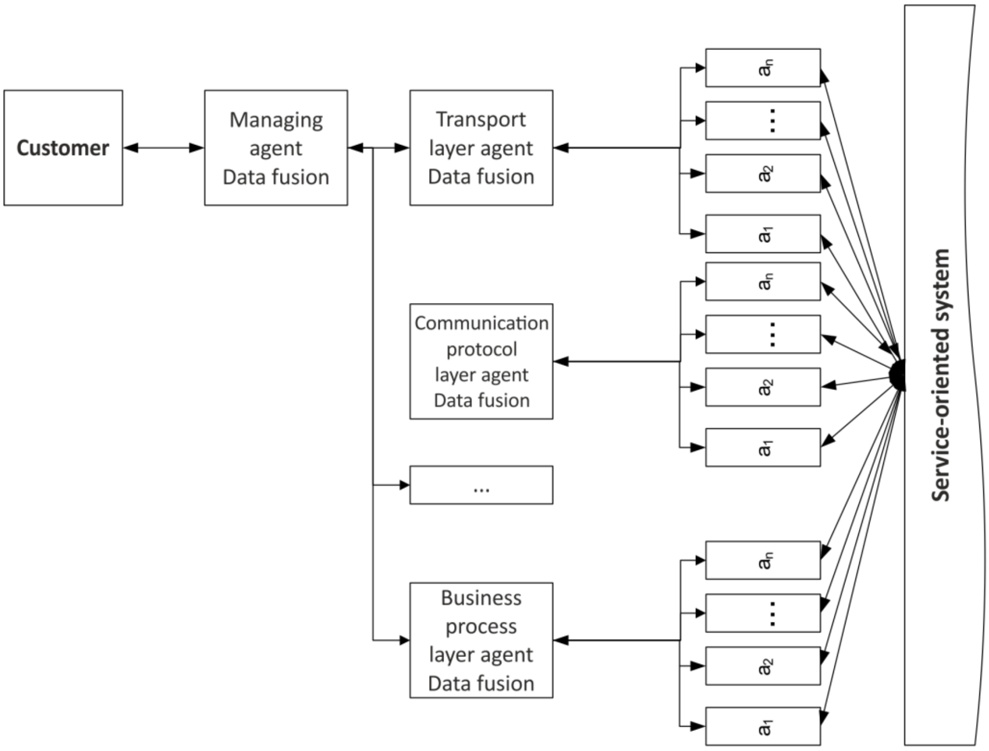
Customer
Managing agent Data fusion
Transport layer agent Data fusion
Communication protocol layer agent Data fusion
...
Business process layer agent Data fusion
$a_n$
$a_2$
$a_1$
Service-oriented system

**Fig. 2.** The architecture of a multi-agent system for estimating the level of security
*Source: Own elaboration.*

$$\omega = \langle b,d,u \rangle ,\ \langle b,d,\ u \rangle \in [0,1]^3 ,\ b+d+u =1 \tag{1}$$

The proposed approach is unique in that it offers the possibility of a formal and precise analysis of the security level of service-oriented systems and enables applying for changes in the level of security of a complex service depending on the level of security of component services. Subjective logic, which has been used as the basis for the processing of knowledge about the level of security, gives an advantage to the proposed approach through the possibility of integrating knowledge from different sources, including removing any contradictions in opinions on the level of security. Conflicting information about the level of security may occur when using data from independent sources of information, which may be agent programs for the system monitoring. The element regarding uncertainty as to the value of the data obtained is an important aspect of the proposed method of assessing the level of security in the context of service-oriented systems, where numerous independent service providers and independent sources of information on the security status used in the service composition process are dealt with [20].

The proprietary elements of the proposed solution include the architecture of a multi-agent security evaluation system for service-oriented systems, a method of estimating the level of security for individual system layers, a method of integration of security level assessments from different agents, and a method of estimating the level of security of complex services.

### 2.3. Research on security threats in the implementation of business processes

Methods for estimating the security level of service-oriented systems, taking into account the specificity of individual layers, have been developed for the proposed architecture [21]. One of the developed methods allows estimating the level of security including data obtained from lower layers (transport, service communication protocol – Figure 1) of a layered reference model for service-oriented IT systems along with high-level dependencies between services, including dependencies defined in the layer business processes of the afore-mentioned model. Low level data concern the measurement of ICT traffic related to communication between services. Data regarding the high level of system description concern the definition of existing links between services – the structure of a complex service (Fig. 3).

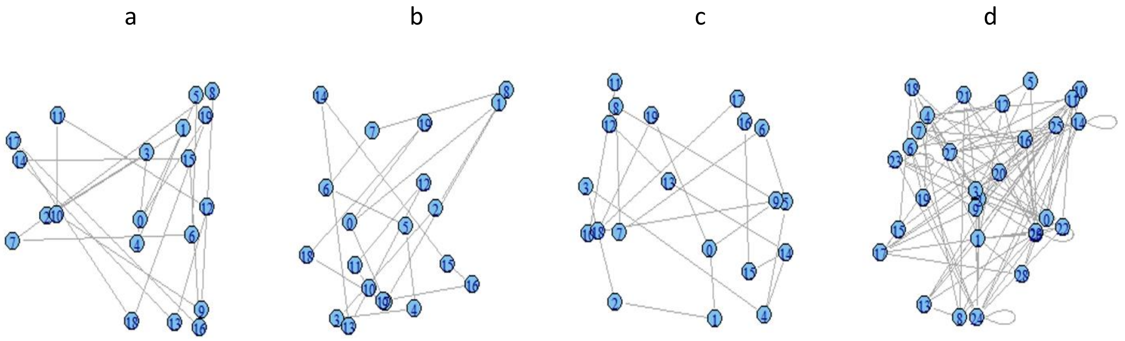

**Fig. 3.** The structure of the examined complex services: a) ring; b) ring + additional connection; c) ring + two additional connections; d) random connections

*Source: Own elaboration.*

It has been shown that for a given complex service there is a significant spatial correlation between data streams entering and leaving individual component services. It has also been demonstrated that any disruption to the business process and the complex service implementing this process, consisting in a repeated call of the selected service or a disturbance of the service execution sequence, gives significant changes in the value of the spatial autocorrelation parameter (Fig. 4).

In consequence, the conducted research has shown that the measurement of spatial autocorrelation may constitute an important element of the system for estimating the security level of services in information systems with service-oriented architecture, and more generally, spatial autocorrelation gives the opportunity to detect fraud in the implementation of the business process logic [22].

The new results obtained from the conducted study include the development and experimental evaluation of the method for estimating the level of security of the IT system. Moreover, the utilization of statistical spatial data analysis to estimate the level of security is also a new feature. In the developed approach, the analogy was used between services implementing the business process and any entities having a fixed spatial structure with specific values describing it, such as the distance between a selected pair of elements.

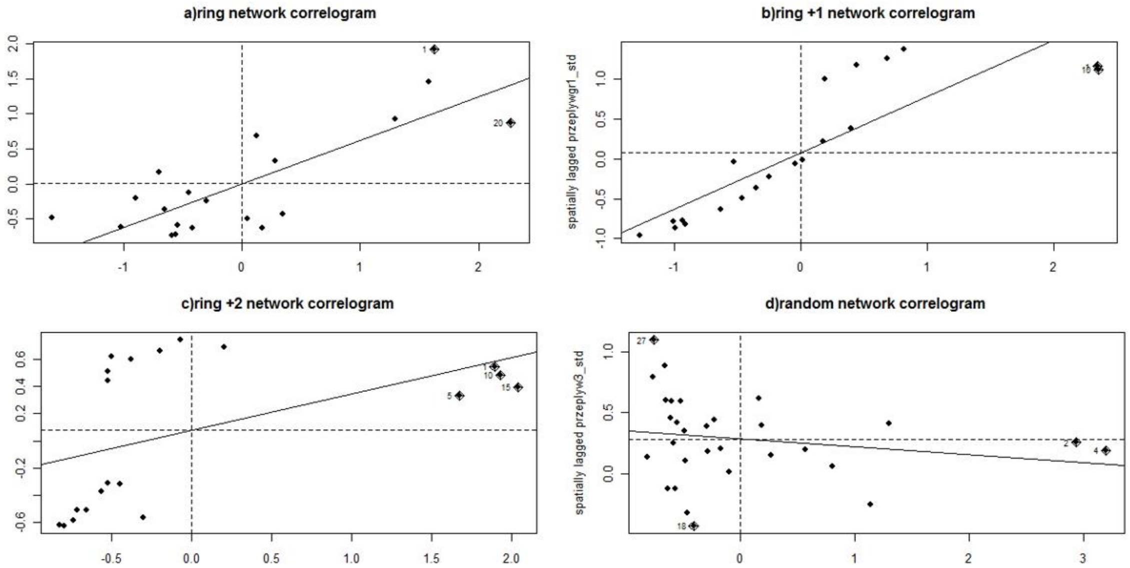

**Fig. 4.** Spatial correlation of the generated ICT traffic for four selected complex service structures

*Source: Own elaboration.*

## Conclusions

Estimating the level of security and the level of trust for service-oriented systems required the adaptation of the methods used for monolithic information systems, and the development of new methods taking into account the different nature of service-oriented systems. Particularly methods of analyzing and identifying atypical states, methods of threat analysis in ICT traffic, as well as methods of defining patterns for typical threats, such as, for example, an attack on the availability of a service (Denial of Service) were used. It was also necessary to develop a range of new methods, including the specific nature of threats and security requirements (distinguished in different layers) of the reference model of service-oriented systems.

The new solutions developed allow for carrying out the assessment of the level of security and the level of trust, using information about the connections between events observed at a low level of system state description (e.g., traffic generated by the service) and events representing high-level functions delivered by the system (e.g., business processes).

### Acknowledgement

No acknowledgement and potential founding was reported by the authors.

### Conflict of interests

The authors declared no conflict of interests.

### Author contributions

All authors contributed to the interpretation of results and writing of the paper. All authors read and approved the final manuscript.

### Ethical statement

The research complies with all national and international ethical requirements.

### ORCID

Dominika Dudziak-Gajowiak https://orcid.org/0000-0001-6898-7241

Grzegorz Kolaczek https://orcid.org/0000-0001-7125-0988

Krzysztof Juszczyszyn https://orcid.org/0000-0002-9326-6734

## References

1. Harris B, Hunt R. *TCP/IP security threats and attack methods*. Computer Communications. 1999;22(10):885-97.
2. Dlamini MT, Eloff JHP, Eloff MM. *Information security: The moving target*. Computers & Security. 2009;28(3-4):189-98.
3. 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.
4. Conti M, Chong S, Fdida S, et al. *Research challenges towards the Future Internet*. Computer Communications. 2011;34(18):2115-34.
5. Chen Y, Paxson V, Katz RH. *What's New About Cloud Computing Security?* University of California, Berkeley Report No. UCB/EECS-2010-5 January. 2010;20(2010):1-8.
6. Rahman NHA, Choo K-KR. *A survey of information security incident handling in the cloud*. Computers & Security. 2014;49:45-69.
7. Gasser M. *Building a secure computer system*. New York: Van Nostrand Reinhold Company New York; 1988.
8. Pfitzmann B, Waidner M. *A general framework for formal notions of "secure" systems*. Hildesheim: Universität Hildesheim, Institut für Informatik; 1994.
9. Harmening JT. *Security Management Systems*. In: Vacca J (ed.). *Managing Information Security*. Waltham: Elsevier; 2014:47-55.
10. *Introduction to Computer and Network Security*. Network Security. 2013;11.
11. Chneider D. *The state of network security*. Network Security. 2012;2:14-20.
12. Benson GS, Akyildiz IF, Appelbe WF. *A formal protection model of security in centralized, parallel, and distributed systems*. ACM Transactions on Computer Systems. 1990;8(3):183-213.
13. Foster I, Kesselman C, Tsudik G, Tuecke S. *A security architecture for computational grids*. In: *Proceedings of the 5th ACM conference on Computer and communications security – CCS '98*. New York: ACM Press; 1998:83-92.
14. Papazoglou MP, Traverso P, Dustdar S, Leymann F. *Service-oriented computing: State of the art and research challenges*. Computer. 2007;40(11):38-45.
15. *Security, S.O.A*. SOA Security. Information Sciences. 2008.
16. Brotby K. *Information Security Governance*. John Wiley & Sons; 2009.
17. Pipkin DL. *Information security: protecting the global enterprise*. Upper Saddle River, NJ: Prentice Hall PTR; London: Prentice-Hall International; 2000.
18. Gambetta D. *Can We Trust Trust?* In: Gambetta D (ed.). *Trust: Making and Breaking Cooperative Relations*. Oxford: University of Oxford; 2000:213-37.

19. Kolaczek G. *Multi-agent platform for security level evaluation of information and communication services*. In: Nguyen NT, Trawinski B, Katarzyniak R, Jo G-S (eds.). *Advanced Methods for Computational Collective Intelligence*. Berlin, Heidelberg: Springer; 2013:107-16.
20. Kolaczek G, Juszczyszyn K. *Smart security assessment of composed Web services*. Cybernetics and Systems: An International Journal. 2010;41(1):46-61.
21. Kolaczek G. *Spatial Analysis Based Method For Detection Of Data Traffic Problems In Computer Networks*. Uncertainty Modeling in Knowledge Engineering and Decision Making. 2012:919-24. https://doi.org/10.1142/9789814417747_0147.
22. Kolaczek G, Juszczyszyn K, Swiatek P, et al. *Trust-based security-level evaluation method for dynamic service-oriented environments*. Concurrency and Computation: Practice and Experience. 2015;27(18):5700-5718.

## Biographical notes

**Dominika Dudziak-Gajowiak** – M.Sc., graduate of the Faculty of Computer Science and Management at the Wroclaw University of Technology (specialization: Computer Science), employee of the Faculty of Management of the General Tadeusz Kosciuszko Military University of Land Forces in Wroclaw since 2014, member of the Polish Information Processing Society since 2010, for over ten years she has been dealing with the practical aspects of the security of IT systems and networks. Author or co-author of publications in the field of IT systems and networks as well as risk management.

**Grzegorz Kolaczek** – Dr. hab. Eng., graduate of the Faculty of Electronics at the Wroclaw University of Technology, in 1998 he graduated from the Reserve Cadet Officer School at the Armaments and Electronics Training Center in Olsztyn; research and teaching worker at the Wroclaw University of Technology since 1997, and has been conducting research in the field of security of IT systems and networks for over twenty years. The main subject of the undertaken research is the analysis and modeling of selected ICT security indicators, particularly the level of security and the level of trust in contemporary IT systems characterized by the variability of the execution environment and the significant role of communication between elements of the distributed processing and data storage environment. Author of over 90 publications in conference materials, magazines and chapters in books, reviewer of articles in several international journals, participant and head of research tasks in four projects financed from the Operational Program Innovative Economy, expert of the National Center for Research and Development, the Lower Silesian Marshal's Office and the Project Center *Digital Poland*.

**Krzysztof Juszczyszyn** – Dr. hab. Eng., graduate of the Faculty of Electronics at the Wroclaw University of Technology, research and teaching worker at the Wroclaw University of Technology since 1997, for over twenty years he has been conducting research in the field of dynamics and prediction of the behavior of complex network systems and the security and performance of complex service systems. He is the author of over 130 publications in international conference materials, magazines and chapters in books, article reviewer and editor of special editions in over a dozen international journals. Participant of 9 national and international research projects (as a contractor, tasks and projects manager), financed from funds such as Operational Program Innovative Economy. Expert, reviewer of project applications and auditor of projects funded by the European Commission, the Ministry of Science and Higher Education, the Slovak Academy of Sciences, the National Center for Research and Development and the Lower Silesian Marshal's Office.

## Rozwiązywanie problemów z zarządzaniem bezpieczeństwem systemów teleinformatycznych z uwzględnieniem zmiennej charakterystyki środowiska i systemu

**STRESZCZENIE** W pracy została zaprezentowana istota problemów pojawiających się w procesie zarządzania bezpieczeństwem teleinformatycznym w kontekście systemów charakteryzujących się znaczącą dynamiką konfiguracji oraz heterogenicznością zasobów zarówno w warstwie sprzętowej, jak i programowej. Przedstawiono podstawowe różnice w zarządzaniu bezpieczeństwem w systemach o tradycyjnej scentralizowanej i monolitycznej architekturze oraz w systemach o architekturze zorientowanej na usługi. Przedstawiono warstwowy model odniesienia dla systemów zorientowanych na usługi, z uwzględnieniem którego zdefiniowane zostały podstawowe cele bezpieczeństwa teleinformatycznego dla dynamicznych systemów informatycznych. Omówiono podstawowe założenia wieloagentowego systemu analizy bezpieczeństwa teleinformatycznego w systemach zorientowanych na usługi oraz przedstawiono wyniki analizy bezpieczeństwa z uwzględnieniem korelacji pomiędzy zdarzeniami obserwowanymi w niskich i w wysokich warstwach modelu odniesienia.

**SŁOWA KLUCZOWE** bezpieczeństwo teleinformatyczne, wykrywanie zagrożeń, systemy zorientowane na usługi, poziom bezpieczeństwa

### How to cite this paper

Dudziak-Gajowiak D, Kolaczek G, Juszczyszyn K. *Solving problems relating to ICT security management systems including various characteristics of the environment and system*. Scientific Journal of the Military University of Land Forces. 2019;51;2(192):321-34.

DOI: http://dx.doi.org/10.5604/01.3001.0013.2607