Telecommunications Networks Risk Assessment with Bayesian Networks

Marcin Szpyrka, Bartosz Jasiul, Konrad Wrona, Filip Dziedzic

Telecommunications Networks Risk Assessment with Bayesian Networks

Marcin Szpyrka[1], Bartosz Jasiul[2], Konrad Wrona[3], and Filip Dziedzic[1]

[1] Department of Applied Computer Science
AGH University of Science and Technology
Al. Mickiewicza 30, 30-059 Kraków, Poland
mszpyrka@agh.edu.pl, filipdz@student.agh.edu.pl
[2] Military Communication Institute
ul. Warszawska 22a, 05-130 Zegrze, Poland
b.jasiul@wil.waw.pl
[3] NATO Communications and Information Agency
Oude Waalsdorperweg 61, 2597AK Den Haag, The Netherlands
Konrad.Wrona@ncia.nato.int

Abstract. We propose a solution which provides a system operator with valuation of security risk introduced by various components of the communication and information system. This risk signature of the system enables the operator to make an informed decision about which network elements shall be used in order to provide a service requested by the user while minimising security risk related to service execution. In considered scenario transmitted data can be intercepted, modified or dropped by an attacker. Each network component and path can be potentially used to compromise information, since an adversary is able to utilise various vulnerabilities of network elements in order to perform an attack. The impact and probability of such successful attacks can be assessed by analysing the severity of the vulnerabilities and the difficulty of exploiting them, including the required equipment and knowledge. In consequence, each possible service work-flow can be assigned a security risk signature.

Keywords: telecommunications networks, risk assessment, Bayesian networks

1 Introduction

Modern network infrastructure enables transport of information between a sender and a receiver by using different paths composed of multiple network links and nodes. It is a heterogeneous environment which involves various protocols, operating systems, software and hardware [30]. Moreover, a network consists of separate administrative domains, managed by different authorities. In such complex environment software bugs, protocol flaws, non-installed patches, obsolete network components, etc. introduce a risk of unauthorised disclosure or modification of transmitted information.

The diversity of telecommunication devices and protocols must be taken into account when sensitive information is transmitted. It is important not only to protect information by cryptographic measures including confidentiality, integrity and authenticity, but to take into account availability of the information as well. The operator must

be made aware of potential risk of information being compromised when a specific distribution path is chosen. Naive solution consisting of stopping information exchange in case of any non-negligible risk is not viable because existence of any, even smallest, applicable and not mitigated threat would lead to stopping all communication. The solution proposed in this paper focuses on delivering a measurable indicator of risk, so-called risk signature. The risk signature takes the form of quantitative values that can be compared during the decision process, thus offering an advantage over qualitative risk indicators, such as low, medium and high.

2 Motivation

The work presented in this paper has been motivated by challenges related to development of the Information Exchange Gateway (IEG) concept. The North Atlantic Treaty Organization (NATO) and national forces have defined the concept of an IEG to facilitate secure communications between different security and management domains [11]. Related to IEG is the concept of Content-based Protection and Release (CPR) [36]. CPR aims to improve timely sharing of information in the NATO Network Enabled Capability (NNEC) and the Future Mission Network (FMN) [15] environments. Potential implementation scenario for the IEGs using CPR policies is communication between NATO domains and non-NATO organisations, such as United Nations, International Committee of the Red Cross and other non-government organisations.

In current operations timely sharing of information is hampered due to a number of limitations that are inherent to the traditional use of security markings. CPR overcomes these limitations by enforcing access control based on the content properties of an information object instead of a security marking. In CPR the decision to release information object to a user is based on a protection and release policy that expresses requirements the user and the operational environment (e.g. user's terminal) must meet in order to access an information object with a given set of content properties. The requirements are translated to user and terminal attributes; as such CPR is an extension to Attribute Based Access Control (ABAC) [16].

Of particular importance for the approach presented in our contribution is that the CPR policy can also take into account specific environmental attributes such as the risk signature of the network. This enable CPR to provide risk-based adaptive access control. In our proof-of-concept implementation based on XACML 3.0 architecture [27] such risk signature can be obtained by the Policy Information Point from a Dynamic Risk Assessment system [20]. Current IEG solution assumes that surroundings of the protected domain are hostile and their the main source of threats to the information exchange. However the state of the protected domain can also influence a level of risk involved in information exchange process. For example, if some software used on nodes of protected domain has some unpatched vulnerabilities, a communication channel between untrusted domain and protected domain may introduce a possible attack path for outsider attacker. Ability to perform such attack may depend on IEG accepting mediation of particular content type or protocols. If one cannot eliminate risk, in order to control the flow of information between the domains the level of risk should influence the decision whether the information will be sent or dropped. Thus IEG should be able

to selectively and dynamically modify its release policy, depending on a level of risk existing in the internal system. In this paper we present an approach for dynamic risk assessment which can be used in order to support risk-adaptable access control [23].

3 Related Work

The presented approach is in accord with recent research in the network security area, where a number of approaches (including formal ones) to the analysis and design of security systems has been proposed. For example, a formal graph model of a computer network with a variable topology is consider in [22]. The model is used for the verification of security constraints. An extension of attack graphs called multiple-prerequisite graphs is considered in [17]. A computer software based on it is used to classify vulnerabilities and recommend actions to improve network security. Anticipation game framework with the so-called strategy objectives is considered in [13]. This extension of attack graphs is used to coupe with both the financial and temporal aspects of attacks. Some authors focuses on formal approach to the design of network elements e.g. firewalls. For example, the design of a network firewall with a formalised rule-based framework called XTT2 [26] is proposed in [25]. Another rule-based approach that uses RTCP-nets [31] is considered in [32] and [34]. Moreover, exclusion rule-based systems are proposed in [33]. Due to such frameworks possible anomalies in the security policy can be eliminated during the design stage.

There are several methodologies used to asses the risk. One of the most popular is CCTA Risk Analysis and Management Method (CRAMM) [1], which is used in the UK, Denmark and Czech Republic. NATO uses a modified version of CRAMM, compliant with NATO security policy, supporting directives and guidance. CRAMM analyses vulnerabilities of the system and potential threats that may have impact on loss of assets and functionality. It is a qualitative methodology that covers identified aspects that may affect the risk: personnel security, physical security and security of information. It utilises a large database with detailed questions and it is compliant with ISO/IEC standard [18]. A week point of this technique is a lack of possibility to analyse algorithm used to calculate the risk.

Pilar [3] is a risk assessment tool based on Methodology for Information Systems Risk Analysis and Management (MAGERIT) [24] developed in Spain. This methodology provides a qualitative risk assessment. Risk is represented as the impact of the threat weighted by its rate (or expectation) of occurrence. A customised version of Pilar is used also within NATO.

The Expression of Needs and Identification of Security Objectives (EBIOS) [9] methodology has been created by the French National Security Agency. The methodology covers 5 steps: context, security needs, threats analysis, identification of security objectives and identification of security requirements. It allows to assess, communicate, and choose appropriate mitigation measures for risks related to information security.

Method for Harmonized Analysis of Risk (MEHARI) is another French information risk assessment method, developed by association of information security professionals and designed for an analysis of risk situations described through scenarios [4].

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method [10] is a framework for identifying and managing information security risks developed by Computer Emergency Response Team. It also is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning. The method is used to: (i) identify critical assets and the threats to those assets, (ii) identify the vulnerabilities, both organisational and technological, that expose those threats, creating risk to the organisation, and (iii) develop a protection strategy and risk mitigation plans to support the organisation's mission and priorities.

4 Case Study

As an illustrative example for the proposed approach and calculation of risk we will use hypothetical protected network shown in Fig. 1. The network provides an access to confidential data by using two redundant database servers. The only way to collect the data is to send a request to one of the two web servers. A web server sends a request to a database server and then provides the user with the received answer. A firewall is used to isolate the network from the Internet. The security policy allows users from other domains to send requests to the services located in the protected domain. Due to different transmission media, the possible access routes differ in the level of security [35].

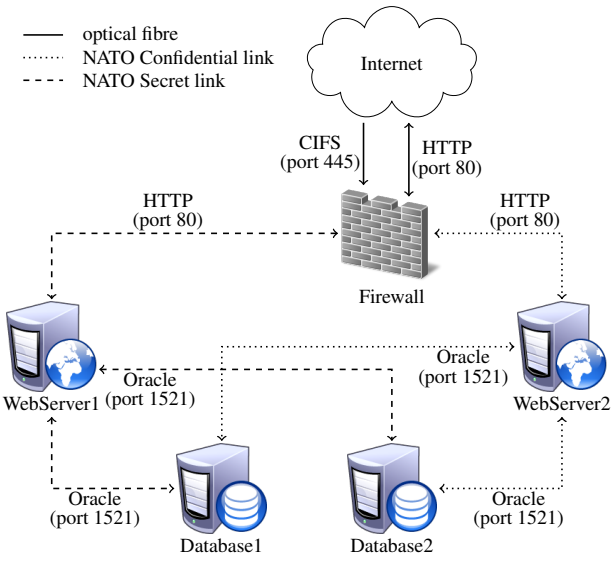

Fig. 1. Network topology

While estimating the risk of information retrieval, it is necessary to take under consideration different confidentiality protection levels for the used transmission media. Moreover, there are additional factors affecting the security of depicted network. These

are various services offered in the domain and software installed on devices. Usually, the more equipment, protocols and software are used in the network, the more potential vulnerabilities are present. These vulnerabilities might be used for taking control of either a device or a service and can lead to revealing sensitive information to adversary. Scenario presented in Fig. 1 is partially related to current NATO works on providing information exchange capability for information domains with different classification levels, e.g., NATO Secret, NATO Confidential, and Mission Secret. In the past military networks with different confidentiality level had to be completely separated. Currently, in order to facilitate information sharing, collaboration and reduce duplication of data, there is a trend to provide controlled and secured interconnection of networks operating on different security levels. Risk assessment in this case is identified as a crucial element in taking decision whether to send (or not) the information.

5 Proposed Solution

The proposed risk analysis method is composed of two main components. The first component (see: box 1 in Fig. 2) is dedicated to evaluation of a risk level of individual network elements and the network as whole. The second one (see: box 2 in Fig. 2) is to assess the influence of the risk introduce by the individual network elements involved in execution of a service offered to the end user on the total risk signature of this service.

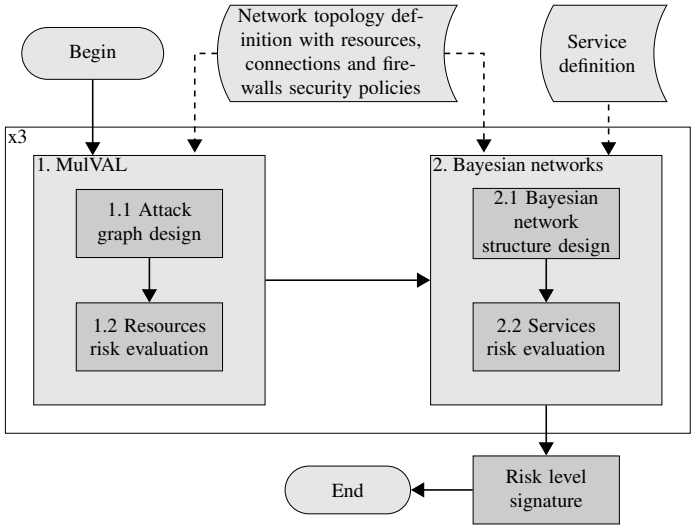

Fig. 2. The proposed approach scheme

The first part of risk assessment method is based on MulVAL tool [28] (see also Sec. 5.2). Attack trees [29] were chosen to assess likelihood of successful attacks on assets vulnerabilities. Attack trees (see Sec. 3) provide a formal, methodical way of

describing structure of attack on specific goal. Precisely, the root node represents the object of an attack and leafs are the steps that must be done to achieve the goal. For instance, if a malicious user of a corporate network wants to read a document stored at his supervisor's computer, he needs to get access to this computer. He can trick the supervisor into running specially prepared code that will send documents to him via e-mail (social engineering attack). Alternatively, he can brake into supervisor's office, then start the computer and guess the password. At last, he can recognise the infrastructure of the network, identify the computer he wants to take control over, compromise the personal firewall, which was not updated, and inject a code that will allow him to download the document by the FTP protocol.

The second part of our method takes into account that the specific services provided to the users usually rely only on a subset of all network elements. Therefore, the fact that some high risks elements are present in the network does not necessarily mean that the particular service is exposed to high risk as well. For example, the fact that an email server is exposed in a specific network configuration to a high security risk might be irrelevant for a service which provides end user with an access to geographic information stored in a database. Thus, in order to provide a meaningful assessment of risk level which a particular service is exposed to and therefore estimate risk which is transferred to the end user and his operations the risk assessment has to take into account a specific set of network links and nodes which are utilised by the service [35]. Every service can be described as a work-flow, involving different network elements, such as servers, routers, and links. We model the dependencies between steps of the work-flow as Bayesian network (also called belief network) [12,14] (see also Sec. 5.3).

5.1 System Description

In the example considered in Sec. 4, it is assumed that the detailed network topology with its resources and connections among them must be described and provided to MulVAL tool. Vulnerabilities of network elements, software and protocols are obtained from National Vulnerability Database (NVD) [6]. This database, widely used by various security vendors and computer emergency response teams, includes information on specific threats. A record from NVD, called CVE (*Common Vulnerabilities and Exposures* [2]), contains:

- CVE Identifier (eg. CVE-2012-5689),
- description (*short information on vulnerability*),
- asset impacted (*some software, protocol*),
- version infected,
- severity,
- impact,
- score (*value representing potential harmfulness of vulnerability*).

5.2 MulVAL

The system description is used by MulVAL tool to calculate the risk of every affected network element. In fact, MulVAL is used three times in order to assess the risk for

confidentiality (C), integrity (I) and availability (A). MulVAL (Multi-host, Multi-stage Vulnerability Analysis Language) [28] is a research tool used to manage the configuration of an enterprise network such that the security risks are appropriately controlled. MulVAL provides a reasoning engine for automatically identifying vulnerabilities in an enterprise network. It uses Datalog facts to represent configuration information and Datalog rules to represent attack techniques and OS security semantics. After analysing the configuration of a network, the MulVAL reasoning engine outputs a logical attack graph. An example of such a graph (borrowed from [5]) is shown in Fig. 3.

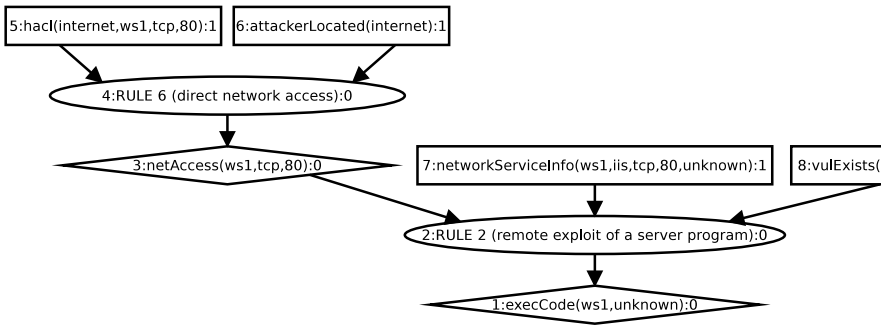

Fig. 3. Example of MulVAL attack tree [5]

A logical attack graph directly encodes the logical causality relationship among configuration settings and potential attacker privileges. Its key goal is to show *why an attack can happen*. There are three kinds of vertices in such a graph: rectangle vertices represent facts, elliptic vertices represent reasoning rules and diamond vertices represent privileges an attacker can obtain through exploiting the vulnerabilities in the considered system. The part of a logical attack graph shown in Fig. 3 refers to estimating the probability of a successful database server attack.

At the first glance, the value of the risk obtained from MulVAL can be perceived as sufficient. In fact, this method delivers assessment of risk for the network. However, the obtained value does not take into account that some network components might be irrelevant for execution of a particular service, thus even if they are high risk assets, they may not have much influence on risk level for delivery of the service to the end user. In fact, there can be various routes more often used to exchange of information. Thus, additional method is required in order to amend the value obtained from the first assessment and to present the actual risk for the particular service or mission objective supported by the system.

5.3 Bayesian Networks

Bayesian networks [19] were identified as a suitable method to accomplish this goal. Bayesian networks allow for inverse representations of the probabilities concerning two events. For instance, event B is a consequence of event A, what can be described as

$A \rightarrow B$. It means that A is the reason for the consequence B. However, the question often is: *What is the probability of A if B was observed?* The answer can be calculated from the statement of Bayes' theory:

$$P(A|B) = \frac{P(A \cup B)}{P(B)} = \frac{P(B|A)P(A)}{P(B)}, \text{ where } P(B) > 0 \tag{1}$$

As noted earlier, we model the dependencies between steps of the service workflow as Bayesian network. The network elements are used by the service in a specific order which has to be captured in the model. Some of the elements might appear in these workflows several times (e.g. a particular link can be used for transmitting both a request to the database and an answer to the query). Similarly, the specific steps of the service workflow can be implemented by using several different network elements. For example, there might be several independent communication links available between a Web server and a database and the database might be replicated on several separate servers for sake of performance and redundancy. In order to deal with possible cycles, it was necessary to represent some of the nodes multiple times in the resulting Bayesian network. However, this multiplication does not interfere with the calculation of the final risk values, as the risk introduced by the particular network element is taken into account only once in the overall calculation. Every network element is assigned three independent risk values related to confidentiality, integrity and availability. For the network nodes, these risk values are calculated by using the information about relevant vulnerabilities, provided in the NVD, and known applicable attacks modeled using MulVal methodology. For the network links, a simplified model has been used, assigning static risk values in the C-I-A dimensions, depending on the characteristic of the links.

The reasoning in the Bayesian network describing service dependencies has been performed by clustering algorithm as described in [21]. This algorithm consists of two stages. In the first stage directed graph representing dependencies between vulnerabilities and attacks is decomposed to a tree. In the second stage the appropriate inference on the obtained tree is conducted. The overall risk level is calculated from a perspective of the user accessing the service and consists of three values, describing risk to confidentiality, integrity and availability of the service. The results and the proof of concept are shown in Sec. 6.

6 Proof of Concept

In order to validate the proposed approach in practice, a prototype software called *Network risk assessment tool* has been developed. The application uses a client-server architecture, with a front-end based on a Web browser supporting JavaScript. The software has been developed by using Java and Play Framework [7]. All the calculations for Bayesian networks were performed with the aid of the SMILE library [8] and for Bayesian networks visualization the GeNIe development environment has been used. The back-end application uses the PostgreSQL database server to provide all data which is necessary for risk calculations.

The developed tool takes under consideration different network devices such as hosts, servers etc. and connections among them. The MulVAL software enable us to take into consideration firewalls configuration and dependencies among resources. Dynamically constructed Bayesian networks make it possible to assess the risk of functioning of any particular service. In order to provide reliable results, we have used real information about vulnerabilities obtained from the US National Vulnerability Database [6].

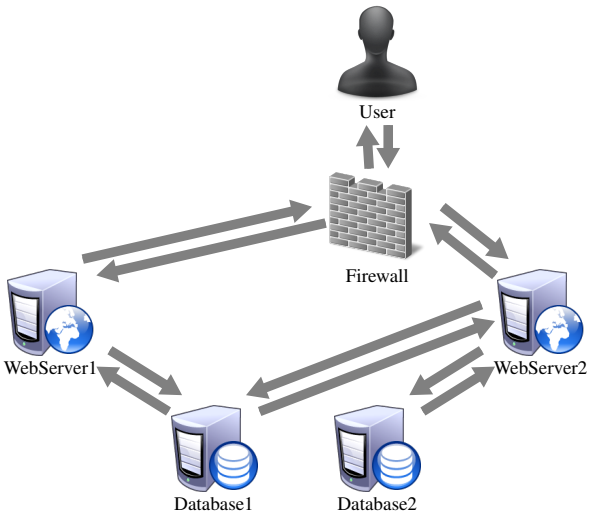

Fig. 4. Possible communication routes

The application has been tested successfully. One of the test cases based on the network shown in Fig. 1 is presented below. Suppose, the possible communication routes are defined as shown in Fig. 4. In such a case, we have redundant routes used to access data stored in the database servers. The aim of the computation is to assess the risk for the service that guarantee access to the data.

The redundant routes decrease the risk of loss of access to the data significantly. On the other hand, the greater the number of devices in a network is, the greater the risk of data being compromised. It is a result of potential vulnerabilities introduced by every additional node or link. These vulnerabilities might be exploited by the adversary to get an access to information or to disrupt communication.

The considered test scenario illustrates also the impact of vulnerabilities on the risk for three security dimensions: confidentiality, integrity and availability. Different vulnerabilities have different influence on the assessed risk signature. This is due to variations in difficulty of vulnerability exploitation, harmfulness, impact on the whole communication, etc. As a part of validation scenarios, we have also simulated that some vulnerabilities were detected and the related risks mitigated, in order to observe how this process influences the overall risk signatures. Values of estimated risk are shown in Table. 1.

Table 1. Description of the test case scenario

No	Step description	Risk		
		C	I	A
1	Vulnerability: non-identified. Risk assessed on the basis of historical data.	0.07108	0.07108	0.01783
2	Vulnerability: HTTP IIS Server at WebServer 1, monitoring of port 80 TCP. The vulnerable configuration is seen very rarely in practice (difficult utilization). CVE Access Complexity: High. Result: Insignificant increase of confidentiality risk	0.08448	0.07108	0.01783
3	Vulnerability: none - exclusion of HTTP IIS Server vulnerability from point 2. Risk reset to initial values from Step 1.	0.07108	0.07108	0.01783
4	Vulnerability: HTTP IIS Server misconfiguration at Web Server 1. CVE Access Complexity: Medium. Accessible for medium-skilled intruders. Significant change of risk for confidentiality	0.34257	0.07108	0.01783
5	Vulnerability: new HTTP infection at WebServer 2. CVE Access Complexity: Medium. Vulnerability affects all security measures.	0.36549	0.19174	0.02558
6	Vulnerabilities: 1) new infection at Database 1; 2) software misconfiguration at whole network. CVE Access Complexity: Medium. Vulnerability no. 1 affects integrity and availability. Vulnerability no. 2 affects all security measures. Risk: significant increase of all values. Due to redundant routes information is still available, however it is exposed to disclosure and modification.	0.36549	0.25429	0.22009

7 Conclusions

The approach presented in this paper is the first step to assess the risk of compromising services and information provided by a heterogeneous networking environment. Presented solution assesses the risk derived from vulnerabilities of both network links and network nodes, including the vulnerabilities introduced by software and hardware configuration. Current implementation takes into account network elements that are vulnerable to attacks resulting in leakage, modification or unavailability of transmitted data as well as static technical security countermeasures, which can be used to reduce the applicable attack surface. One possible extension of our model is the possibility of modeling of dynamic deployment of technical security countermeasures that reduce risk. Such technical countermeasures include, e.g. intrusion detection systems, network guards and dynamically changing security policy. Obviously, it is impossible to fully exclude the risk involved in the operation of telecommunication networks due to various malware, vulnerabilities of operating systems and network components. To imagine the number of threats, one can observe how often the software (including anti-virus tools) installed on his machine are updated. Therefore information stakeholders must deal with the risk and they need to know the risk signature of their system. The proposed solution provides them with a risk valuation, which can be used by network nodes to find the best route for information exchange and can help network administrators to take appropriate decision about which network links should be considered safe or risky.

The novelty of our solution is in two-step risk assessment. The first step relies on evaluation of attack graphs and uses vulnerabilities description (based on NVD) and

network configuration information to assess risk signature for individual network assets. Our approach take into account both risk self-induced by particular assets and the risk induced by the operational environment. The second step involves calculation of risk signature for a particular service offered by the system to end users. Calculation of risk is performed on the basis of Bayesian networks, which allow us not only to obtain a detailed risk signature, but also to analyze reasons and consequences of risk. Our approach is comprehensive and takes into account all system components and network communication links required to provide user with a service. The calculated risk signature covers all three dimensions of security, i.e. confidentiality, integrity and availability. Our solution is more of a quantitative than a qualitative methodology when compared to some of the widely used methods, such as CRAMM or Pilar. Thus, we believe that our proposal offers broader and more detailed approach to risk assessment for system objectives and user services.

Acknowledgements

Work has been partially financed by the European Regional Development Fund the Innovative Economy Operational Programme, INSIGMA project no. 01.01.02-00-062/09.

References

1. CCTA Risk Analysis and Management Method. http://www.cramm.com/
2. Common Vulnerabilities and Exposures. http://cve.mitre.org/
3. EAR/Pilar - Risk Analysis Environment. https://www.ccn-cert.cni.es/
4. MEHARI - Method for Harmonized Analysis of Risk. http://www.clusif.asso.fr/
5. MulVAL Attack Paths Engine. http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/MulVAL_Attack_Paths_Engine_-_User_and_Programmer_Guide
6. National Vulnerability Database. http://nvd.nist.gov/
7. Play Framework. http://www.playframework.org/
8. SMILE Documentation. http://genie.sis.pitt.edu/wiki/SMILE_Documentation
9. Agence nationale de la sécurité des systèmes d'information: Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) (2010)
10. Alberts, C.J., Behrens, S.G., Pethia, R.D., Wilson, W.R.: Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, version 1.0 (1999)
11. Apiecionek, Ł., Romantowski, M., Śliwa, J., Jasiul, B., Goniacz, R.: Safe exchange of information for civil-military operations. In: Military Communications and Information Technology: A Comprehensive Approach Enabler, pp. 39–50. WAT Publishing (2010)
12. Barber, D.: Bayesian Reasoning and Machine Learning. Cambrdge University Press (2013)
13. Bursztein, E., Mitchell, J.: Using strategy objectives for network security analysis. In: 5th China International Conference on Information Security and Cryptology (Inscrypt) (2009)
14. Darwiche, A.: Modeling and reasoning with Bayesian networks. Cambridge Univ. (2009)
15. Domingo, A., Wietgrefe, H.: A NNEC-compliant approach for a Future Mission Network. In: Proc. of the Military Communications Conference (MILCOM) (2012)
16. Hu, V.C., Ferraiolo, D., Kuhn, R., Friedman, A.R., Lang, A.J., Cogdell, M.M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K.: Guide to Attribute Based Access Control Definition and Considerations (Draft). NIST Special Publication 800-162. Gaithersburg, MD (2013)

17. Ingols, K., Lippmann, R., Piwowarski, K.: Practical attack graph generation for network defense. In: Proc. of ACSAC Conf. 2006, pp. 121–130. IEEE Computer Society (2006)
18. ISO/IEC: ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements (2008)
19. Kjaerulff, U., Madsen, A.: Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis. Springer (2008)
20. Lagadec, P.; Dandurand, L.; Bouillon, E.; Wrona, K.; Torrente, S.: Cyber Defence Situational Awareness and Dynamic Risk Assessment. In: NATO Research and Technology Organisation Symposium on Information Assurance and Cyber Defence. Tallin, Estonia (2010)
21. Lauritzen, S., Spiegelhalter, D.J.: Local computations with probabilities on graphical structures and their application to expert systems. Journal of the Royal Statistical Society series B **50**, 157–224 (1988)
22. Matousek, P., Ráb, J., Rysavy, O., Svéda, M.: A Formal Model for Network-Wide Security Analysis. In: Proceedings of the 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, pp. 171–181. IEEE Comp. Soc. (2008)
23. McGraw, R.: Risk-adaptable access control (radac). In: NIST Privilege (Access) Management Workshop (2009)
24. Ministerio de Administraciones Públicas: MAGERIT – version 2, Methodology for Information Systems Risk Analysis and Management, Book I – The Method (2006)
25. Nalepa, G.J., Ligęza, A.: Designing reliable Web security systems using rule-based systems approach. In: E. Menasalvas, J. Segovia, P.S. Szczepaniak (eds.) Advances in Web Intelligence. AWIC Conference 2003, *LNAI*, vol. 2663, pp. 124–133. Springer-Verlag (2003)
26. Nalepa, G.J., Ligęza, A., Kaczor, K.: Formalization and modeling of rules using the XTT2 method. International Journal on Artificial Intelligence Tools **20**(6), 1107–1125 (2011)
27. OASIS: eXtensible Access Control Markup Language ver. 3.0. Tech. Rep. August (2010)
28. Ou, X., Govindavajhala, S., Appel, A.: MulVAL: A logic-based network security analyzer. In: Proc. of 14th USENIX Security Symposium. Baltimore, Maryland, USA (2005)
29. Schneier, B.: Attack trees: Modeling security threats. In: Dr. Dobbs' Journal (1999)
30. Sliwa, J., Gleba, K., Chmiel, W., Szwed, P., Glowacz, A.: IOEM - Ontology Engineering Methodology for Large Systems. In: P. Jedrzejowicz, N.T. Nguyen, K. Hoang (eds.) Computational Collective Intelligence: Technologies And Applications: ICCCI 2011 Conf., *Lecture Notes in Artificial Intelligence*, vol. 6922, pp. 602–611. Springer-Verlag (2011)
31. Szpyrka, M.: Analysis of VME-Bus communication protocol – RTCP-net approach. Real-Time Systems **35**(1), 91–108 (2007)
32. Szpyrka, M.: Design and analysis of rule-based systems with Adder Designer. In: C. Cotta, S. Reich, R. Schaefer, A. Ligęza (eds.) Knowledge-Driven Computing: knowledge engineering and intelligent computations, *Studies in Computational Intelligence*, vol. 102, pp. 255–271. Springer-Verlag (2008)
33. Szpyrka, M.: Exclusion rule-based systems – case study. In: International Multiconference on Computer Science and Information Technology, vol. 3, pp. 237–242. Wisła, Poland (2008)
34. Szpyrka, M., Szmuc, T.: Decision tables in Petri net models. In: M. Kryszkiewicz, J. Peters, H. Rybinski, A. Skowron (eds.) Rough Sets and Intelligent Systems Paradigms, *LNAI*, vol. 4585, pp. 648–657. Springer-Verlag (2007)
35. Wrona, K., Hallingstad, G.: Real-time automated risk assessment in protected core networking. Telecommunication Systems **45**(2-3), 205–214 (2010)
36. Wrona, K., Hallingstad, G.: Controlled information sharing in NATO operations. In: IEEE Military Communications Conference (MILCOM), pp. 1285–1290. IEEE (2011)