Modelling compliance threats and security analysis of cross border health data exchange

Mike Surridge✉ [0000-0003-1485-7024], Ken Meacham, Juri Papay, Stephen C. Phillips[0000-0002-7901-0839], J. Brian Pickering[0000-0002-6815-2938], Ardavan Shafiee, Toby Wilkinson[0000-0002-2621-5400]

University of Southampton IT Innovation Centre, Southampton, UK
{ms,kem,jp,scp,jbp,ash,stw}@it-innovation.soton.ac.uk

Abstract. Digital health data is created, stored and processed in healthcare IT infrastructures. These infrastructures are the target of large-scale cyber-attacks and are found to be vulnerable, primarily for two main reasons: the heterogeneity of infrastructure and the numerous stakeholders (medical staff, managers, patients, regulators etc.). Furthermore, the stakeholders have different attitudes, skills, awareness and data handling practices that offer many opportunities for malicious activities. Healthcare in general is characterised by a multitude of regulations and adherence to them is essential to the functioning of the system. Compliance management is usually described in terms of risks and involves activities such as risk identification, assessment and treatment. Our paper conceptualises the notion of a "compliance threat" and discusses the security of cross-border health data exchange. The paper presents the architecture of the System Security Modeller and illustrates the security risk assessment of the "break glass" scenario which requires health data communication in an emergency situation.

Keywords: health data, compliance, GDPR, security, modelling

1 Introduction

Businesses and organisations have to operate in an environment with ever increasing numbers of regulations. Compliance management assumes adherence to regulations and standards and can be described by activities such as risk identification, risk assessment and treatment. The regulations are not static: government and industrial bodies tend to make changes. This, along with frequent changes to a business and its infrastructure, results in a need for regular compliance audits. Achieving full compliance with all regulations may even be impossible, especially considering that the requirements can be conflicting and also involve stakeholders with different interests.

In this environment it is becoming difficult for organisations to identify, prioritise and respond to regulatory demands that impact their business. Non-compliance may result not only in financial penalties but can threaten the functioning and the very existence of the business. As the number and complexity of regulations increases, the

cost of demonstrating compliance also grows. Therefore, automating compliance checking could help reduce cost, avoid duplication and allow companies to react quickly to the deficiencies identified by auditing.

The paper introduces a methodology for modelling compliance in the context of threat analysis. It presents the System Security Modeller (SSM) tool which allows automated identification of end-to-end security risks and compliance issues during system design. It also calculates the impact of non-compliance for the overall system architecture. The application of the SSM is illustrated on a use case scenario involving the exchange of medical records across national boundaries within the EU.

Section 2 provides a short survey of related work. Section 3 introduces the architecture of System Security Modeler, which can be used for security threat analysis and compliance assessment. Section 4 describes non-compliance as a threat and provides examples. Section 5 describes the "break glass" scenario illustrating the security aspects of health data exchange across national boundaries. Section 6 summarises the paper.

2 Related Work

2.1 Compliance management

Compliance management is a risk-based optimisation problem aiming to reduce the cost of audits, and the identification and resolution of non-compliance issues. The approach uses dynamic programming to find the balance between the need to satisfy the multitude of regulatory requirements and the available resources [1].

The CORAS framework is based on the ISO 31000 [2] standard and incorporates the method, formal compliance specification language and risk analysis tool [3]. The CORAS language contains elements such as assets, threats, risks and controls. The compliance risks are calculated based on the probability of occurrence and the consequence of incidents. The CORAS methodology was applied in various domains for example, oil and gas exploration [4,5] and for the analysis of legal documents [6].

Finding a suitable graphical representation can significantly reduce the complexity of compliance management. This allows change of regulations to be monitored as well as the status of compliance within an organisation [7].

For compliance modelling it is important to identify the stakeholders who need to take actions to ensure that the system is compliant with the regulations. This assumes the existence of trust-relations and the distribution of work between stakeholders who manage compliance risks [8].

Document and model-based approaches to compliance management were compared in [9] according to the effort required for modelling, interpreting, documenting and monitoring the status of compliance. The paper presented a model of a hospital using three different notations: User Requirements Notation (URN), Goal-oriented Requirement Language (GRL) and Use Case Maps (UCM). These notations provided the means to capture the goals, assets, actors and tasks required for achieving data privacy compliance. The paper concludes that using a mixture of document and model-based approaches offers the best trade-off.

One of the issues is understanding legal documents and translating them into models and policies that can be followed by an organisation in order to achieve compliance. Breaux *et al.* suggested to use Semantic Parametrisation to help with the disambiguation of documents for extracting the rights and obligations of stakeholders that impact their privacy and security requirements [10].

The objectives, processes and policies required for building a compliance management system are described in the ISO 19600 standard [11]. Understanding the operation of an organisation is one of the key elements of this standard. This involves analysing all compliance obligations and the possible risks. The standard also outlines the role and responsibilities of stakeholders in planning, implementation and operation of processes that ensure an organisation's compliance with the regulations [12].

Recently several GRC (Governance Risk Compliance) platforms have been developed that allow adherence to standards and regulations to be tracked [13,14]. Although businesses are aware of the importance of GRC, in practice this task is often handled by different units which use different methods and tools. As a result, the information about compliance is scattered in separate spreadsheets, text documents and even emails which makes auditing difficult. The main purpose of GRC platforms is to automate business processes, to integrate the information produced by different units and provide a real time picture about the GRC status.

2.2 Threat Modelling

Over the years numerous methods have been developed for identifying and analysing threats in ICT systems. In threat modelling we can distinguish four stages, these are: system design, threat identification, threat addressing, and validation [15]. Threat modelling and analysis tools in general terms can be classified as: asset, attacker and software centric tools.

Software centric tools, for example VsRisk [16], Threat Modeling Tool [17] and ThreatModeler [18] are based on vulnerability databases such as OWASP [19]. These tools mainly address software related threats; however they find it difficult to identify threats related to human factors or inappropriate use of the system.

Attacker centric tools such as SeaMonster [20] and securiCAD [21] are better suited for modelling human behaviour, which depends on expert knowledge of the techniques used by the attacker. One of the difficulties is to relate the attacks to system resources and to identify appropriate countermeasures.

Asset centric methods are based on standards ISO 27005 [22] and ISO 31010 [23]. They capture the relationship between threats and system components. These methods assume the involvement of a security expert with extensive knowledge of the types of threats that can affect the system. Manual analysis to identify threats and appropriate responses takes a long time and it is an error prone process.

3 System Security Modeller

The SSM enables automated security risk analysis and identification of counter measures to address security threats. Based on the information in a knowledge base

the primary and secondary threats for the given system model are automatically generated for each asset, along with corresponding candidate control strategies. Primary threats are caused by system faults or malicious activity. Secondary threats represent the propagation of threats through the system This detailed information helps users to understand what measures are required to counter the threats. Compliance threats (described below) are also detected.

The architecture of SSM follows a layered pattern with a clear separation between the Presentation, Access Control, Service and Persistence layers (**Fig. 1**). The browser provides a graphical user interface, written in JavaScript and HTML5. The server side is accessed via a REST Controller which forwards requests to functional modules. System Model Designer provides for the construction of system models by connecting assets. The Model Validator checks and enhances the initial model by generating inferred assets and relations. The Model Querier provides a set of predefined queries for retrieving different parts of the model. The User & Model Management module provides an API for the database which contains Model Metadata and user-related information.

The Persistence layer uses two databases. The Triple store contains the Core Model, Domain Model(s) and System Model(s). The Core Model is an ontology which defines the vocabulary and the relationships between its terms. Domain Models (installed by an administrator) define asset types, permitted relationships, threats and controls relevant to a particular domain. Each System Model (created by a user) uses the elements of a Domain Model to represent the system that the user is modelling: a network of assets and their relationships along with the associated threats and controls (see examples in **Fig. 2** and **Fig. 3**). The User & Model database stores Model Metadata and User details.

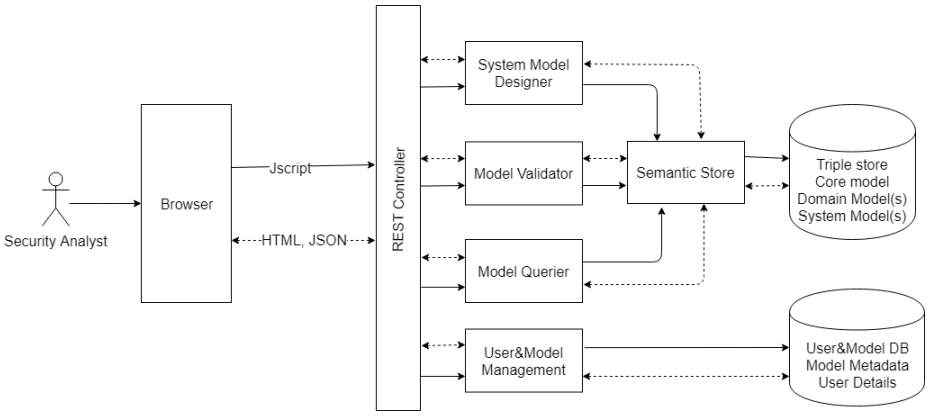

Fig. 1. The main building blocks of the System Security Modeller. The full arrows represent controls and the dashed arrows data flows.

4 Non-compliance as a Threat

The SSM conceptualises non-compliance as a special class of threat. Security threats in our models have the potential to cause misbehaviour (an undesirable effect) in an asset as a result of external causes. Compliance threats differ in that they themselves cause no misbehaviours and have no external causes: they are inherent to the configuration of the system. Security threats also have an associated risk level whereas compliance threats are either present or not. Due to the fact that regulations tend to mandate processes or controls which will mitigate certain classes of threat, there is often an overlap between the security threats found in our models and the compliance threats: controlling for one will often resolve the other. Thus, non-compliance can have security implications by making the system vulnerable to malicious attacks. For example, regulations can mandate that all sensitive personal data must be encrypted and communicated via secure channels. The regulations may stipulate which patterns of interactions between the assets (human and technological) are permitted and which are prohibited. Compliance threats are usually caused by faulty design or misconfiguration rather than malicious activity. To address compliance threats multiple measures often need to applied, for example changing the network of assets (adding/removing assets and relations), using data masking or consent management tools, etc.

To illustrate compliance threats, two examples are provided. The first illustrates country-specific rules for the access and storage of genetic data and the second describes SHiELD best-practice requirements for cross-border health data communication. The GDPR standard mandates that all personal data must be collected and processed lawfully and fairly. The regulations stipulate the type of data that is allowed be communicated and what transformations (i.e. data masking, anonymisation) the data must undergo. In addition to the general GDPR rules, individual countries can also introduce regulations regarding special categories of data such as health data. For

example, they may also introduce specific rules mandating patient's consent prior to accessing any health data.

To check compliance, we validate that both the standard GDPR rules are followed and that country-specific regulations are also satisfied. These requirements state the conditions for data encryption, communication, storage and access. For example, in Spain the regulation stipulates that any genetic data transferred over a network must be encrypted. The regulation in Italy states that access to the space where the genetic data is stored must be restricted to authorised persons only, who must be identified using a biometric key. Access to the genetic data must also be logged to keep track of all access attempts. Furthermore, the audit trail should be made available to citizens whose data was accessed (the data subject). This case can be illustrated by a simple system model consisting of a database server, genetic data, data centre and system administrator (**Fig. 2**).

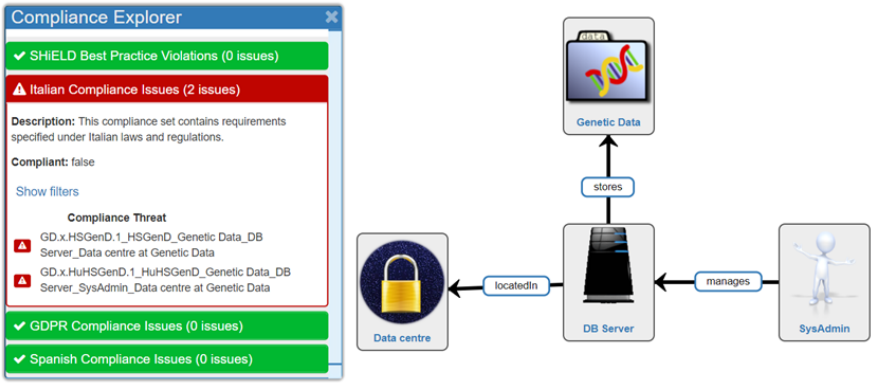

Fig. 2. Compliance with the national regulations concerning access to genetic data.

The Compliance Explorer of SSM indicates two threats for the Italian regulations, that can be resolved by selecting all three controls: Access Control at Data Centre, Biometric ID Verifier at the Data Centre and Logging at DB Server.

5 Break Glass Scenario

Tourism in Europe is one of the most important industries: about 10% of the GDP can be linked directly or indirectly to tourism. According to estimates from the World Tourism Organisation in 2016, 37.6 million tourists visited the UK alone, with 27.9 million from Europe [24]. This mass movement of people also has health implications as visitors from abroad might need emergency medical treatment. In this case access to health data may well be essential. The technology for the exchange of health data is already available, however there are security, legal and compliance issues related to cross border data traffic.

The following “break glass” scenario (also found in [25]) illustrates how health data requirements affect system design. This scenario is illustrated in **Fig. 3** and can be described as follows. An Italian tourist while on holiday in Spain suffers a medical emergency that requires urgent treatment. The Spanish doctor at the hospital’s emergency department contacts Italy via the NCP (National Contact Point) requesting emergency non-consensual access to the patient’s records. The storage and access to health data is governed by the jurisdiction of corresponding countries. The process flow is shown along the top line of the Figure (“Web browser” to “Health record database”) and the various hosts and network infrastructure to convey the messages are shown lower down the figure. All the hosts (including network routers) are linked to specific jurisdictions. The key relationships to the health record are also shown: that the data relates to a human, that it is stored on a server in Italy and received by the “Web browser” in a different jurisdiction.

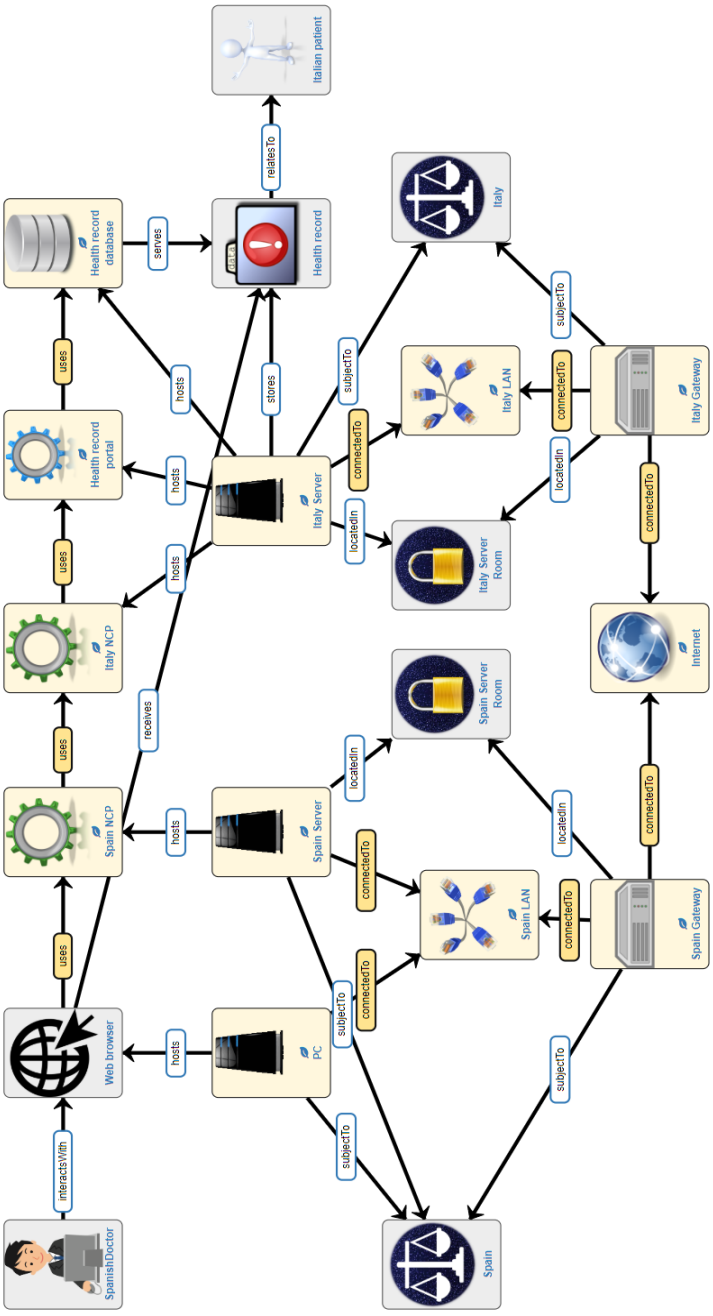

Fig. 3. Modelling the “Break-glass” scenario.

The system model consists of just 20 assets placed by the user but the SSM identifies 306 primary and 164 secondary security threats (many similar). The SSM sup-

ports an iterative process for applying controls and recomputing the number of active threats. For illustration purposes we consider the effect of software patching control. Applying only software patching to the servers, gateways and the PC resolves 129 threats.

The compliance threat analysis shows there are three GDPR compliance issues, one Spanish regulatory compliance issue, and one SHIELD best practice compliance issue. **Fig. 4** shows the SHiELD best practice compliance threat diagram for cross-jurisdictional data transfer which is matched to the elements in **Fig. 3** and thus identified as present in this scenario.

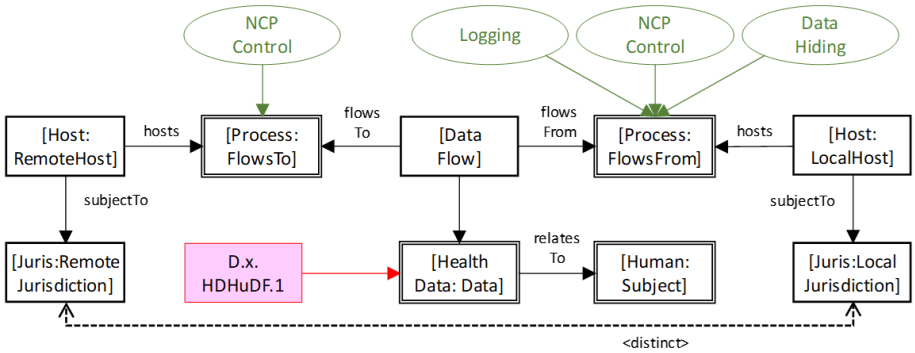

Fig. 4. Cross-jurisdictional data transfer threat.

Error! Reference source not found.Fig. 5 is the dialogue box shown to the user to explain this compliance threat. The compliance threat relates to health data being transferred between two jurisdictions (Italy and Spain here). To be compliant, the software processes on either side of the border ("Italy NCP" and "Spain NCP" in **Fig. 3** and shown as "<distinct>" in **Fig. 4**) must be NCP-regulated exchange processes and data hiding and logging controls should also be used.

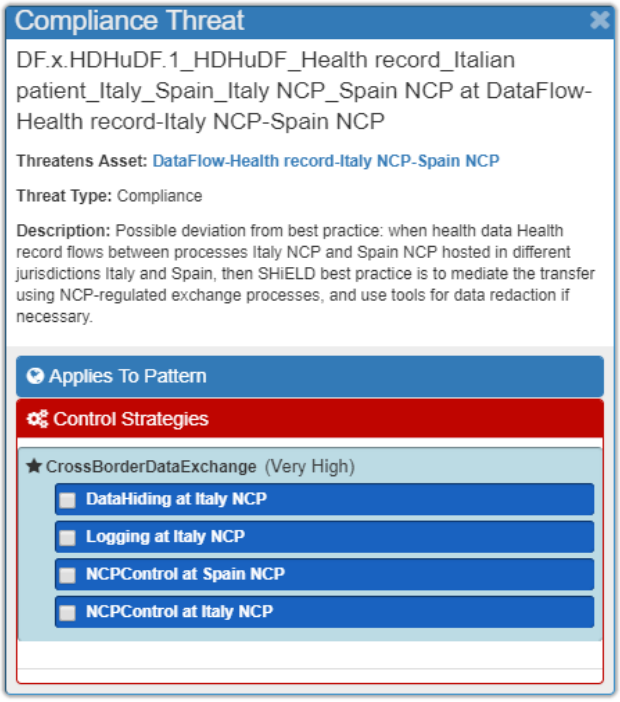

Fig. 5. The SSM identifies a compliance threat (defined as best practice by the SHiELD project) relating to cross-jurisdiction data exchange and proposes the necessary controls.

Summary

This paper interpreted non-compliance as a threat and investigated the security issues of cross border health data exchange. Compliance threats are not security threats and they have no effect on the confidentiality, integrity or availability of data but on the interpretation of local (or national) regulation. In this case the threat is that the system would be non-compliant with the corresponding regulation. The issue of national regulatory compliance was illustrated using the example of genetic data. Genetic data is one of the types of data listed in the GDPR Article 9(4) under which member states may enact their own regulations.

The paper then demonstrated the use of the SSM for security and compliance analysis of a "break glass" scenario illustrating cross border health data exchange. The SSM identifies the potential weaknesses of the system model, automatically generates threat definitions, computes any cascading effects and proposes controls for the mitigation of threats. The security expertise in SSM is encoded in a Domain Model (an ontology) that can be reused for the inference and diagnosis of threats in ICT systems covering both design and run-time. SSM uses semantic and machine reasoning technologies for creating models of systems and associated security properties.

Acknowledgement. The work presented in this paper was funded by the European Union's H2020 research and innovation programme under grant agreement No. 727301 (SHiELD).

References

1. Muller, S., & Supatgiat, C. (2007). A quantitative optimization model for dynamic risk-based compliance management. IBM Journal of Research and Development, 51(3.4), 295-307.
2. "ISO 31000", https://www.iso.org/iso-31000-risk-management.html
3. Refsdal, A., Solhaug, B., & Stølen, K. (2015). Security risk analysis of system changes exemplified within the oil and gas domain. International Journal on Software Tools for Technology Transfer, 17(3), 251-266.
4. Refsdal A., Solhaug B., Stølen K.: Security risk analysis of system changes exemplified within the oil and gas domain. International Journal on Software Tools for Technology Transfer, vol 17(3), pp. 251-66 (2015).
5. Solhaug, B., & Seehusen, F. (2014). Model-driven risk analysis of evolving critical infrastructures. Journal of Ambient Intelligence and Humanized Computing, 5(2), 187-204.
6. Mahler, T. (2008). Tool-supported legal risk management: a roadmap. Eur. J. Legal Stud., 2, 146.
7. Bellamy, R. K., Erickson, T., Fuller, B., Kellogg, W. A., Rosenbaum, R., Thomas, J. C., & Wolf, T. V. (2007). Seeing is believing: Designing visualizations for managing risk and compliance. IBM Systems Journal, 46(2), 205-218.
8. Surridge, M., Correndo, G., Meacham, K., Papay, J., Phillips, S.C., Wiegand, S. & Wilkinson, T. (2018) Trust Modelling in 5G mobile networks. In, SecSoN '18 : Proceedings of the 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges. ACM SIGCOMM 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges (24/08/18) New York, NY. ACM, pp. 14-19. (doi:10.1145/3229616.3229621).
9. Ghanavati, S., Amyot, D., & Peyton, L. (2008, September). Comparative analysis between document-based and model-based compliance management approaches. In 2008 Requirements Engineering and Law (pp. 35-39). IEEE.
10. Breaux, T. D., Vail, M. W., & Anton, A. I. (2006, September). Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In 14th IEEE International Requirements Engineering Conference (RE'06) (pp. 49-58). IEEE.
11. ISO 19600:2014 - Compliance management systems – Guidelines, https://www.iso.org/standard/62342.html
12. Bleker, S., & Hortensius, D. (2014). ISO 19600: The development of a global standard on compliance management. Business Compliance, 2, 1-12.
13. "RSA", https://www.rsa.com/en-us/products/integrated-risk-management/archer-platform
14. "CURA", https://www.curasoftware.com
15. Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons.
16. "VsRISK", https://www.vigilantsoftware.co.uk/.
17. "Threat Modeling Tool," Microsoft, https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
18. "Threat Modeler", http://threatmodeler.com.
19. "OWASP", https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

20. Meland, P. H., Spampinato, D. G., Hagen, E., Baadshaug, E. T., Krister, K. M., & Velle, K. S. (2008). SeaMonster: Providing tool support for security modeling. Norsk informasjonssikkerhetskonferanse, NISK.
21. “securiCAD”, https://www.foreseeti.com/.
22. ISO/IEC, “ISO 27005: Information technology -- Security techniques -- Information security risk management”, 2011.
23. ISO/IEC, “ISO 31010: Risk management – Risk assessment techniques”, 2009.
24. “World Tourist Organization”, http://www2.unwto.org/
25. Larrucea, X., Santamaria, I., & Colomo-Palacios, R. (2019). Assessing source code vulnerabilities in a cloud-based system for health systems: OpenNCP. IET Software, 13(3), 195-202.