DYNAMIC RISK ASSESSMENT IN INFORMATION SYSTEMS: STATE-OF-THE-ART

David López[1,2], Oscar Pastor[2], Luis Javier García Villalba[1]

[1] Group of Analysis, Security and Systems (GASS)
Department of Software Engineering and Artificial Intelligence (DISIA)
School of Computer Science, Office 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n, Ciudad Universitaria, 28040 Madrid, Spain
Email: {dlcuenca, javiergv}@fdi.ucm.es

[2] Systems Engineering for the Defence of Spain, S.A (ISDEFE)
Defence and Security Direction
Email: {dlcuenca, opastor}@ isdefe.es

Abstract

Nowadays Risk Management is a common practice in the Information Systems security field. It is usually supported by a Risk Assessment process, which is done at regular but unfortunately large intervals. This lack of a continuous Risk Assessment process in an ever-changing environment, such as Information Systems, tends to make Risk Management a more complex and less accurate task. In this paper different existing approaches to face Dynamic Risk Assessment and Management are recapitulated along with their pros and cons and finally, future action lines are proposed in order to avoid existing gaps.

Keywords - Dynamic Risk Assessment, Online Risk Assessment, Real Time Risk Assessment.

1 INTRODUCTION AND PAPER STRUCTURE

Risk Assessment (hereinafter RA) is common practice in Information Systems (hereinafter IS) domain. Unfortunately, it is generally approached just as an isolated and discrete exercise done in predefined intervals. This is undoubtedly useful for long-term management planning, but might waste the potential to prevent and treat those risks arising in the meantime, in alignment with our RA methodology and Risk Management (hereinafter RM) policies. IS security tools sometimes offer continuous risk evaluation features but they are based on their own proprietary methodologies, thus likely following different analysing methods and mitigation strategies to the ones chosen to develop our RM capabilities. This motivates the thorough analysis of present Dynamic Risk Assessment approaches, applied to the continuously changing IS environment. Results outline that integration of security systems and tools designed to assess risks in a dynamic or even real-time basis, while following renowned methodologies, appears to be an interesting improvement area.

RA and RM applied to IS are useful tools to assess risk exposure and drive management actions, when designing Organization's risk mitigation plans on a given moment in time, as summarized in Section 2. Nevertheless, Risk Assessment/Management presents an unattended and actually wasted potential to ease the real-time security decision making, by taking advantage of continuous risk exposure monitoring. Unfortunately, this potential has not yet been fully developed, but efforts on this way have already been made. Section 3 gathers main currents that try to endorse this capability, mainly adopted under the concept of Dynamic Risk Assessment (hereinafter DRA). This concept encloses the continuous update of inputs influencing on risk assessment, in order to optimize ulterior management decisions based on current risk circumstances. Conclusions drawn from previous analyse are exposed in Section 4, which also propose future action lines to be developed.

2 BACKGROUND

2.1 Risk Assessment and Risk Management Concept

RM aims to help Organizations, establishing priorities and focusing security resources in order to reduce risk exposure. Risks, being very different in their nature, may reach high importance when they affect IS, since nowadays this largely supports our society's welfare state.

RM process lays on RA technique. RA is defined [1] as the process that tries to identify, analyze and evaluate, through a broad range of involved variables, potential events with a measurable impact on an Organization's objectives. It implies a foresight exercise, based on both historical data and rational event analysis. Outcomes of RA are not intended to replace empirical evidences, but there are usually not enough of them to provide a good insight on risk exposition. Expert judgment is often a relevant source of information on the subject, and models based on traditional probability theory are commonly used tools. Assuming risk is a dynamic concept that fluctuates over time in response to environment evolution, RM is expected to follow-up the changes so as to monitor their effects. It may be done on the basis of a reiterated assessment that allows contrasting subsequent results coherently.

2.2 Information Systems Methodological Risk Assessment

RA complexity grows along with the environment and Information System complexity. Understanding and evaluation of RA factors carry a certain degree of subjectivity, as long as they are not always driven by objective data or facts observation. However, for a RA to be further useful, it must be precise and allows contrast and comparison against previous assessments, or against assessments done in similar environments. This is the main reason to adopt a methodological approach, which will also decrease the aforementioned analyst subjectivity impact on the assessment.

Throughout IS technologies field, cutting-edge methodologies are the following, mainly supported or sponsored by the quoted organizations: ISO 27005:2011 (IEC - International) [2]; MAGERIT (Ministry of Public Administration - Spain) [3]; OCTAVE (SEI Carnegie Mellon University - USA) [4]; CRAMM (Siemens Insight Consulting - UK) [5]; EBIOS (DCSSI - France) [6]; IT Baseline Protection Manual (BSI - Germany) [7]; and NIST SP800-30 (NIST - USA) [8].

There are several tools that implicitly apply some of these methodologies and aid the RA process. They tend to offer features such as knowledge bases, workflows, as well as automatic computation. European Network and Information Security Agency (ENISA) inventory on Risk Assessment and Management methodologies [9] compiles most renowned methodologies and their associated tools, with a brief comparison. As a rule, those methodologies are based on similar key principles defined as follows, keeping some differences in mind. They interrelate as shown in [2] and in Fig. 1.

A. Assets:

They are not only hardware, networks or software (always related to an IS), but also all those supporting the underneath infrastructure such as staff (administrators, operators, users...) or facilities. It may include even much more intangible ones like information, brand image or reputation. Assets have a relative value for an Organization, and are often linked between them, generating a hierarchy.

B. Threats

The events or root causes that may provoke an incident, with unwanted results for an Organization's objectives materialized on harm or loss of assets.

C. Vulnerabilities

Flaws or weaknesses on procedures, design, implementation or internal security controls in IS, that may be exploited purposely or accidentally.

D. Impact

It is the result arising from a threat taking advantage of asset vulnerabilities, and thus causing a certain degradation or loss of the asset's value.

E. Probability / Frequency

Likelihood of, or number of times, a threat happens over a given period of time.

F. Risk / Residual Risk

It is the potential that a given threat will exploit a vulnerability of an asset and thereby cause harm to the Organization. Safeguards and risk treatment allow to lower risk to a certain remaining value.

G. Safeguards

They are security measures (resources or procedures) that somehow mitigate risk. Depending on their nature, they can focuse on prevention, protection, detection, isolation, confrontation, recovery, etc.

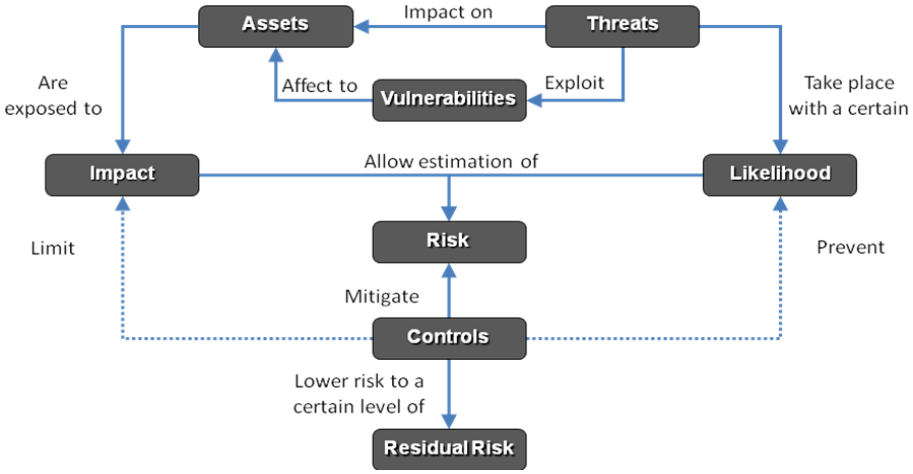

Fig. 1 Conceptual diagram of RA key factors and their interrelations, based on Magerit methodology (site: https://www.ccn-cert.cni.es/publico/herramientas/pilar43/en/index.html)

3 DYNAMIC RISK ASSESSMENT AND MANAGEMENT

Changes happening on IS, modify in some way the initial picture. This implies that RA inputs are no more the ones used to formerly assess the IS risk exposure. Thus, accuracy of RA outcomes decreases and uncertainty rises over time. RM needs to take those changes into account, in order to be effective when mitigating risk exposure. Standards are aware of this requirement. International standard ISO 27001 [10] compels to do it, under the PDCA (Plan – Do – Check – Act) concept. It establishes a cycle where RA is repeated over defined periods of time, and RM planning is adapted to the new scenario of risk. NIST (National Institute of Standards and Technology) also defines a six-step process for RM [11] that is iterated all through the IS lifecycle. Nevertheless, this is a false sense of dynamism since these iterations take place on discrete (and usually long) periods of time. The shorter those periods are the better, although crucial changes to risk exposure could happen meanwhile.

3.1 Dynamic Risk Assessment and Management Concepts

As already stated, there are several factors to be taken into account on RM, which are subjected to randomness and dynamism. They can be grouped in 4 sets: IS changes, mainly addition, modification or suppression of assets, as well as alterations on maintenance services, resources, providers and so on, supporting the IS; Zero-day vulnerabilities or new detected threats, but also unknown threats and vulnerabilities, affecting the Organization' assets; Evolution of already known threats and ultimately monitored threats causing an incident; and Security measures or safeguards implementation, modifying the expected impact or probability that a threat harms an asset. Literature sometimes defines as the simple discrete reiteration of RA over defined periods of time [12], the same way standards promote with RM cycles. Through the following sections, a broader literature analysis will show alternative approaches and concepts surrounding DRA, where focus is put on a continuous feeding of inputs, allowing a more suitable characterization of variables. When something in the IS or its environment suffers a change, RA inputs may be altered to reflect it. Then RA computations will throw new results that might assist in allocating better Organization's security resources.

Literature sometimes refers to "Online Risk Assessment" [13], [14] or "Real Time Risk Assessment" [11], [15] as synonymous of the herein used "Dynamic Risk Assessment". Although DRA is the most repeated term, they all principally rely on a regular update of the RA variables defining the IS and its

environment. Occasionally, attention is shifted to dynamics during the phase of risk treatment. This paper tries to compile and review literature touching upon the DRA subject to establish similarities in their approaches. They have been catalogued according to their scope and inspiring principles, although drawing a separation line has been difficult since concepts are mixed or interrelated at times.

3.2 Dynamic Risk Assessment Evolution

A. Database Inputs

Massive factual and trustworthy data gathering is really difficult to achieve, being one of the main drawbacks of RA, and making it hard to get a realistic outcome of the process. So specialized and reliable sources of information should be located, which in addition are to be regularly updated. Nowadays there are standardized formats to exchange this data, depending on the researched information [16] such as: CVE, NVD, CPE, OVAL, KML, CVSS, etc.

Nowadays several repositories of data for open use exist, even with government support such as National Vulnerability Database provided by NIST [17]. It is basically focused on IS vulnerabilities broadcasting. Other initiatives [18], [19] try to promote the sharing of information (anonymously when required) about threats, vulnerabilities, intrusions, security incidents, etc. through CERTs (Computer Emergency Response Team) or CSIRTs (Computer Security Incident Response Teams).

B. Attack Trees and Graphs

This approach tries to define attack patterns an attacker is prone to follow against the IS. These patterns capture dynamics of an attack and stages it has to go through in order to reach final target.

When talking about physical security, anyone is able to conceive a defensive architecture with several subsequent layers of protections (trenches, fences, walls, armored doors, safe boxes, etc.). The attacker must overcome all of them, or at least all those blocking its way, to reach its target.

Graph and attack trees display on its own way the paths that lead from an attacker to a likely target. These paths are composed of interconnected nodes, and each of the nodes is a step (action to be done, vulnerability to be exploited, etc.) the attacker has to complete to reach next node. There can be several paths or branches arriving to the same final target. Each node has an associated probability that the attacker succeeds, and the enchainment of probabilities in all the nodes and paths gives the likelihood of the final target node being accomplished. This kind of RA can be applied from two different points of view:

1) Crisis simulation, where there are attack scenarios for training purposes. They can be used to emulate real situations, and let technical staff or management to play their role. This is in no case a dynamic type of RA;

2) Dynamic Risk Management based on real-time response to security incidents. Thus there has to be a security framework with systems able to detect security events such as IDS/IPS, and let the RA tool knows in which stage of development the attack is (meaning: exact node within the tree/graph the attacker already achieved). This approach allows foreseeing next steps expected from the attacker, and where the path can be hardened to avoid its progress. There are security tools with features for alert and assessment of events, but the last are done on the basis of a narrow or limited knowledge of the IS, instead of the most extensive knowledge the RA tool may have of the IS and its environment.

Herein risk estimation is commonly done by using Bayesian Networks [20]. They make use of Directed Acyclic Graphs (DAGs) to establish probabilistic relationships between variables. Hierarchical Coordinated Bayesian Model (HCBM) can also be applied [21] to assess extreme event likelihood, integrating several knowledge databases regarding those events.

Dantu [22] proposes that paths and probability of node exploitation could be attacker specific depending on its profile and skills (script kiddies, hackers, insiders, etc.). There are different predefined profiles and vulnerabilities linked to them, balancing complexity versus expected expertise. In this way trees become customized. Computations are also based on Bayesian Networks.

Another peculiar case is the Network Security Risk Model (NSRM) used in Process Control Network (PCN) environments [23]. It turns to characterize dynamism like a cyclical comparison between RA at a given moment (baseline) and attack trees simulations, leading to enhancement of mitigation

strategies. Nonetheless, it is self-critical arguing that it may be helpful to have real-time inputs and learning capabilities to better react against attacks.

C. Joint Approach

Previous solutions focus on a few important matters regarding IS risk estimation, but leave the rest aside. Some efforts [20] are centered on attack trees usage followed by mitigation planning based on cost-benefit (ROI), but also taking inputs from CVSS database about vulnerabilities and their exploitation factors. It deserves a special mention Lagadec [16] that faces three downsides on current security tools: poor interoperability; hard to understand display of information; and lack of an overall picture. It advocates for the use of two interconnected tools, being developed in the realm of OTAN: CIAP (Consolidated Information Assurance Picture) in charge of information gathering from multiple sources and using sound standards, about network architecture, vulnerabilities, alerts and so on; and DRA (Dynamic Risk Assessment) that carries out an initial RA also using attack trees, and from then on is actively handling new inputs to update the assessment. It also suggests measures to adapt IS security to new risk exposure.

D. IS Security State Monitoring

Current trend in IS security management is SIEM (Security Information and Event Management) technologies adoption [24]. SIEM offers features such as log management, compliance reporting, real-time monitoring and incident management. SIEM architectures usually rely on IDS/IPS (Intrusion Detection/Prevention Systems) deployed all over the network, in order to trace malicious activity within. Information gathered may be useful for updating attack trees as already referred. Nevertheless it may become also valuable if used to methodologically reassess risk on real-time, based on changes detected and notified by those systems. This employment of DRA is a far more high-level management approach than attack trees, which are basically system administrator-oriented. Some authors [14] are prone to apply IDS/IPS architectures and Hidden Markov Models (HMM). Distributed IPS (DIPS) are customized to predict threat levels and update affected assets risk exposure by using fuzzy logic. The fact that DIPS monitor the network on a distributed architecture may improve threat prediction, assessing risk based on a given security status (Normal, Intrusion Attempt, Intrusion in Progress or Successful Attack). HMM characterize a dynamic system (similarly to dynamic Bayesian Networks) where future evolution only depends on its current state, regardless of the previous ones.

Mu [13] introduces a model called IDAM&IRS. It quantitatively assesses the risk in an intrusion scenario evaluating the target security state. Firstly, it filters and correlates alerts from IDS, then assesses assets risk state (considering volume, relevance, trustworthiness and typology of the alerts). Finally an administrator or automatic intrusion response system may use the assessment to provide better response decisions. Risk is computed based on the combination of different pieces of evidence in order to reduce uncertainty (D-S evidence theory).

Some works reuse cellular biology notions, such as Autonomic Defense Network (ADN) [25] that relies on the cooperative effort of security and monitoring devices distributed on the network. In Hu [15] several types of signals (alarm, discrimination or co-stimulation) are exchanged between devices or “analysis centers”, according to Danger Model which inspires the ADN concept. Specific combinations of these signals, released on the basis of network events, imply the existence of a real risk. By contrast when just one signal exists it means risk is in a transitional state.

There are approaches where risk is a function of operative factors, like resources availability. Intentional threats are let aside, taking into account that operational IS risks may also impact on business continuity, even with worse consequences than a purposeful attack. In [26] resources are dynamically assigned to computation tasks, according to the risk of non-compliance with a client SLA (Service Level Agreement). The model adapts to incidents such as node failure, unavailable staff or scheduling problems. Calculus and probability of node failure spreading is done with Bayesian statistical models, using Poisson processes and Gamma distribution. Fu [27] applies DRA to MANET Ad-hoc networks setup in line with their nodes’ risk exposure. It is done through attribute analysis over dynamic time sequence. Attributes used to assess risk, range from communication properties (loss tolerance, throughput or end-to-end delay) to physical ones (mobility, signal or location).

3.3 Dynamic Risk Treatment

A. Risk Optimization with Decision Trees

Trees can also be used for risk mitigation strategy selection after a change in the IS or its environment occurs. Trees don't reflect risk related to an attack anymore. Instead they show the most effective mitigation path to follow, in order to minimize the impact caused by a known alteration. Beaudoin [28] illustrate an example of this trees application showing how a new vulnerability could be treated most effectively and prospectively avoiding its future exploit. There are paths moving along different available actions that are applied at moments in time. Best sequence of actions to follow is the one (or alternative ones) that ends in the lower risk node. Generation of decision trees might require a supervised learning process (Reinforcement Learning) leaning on Neural Networks.

B. Automated Incident Response Based on Risk Perception

Incident detection through IDS/IPS (or whatever other security system) should ideally be followed by an effective and immediate reaction whenever possible. Automation of that reaction is the aim of Automated Intrusion Response Systems (AIRS) [13]. The main difficulty has proven to be the capability of guaranteeing a more effective response than the human one. Response given by an analyst or administrator, in place of the AIRS, is a priori supposed to count on a richer contextualization. AIRS development tries to beat that human ability. Gehani [29] presents RheoStat method, conceived to automatically react to IDS alerts, by means of system execution authorization restrictions, based on perceived risk. These restrictions are applied to process affected by the attack.

Automated response to events has to deal with an important weakness such as false positives treatment. Measures applied on the basis of a false security incident could lead to a waste of resources, or even have an undesired impact on business objectives. Some efforts [30] try to avoid this setback by implementing the so-called fusion model that passes through three consecutive phases or levels: first one is an online alert fusion algorithm that reduces redundancy of alerts in order to find the root cause of the incident; the second one handles with uncertainty factors to get a more accurate assessment; and the last level dynamically evaluates the network risk applying HMM.

4 CONCLUSIONS AND FUTURE WORK

There are several approaches trying to face challenges in DRA and Dynamic Risk Management, with different points of view. They tend to focus on some specific dilemma letting other important hints unattended, though some currents try to afford the problem on a holistic approach. Ideally, all changes happening to the IS as well as those affecting its environment should be taken into account when re-assessing the risk, in order to be complete and effective.

In a number of the previously analyzed works, especially the ones involving Attack Trees/Graphs, DRA is conceived as an analysis of attack dynamics based on predefined scenarios. Notwithstanding, this approach might be improved integrating RA tools with real-time events monitoring tools, and ultimately automating response measures in line with RM policies. From an IS point of view, IDS and IPS are the most spread tools offering features that will allow a real-time monitoring of networks to be achieved. Indeed, they sometimes offer their own assessment of risk, linked to detected events. The main drawback is the narrow understanding of the whole IS and its global environment, these systems usually have. On the other hand, tools implementing methodological RA tend to capture a higher level picture of the IS domain that allows decision-making in alignment with Organizational objectives, security policies, etc. Eventually, integration of DRA in a security dashboard could also be achieved, which would bring the IS risk monitoring, and decision-making related to it (based on real-time RA), closer to Management in the unfortunate event of a crisis scenario. The aforementioned integration, requires RA tools to be fed with continuous inputs about IS security status, as depicted in Fig. 2.

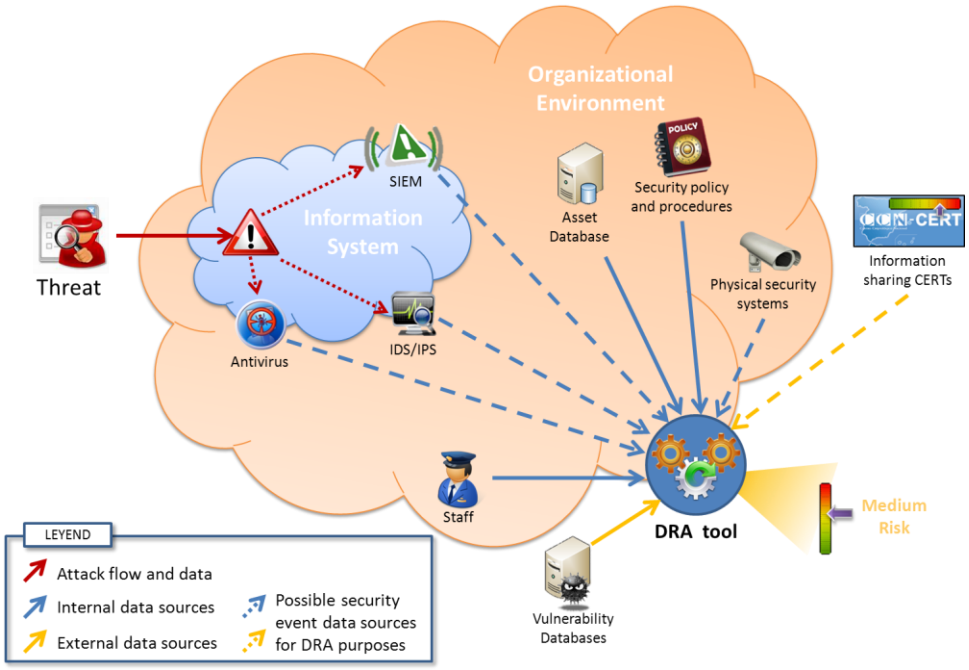

Fig. 2 Dynamic Risk Assessment integrating security systems with DRA tool on real-time

These inputs are to be notified by security tools (adequately pre-screened to avoid an overload of the RA tool) by means of communication interfaces and data models commonly understood and implemented. It may also be useful to consider, integration of physical protection systems (physical IDS, fire detection systems, etc.) in the IS RA process, due to potential attack vectors that may not require a "logical" compromise of systems and networks, or that may comprise an important physical threat component such as theft or destruction, thus falling out of the scope of conventional IS security tools. Finally, risk evaluation might take advantage of the greatest possible quantity of sources, and profit from the exchange and cooperation regarding incident, threat and vulnerability knowledgebase sharing.

Future work will be focused on the development of integration solutions that may allow DRA tools to be fed with added real-time information sources, in order to improve RA accuracy. Solutions may include information sharing data models, and definition of new available input sources for DRA tools.

ACKNOWLEDGMENTS

This work was supported by the Agencia Española de Cooperación Internacional para el Desarrollo (AECID, Spain) through Acción Integrada MAEC-AECID MEDITERRÁNEO A1/037528/11.

References

[1] ISO/IEC 31000:2009 Risk management - Principles and guidelines, 2009.

[2] ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management, 2011.

[3] Ministerio de Administraciones Públicas (MAP). España: MAGERIT versión 3 – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I Método, 2012.

[4] C. Alberts, A. Dorofee: Managing Information Security Risk. The OCTAVE Approach. Addison Wesley, 2005.

[5] Siemens - Insight Consulting: The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures, 2005.

[6] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). France : EBIOS 2010 - Expression des Besoins et Identification des Objectifs de Sécurité. Méthode de Gestion des Risques, 2010.

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI) Deutschland: IT Baseline Protection Manual, 2000.

[8] G. Stoneburner, A. Goguen, and A. Feringa: Risk Management Guide for Information Technology Systems. NIST *Special Publication 800-30*, 2002.

[9] Technical Department of ENISA, Section Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. *European Network and Information Security Agency (ENISA)*, available at: http://rm-inv.enisa.europa.eu, 2006.

[10] ISO/IEC 27001:2005 Information Technology - Security Techniques - Information security Management Systems - Requirements, 2005.

[11] NIST: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. *NIST Special Publication 800-37*, rev. 1, 2010.

[12] W. Qi, X. Liu, J. Zhang, W. Yuan: Dynamic Assessment and VaR-Based Quantification of Information Security Risk. *In Proceedings of the 2nd International Conference on e-Business and Information System Security (EBISS)*, pp. 1-4, May 22-23, 2010.

[13] C.P. Mu, X.J. Li, H.K. Huang, S.F. Tian: Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory. *In Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, pp. 35-48, 2008.

[14] K. Haslum, A. Abraham, S.J. Knapskog: DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment. *In Proceedings of the 3rd International Symposium on Information Assurance and Security (IAS)*, pp.183-190, 2007.

[15] Z.H. Hu, Y.S. Ding, J.W. Huang: Knowledge Based Framework for Real-Time Risk Assessment of Information Security Inspired by Danger Model. *In Proceedings of the International Conference on Security Technology*, pp. 91-94, 2008.

[16] P. Lagadec : Visualization et Analyse de Risque Dynamique pour la Cyber-Défense. *In Proceedings of the Symposium Sur la Sécurité des Technologies de l'information et des Communications (SSTIC)*, 2010.

[17] NIST: National Vulnerability Database. Available from: http://nvd.nist.gov.

[18] P.A.S. Ralstona, J.H. Grahamb, J.L. Hiebb: Cyber Security Risk Assessment for SCADA and DCS Networks. *ISA Transactions Information Assurance and Security (IAS)*, Vol. 46, pp. 583-594, 2007.

[19] D. Fernández, O. Pastor, S. Brown, E. Reid, C. Spirito: Conceptual framework for cyber defense information sharing within trust relationships. *In Proceedings of the Fourth International Conference on Cyber Conflict (CYCON)*, pp. 1-17, Jun. 2012.

[20] N. Poolsappasit, R. Dewri, I. Ray: Dynamic Security Risk Management Using Bayesian Attack Graphs. *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 1, pp. 61-74, 2012.

[21] Y. Haimes, J. Santos, K. Crowther, M. Henry, C. Lian, Z. Yan: Risk Analysis in Interdependent Infrastructures. *Critical Infrastructure Protection*, pp. 297-310, 2007.

[22] R. Dantu, P. Kolan, R. Akl, K. Loper: Classification of Attributes and Behavior in Risk Management Using Bayesian Networks. *IEEE Transactions Intelligence and Security Informatics*, pp. 71-74, 2007.

[23] M. Henry, Y. Haimes: A Comprehensive Network Security Risk Model for Process Control Networks*. Risk Analysis*, Vol. 29, No. 2, pp. 223–248, 2009.

[24] M. Nicolett, K.M. Kavanagh: Magic Quadrant for Security Information and Event Management (SIEM). *Gartner Research*, publication No. G00176034, May. 2011.

[25] M. Swimmer: Using the Danger Model of Immune Systems for Distributed Defense in Modern Data Networks. *Computer Networks*, Vol. 51, pp. 1315-1333, 2007.

[26] K. Voss, Ch. Carlsson, A. Akademi: Consultant Service and Dynamic Risk Assessment. *IST-AssessGrid project (WP.3)*, Sixth Framework Programme, 2008.

[27] C. Fu, J. Ye, L. Zhang, Y. Zhang, H. LanSheng: A Dynamic Risk Assessment Framework Using Principle Component Analysis with Projection Pursuit in Ad Hoc Networks. *In Proceedings of the Seventh International Conference on Ubiquitous Intelligence & Computing and Autonomic & Trusted Computing (UIC/ATC)*, pp. 154-159, Oct. 2010.

[28] L. Beaudoin, N. Japkowicz, S. Matwin: Autonomic Computer Network Defence Using Risk State and Reinforcement Learning. *Cryptology & Information Security Series*, Vol. 3, pp. 238-248, 2009.

[29] A. Gehani, and G. Kedem: RheoStat: Real-time Risk Management. *In Proceedings of the Seventh International Symposium on Recent Advances in Intrusion Detection*, pp. 15-17, 2004.

[30] J. Ma, Z. Li, and H. Zhang: A Fusion Model for Network Threat Identification and Risk Assessment. *In Proceedings of the International Conference on Artificial Intelligence and Computational Intelligence (AICI)*, Vol. 1, pp. 314-318, Nov. 2009.