ISSN: 2617-2070 (Print) ; 2617-2070 (Online)
Journal of Advanced Sciences and Engineering Technologies
Available online at: http://www.jaset.isnra.org

Journal of Advanced Sciences and Eng. Technologies
JASET

Risk and Vulnerability Analyses for the protection of Information for Future communication security Based Neural Networks

Al-Khawaldeh Igried[1]

Hassan Al_Wahshat[2]

Bashar Igried [3]

Al Smadi Kalid

[1] Department of Communications and Electronics Engineering, College of Engineering, Jerash University

dsmadi@rambler.ru

[3]Management Information Systems Department, Ajloun National University

[2]The Hashemite University,Faculty of Prince AlHussein Bin Abdullah For Information Technology

Keywords
Risk analysis
vulnerability validation
attack tree
artificial neural networks

ARTICLEINFO

Article history:
Received 01 august 2018
Accepted 20 august2018
Available online 02 febuary 2019

DOI: DOI:
http://www.doi.org/10.32441/jaset.02.01.03

Copyright © 2018 by author(s) and This work is licensed under the CreativeCommons Attribution InternationalLicense (CC BY 4.0).http://creativecommons.org/licenses/by/4.0/

ABSTRACT

Information security risk analysis has increased the number of complex issues of information security, requiring the participation of specialists in different areas of knowledge. This leads to inability of such systems to evaluate the security state of computer system thoroughly.
Present paper on the intellectual to risk analysis and vulnerability of information systems. The aim of the study is to eliminate subjectivity in the assessment of risks and reduction of time for the process of risk analysis and vulnerability of the computer system. The mathematical tools of artificial neural network and probabilistic attack tree were used in the research. In order to evaluate the efficiency of the developed system, the security assessment for the Windows systems was performed. As the result the conformity between the real security of the information system and the assigned evaluations was proved.

© 2018 JASET, International Scholars and Researchers Association

Journal of Advanced Sciences and Engineering Technologies Journal of Advanced Sciences and Engineering Technologies

Introduction

Use of information systems linked to a particular set of risks, the vulnerability of information technologies and systems. When the risk becomes unacceptably large, modern system of analysis and risk management, are based on very subjective expert opinions or suggest the use of special questionnaires on issues that often have to be incompetent persons. In this case, even the use of mathematically sophisticated algorithms to analyze the data will not help to improve the quality of these assessments. the vast majority of systems is focused on an integrated approach to risk analysis and Managements when an integrated approach addresses the many redundant for analysis of system factors because it takes into account not only the technical scope of the Organization, and consequently, Ana-Lisa threat level directly to the computer part that any activity of the company, has been neglected. In this paper, the proposed method and software system for mining risks and vulnerabilities of inter-information systems based on the use of probabilistic graphs and mathematical apparatus of artificial neural networks and using the real data on the State of the system[1][2].

RELATED WORKS ON INFORMATION SECURITY RISK ASSESSMENT

Traditionally, the risk associated with a particular event can be defined as:

-Risk Incident = (Probability of the incident) x (Impact caused by the incident) although it is nice to write formulas that describe risk in many situations, this formula is not useful. Although this is usually easy (if tedious) to assess the potential damage caused by a hypothetical case, it's not always obvious how to find a value for the probability of an incident of the term. The meaning of the term (usually expressed as a number between 0 and 1) is the result of many

Factors, some of which may not easily be quantified, the developed method to quantify the risks, estimate the probability of a successful implementation of the information system vulnerabilities, as well as to conduct an audit found vulnerabilities, taking into account the assigned ratings and generate recommendations for reducing and eliminating valid risk. The developed method allows you to quantify the risk Existing methods and tools the vast majority of risk analysis and management systems are Complex and are generally expert systems and specialized surveys, complemented by a sophisticated means of mathematical analysis of entered data. Among the systems and techniques that focus on risk analysis of computer systems are the following:

Method and system of Risk Watch

Software system of Risk Watch [3] is designed to conduct risk analysis and selection of sound measures and remedies. The system uses methodology that consists of four phases.

The definition of the subject of the study this stage the system is a set of input parameters. Among them: the type of research organization, the composition of the research system, and the basic requirements of business enterprises in the field of security. Inside the system description of input parameters-the ditch in a certain way is formalized and adopted by the formalization provides further detail of parameters entered. Risk Watch contains a set of templates that include Ka-category, as protected by the resources of the Organization, the potential loss, typical threats and vulnerabilities,

potential protective measures, of which the operator is requested to select the ones for the Organization, are critical. It is the ability to add new categories, as well as modifications of existing ones. Making data specifying the currentstate of the system, you can import the data from the reports of research of vulnerabilities, or entered manually. At this point, potential data vulnerabilities are defined using a questionnaire containing more than600 questions, and are determined by the frequency of occurrence of each of the standards set out in the previous step, criticality, degree of vulnerability threats and valuable resources. This information is then used to calculate the effectiveness of protection.

Risk assessment at this point, after the establishment of links between the threats and losses calculated mathematical expectation of losses for the year, the value of which is accepted as a risk. On the last stage of work, the system generates the reports. The advantages of this method include the following: the method of risk analysis is sufficiently flexible and simple, and the complexity of work is relatively small [4].

Among the main shortcomings is the method of calculating the risk assessments-mathematical-economic expectation of loss for the year is not an acceptable grade for any of the assessed risks.

b) Technique of OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation)conduct risk assessment methodology in an organization, developed [5].For the evaluation of potential incidents in the area of security and the development of adequate countermeasures technique developers offer POPs-give a team made up entirely of members of the organization. With special emphasis on the fact that all the analysis takes place without the participation of third-party expert's and of advisory companies in the field, i.e. directly by the organization.

OCTAVE includes three phases of analysis:

Develop profile of enterprise critical threats. For a description of the profile is to use the so-called "trees" options that enable you to provide a combination of threats and resource in formalized-the therapeutic form; Identify infrastructure vulnerabilities. At this stage the definition was the infrastructure that supports the selected at the previous stage of the vulnerabilities, and examines the technical components of the system, such as, for example, servers and personal computers, which are then scanned for vulnerabilities using security scanners; Development of strategies and plans to ensure security. This STA-Diya includes risk assessment, which is conducted on the basis of the reports of the two previous stages, and is only an estimate of the expected damage, without an assessment of probability on a scale of high, intermediate (mid-dle), low (low); and risk reduction plans, together with the identification of measures to counter the threats. The strength of the OCTAVE is the high degree of flexibility in adapting the methodology under the need of a particular company, achieved thanks to possible self-selection criteria. The disadvantages include a high degree of human intervention that invariably leads to personal's evaluation. The methodology is developed mainly for use in large companies [5][6].

Information security risk assessment models and process

Modern of the effective risk shows the process for information security risk assessment Figure 1. It includes the preparation of a risk assessment, identification of assets, threat identification, and vulnerability Identification and calculation of risk and other stages. It can be divided into six steps in Specification of the operation [7].

-Step 1: determine the object of evaluation: defining data information system, hardware, software Assets give the system functions, borders, critical assets and assets and determine Scope of the evaluation.

-Step 2: assess performance: develop a plan for evaluation in accordance with requirements, define the evaluation process, and select the appropriate assessment methods and tools, and systems.

-Step 3: identify the risk: identification of critical assets and total assets under Evaluation and threat detection in the operating environment and the vulnerability of assets to their own existence, and existing security measures.

-Step 4: risk analysis: combined property assets, analyzes the possibility and consequences of threats, vulnerability and used to calculate the results of the evaluation, Analysis of the effectiveness and reasonable security measures.

-Step 5: risk assessment: toevaluate the results; educate risk assessment report, combined with expert opinion.

Step 6: risk control: according to the instructions require to take effective measures to avoid or reduce the risk so as to effectively monitor systemic risk [8].

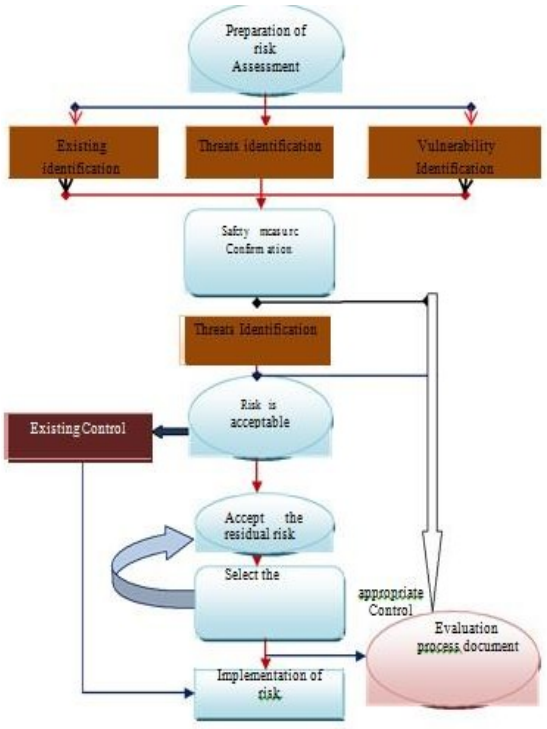

Fig.1: The process of the information security risk assessment

METHOD OF ANALYSIS OF RISKS VULNERABILITIES:

Tree-based model the structure previously used as fault trees. However, their last use of the spread in the area of risk analysis, Attack of the model tree that is very good at assessing risk in situations where these

Multistep and premeditated malicious activities, Attack of the tree is used for the identification and

analysis of potential threats, expressed in the site hierarchy, allowing decomposition abstract attack a

number of more specific steps attack [9]. Attacks are usually modeled using graphical, mathematical, decision tree

structure called the attack tree. In the field of information systems to attack trees recently have been used in various areas of software security and threat analysis from malicious Insiders [10].

In the various studies, it was observed that the requirements and scalability is a critical issue for the trees attack and attack graphs [11]. As a result of these scalability issues using attack trees in real-

World scenarios for large enterprises become impossible. In addition to small and medium-sized enterprise level the necessary level of resources (staff and monetary) prohibit their use. Thus it is the scalability and the effort and time to head over to issue presents a major obstacle in making the attack tree based on the information security evaluation methods.

The method can be described as follows:

Receiving information the investigated system-family, version, service pack and list and banner services. osInf = {S, Ver, SP, serv, servB},

S-family of OPERATING SYSTEMS; Ver = {ver_i} is a finite set (k.m.) suspected OS versions; SP = {sp_i}-k.m. alleged service pack OPERATING

SYSTEM; serv = {serv_i}, k.m.Services; servB = {servB_i}-k.m. banner services.

Obtaining information about vulnerabilities. vulnInf = {vuln_i}, Where; vuln_i is the estimated vulnerability.

building the tree attacks for the target system. The tree nodes are exploits, rib-risk assessment for each individual sheet of wood (exploit). Tree includes all possible exploits for this operating system.

G = (V, E),

Where V is the set of vertices: V = {exp_i}, exp_i is a valid exploit: exp_i = F (osInf, vulnInf);E is

the number of edges: E = {Ri}, Ri — risk assessment for the i- of the exploit.

Building the tree is done using heuristic algorithm based on information about the vulnerabilities of the system. In particular, if an exploit might work without preconditions, it is placed in a node-set to 1 (on the following for the root level of the tree). If there's a successful exploit requires of fires at some preconditions, it is placed in the root of the sub tree, which is implementing the US-terms site [12].

4) Is a risk assessment for each selected exploit, taking into account the information about the operating system {osInf | vulnInf}. Risk assessment in this case is quantitative and is the probability of successful activation exploit.

To obtain a probability estimates can be used various techniques, such as a table. To resolve this problem, use the generalizing neural capabilities CE-TI. Risk calculation is as follows:

Ri = neuronet(norm Rank, confRef, confTarget),

5) Build sequences of exploits. who can get an attacker in performing exploits from the chain.

In Figure.2 The proposed model rules to build and traverse the tree, it could be argued that crawls all

valid vertexes will be made of wood, which can work on this method, you can calculate

the probability that all relevant to your system exploits are found for the specified number of steps.

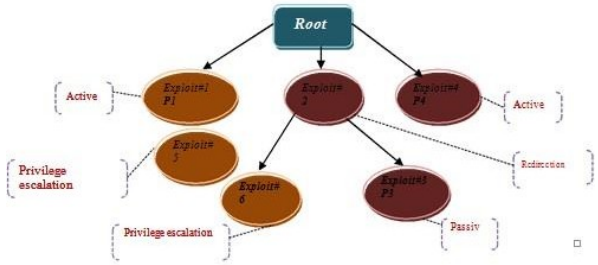

Fig.2 : The proposed model rules to build and traverse the tree

To meet the challenge of generating response probabilities exploits was selected artificial neural network based on radial basis functions, the network is the vector properties associated with the State of the tree.

THE ARCHITECTURE OF THE SYSTEM

Designed system includes the following cooperating components: vulnerability Nessus Security Scanner, Metasploit Framework System Server and Analyzer developed in Mat lab and communicates with other components of the system.

USING KNOWLEDGE TO DETECT ATTACKS ON THE INFORMATION SYSTEM:

Information security threats are usually somehow interlinked with each other. For example, the threat to capture a vulnerable Web server host can lead to the threat of the seizure of control of the site, so in order to anticipate and assess the situation, to take into account the probabilistic relationship threats.

If U is a set of threats to the security of the information system, the ui of U-i-I'm a threat. Under the

assumption that many threats,of course, we will consider that the implementation of the i-th threats can have a chance to lead to the possibility of other threats. This raises the challenge

of calculating P (ui1, ui2 u|,..., uik) is the probability of the threat u, assuming threats ui1, ui2,..., uik (see

Figure 3).

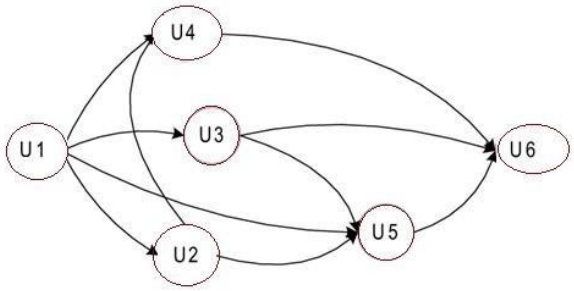

Fig.3: graph based on Information Security Risk

The most reliable attack can be detected by having the fullest possible information about the event. As you can see from the preceding sections, modern systems often record the presence of a specific attack, it

is a specific signature. Analysis of the relationship with the phases of attack threats and predicting the most likely threats

that could be carried out by an attacker is an important task to ensure Information Security. This is

necessary for timely decision-making by blocking malicious attacks.

The next element of the concept of attack detection is the classification. Classification of computer attacks still actively investigated. The main task of developing the classification of computer attacks is to

Ensure the usability of this classification in practice. The main requirements for the classification are disjoint classes, completeness, applicability, integrity, scalability, limb. Interesting approaches to classification network, Classification of threats to security should take into account the structure and

phase of attacks on computer systems, define attributes such as sources and targets of attack, their advantages, multi-level typing. Intrusion detection model must be built on the basis of classification. Thus, the following tasks must be run to determine the most probable of the threat at the moment to have an idea of what the consequences might expect in the shortest possible time, information system, as well as predicting the evolution of the situation with a view to identifying the

Most probable the threats in the future [13].

RISK ANALYSIS

Using the matrix Where the axis reflects the major changes, the variables to be associated meaningfully with each other, Figure 4 is a matrix for the risk analysis of the battle a low risk/high trust and area, high risk/low zone of confidence: where: X represents the data value (cost data); the y-axis represents the history of services (provider's history), and the Z axis represents the location data (data location).

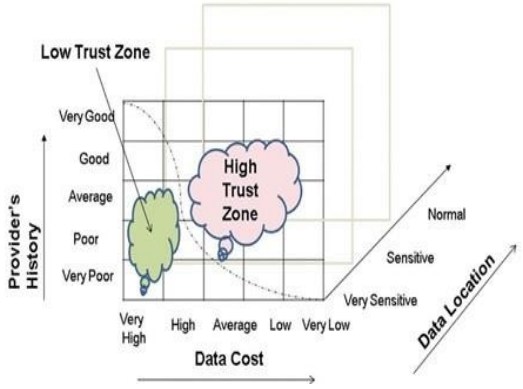

Fig.4: Matrix for risk analysis

Security risks to current operations, as well as for future transactions with the service provider. As a preventive approach to risk assessment is seen as part of the Pro-friendly handbook on how to measure or reactive. For example, the added level of authentication and/or verification can be used for activity that is associated with the zone of low confidence. This method can be used to measure trust and for all future transactions. Based on this method, you can determine the trust, for all future transactions with the service provider. According to provide IDC (International Data Corporation), cloud services are still in an early stage of development. In a number of research gives an overview of known cryptography-related tools to ensure the integrity and consistency of the data stored in the cloud. Some software and hardware solutions to provide continued testing on some of the required data in real time, in the technical

description on AWS (Amazon Web Services) discusses physical security, backup and CEP-in their context, Similarly, other providers, such as Google, Microsoft and others discussed issues of security in the cloud computers Ing to use the infrastructure of cloud computing. In ad to these seven risks, we also identified several other major factors that must be considered providers of cloud

services. These issues include data storage, server security, privileged access users, virtualization, and data portability. Some ideas for modeling trust is invited to identify a core set of change-tonal trust, which may be highly beneficial for the matrix based on issues-SAH in cloud computing security [14].

CONCLUSION

For each of the systems of all the confirmed vulnerabilities were a group of high risk levels assigned system, which proves the efficiency of the system in the appointment of probabilistic risk assessments, as well as its ability to reduce the time the analysis of risks and vulnerabilities to the minimum. In accordance with the results of the research system has a number of advantages over existing means:

-Analyzes and takes into account the real information about the operating system and the operational services of the information system. Calculates risk levels for exploits and implementation of validated found vulnerabilities in accordance with assigned levels (most critical exploits are checked first). Provides a Visual display of how attacks, generates solutions to vulnerabilities and risks. The particular concept of risk management, In each specific case have to adapt the common methodology of risk analysis and management for specific needs of the enterprise, taking into account the specifics of its operation and the conduct of business. Let's look first at the common questions and problems that arise when developing such methodologies, possible approaches to address these issues, and then discuss examples of adaptation and development of relevant corporate procedures.

ACKNOWLEDGEMENTS

The authors are thankful to the AL-Balqa Applied University for their support and to Jerash University by using their Laboratories and premises, our thanks to reviewers for their valuable suggestions to enhance the quality of our article

REFERANCES

[1]. Al Smadi Takialddin, K. A. S., & Orayb, O. AL-Smadi, High-Speed for Data Transmission in GSM Networks Based on Cognitive Radio. American Journal of Engineering and Applied Sciences, 10(1), 69-77.

[2].Camtepe S. A., Yener B. A Formal Method for Attack Modeling and Detection // TR-06-01, Rensselaer Polytechnic Institute, Computer Science Department. 2006. URL: http://citeseer.ist.psu.edu/751069.html (15.03.2012).

[3].Sheyner O., Haines J., Jha S., Lippmann R., Wing J. M. Automated Generation and Analysis of Attack Graphs // Proceedings of the IEEE Symposium on Security and Privacy. Oakland, CA, USA, 2002. P. 273–284.

[4]. Ghaidan, K. A., Al Smadi, T. A., Aljumailly, T. A., & Al-Taweel, F. M. (2011). Development of a new approach for transmitting Digital message on a Frequency Limited Communication Channel transmission. Journal of Advanced Computer Science and Technology Research, 1, 52-62.

[5] Hussein, A. L., Trad, E., & Al Smadi, T. (2018). Proactive algorithm dynamic mobile structure of Routing protocols of ad hoc networks. IJCSNS, 18(10), 86.

[6].Xiao M, Fan S. X, Wu Z. (2009), —A threat-centric model for information security risk assessment, Journal of Wuhan University of Technology, Vol. 31, No. 18, pp. 43-45.

[7]. Yang Y, Yao S. Z.(2009), ―Risk assessment method of information security based on threat analysis‖.Computer Engineering and Applications, Vol. 45, No. 3, pp. 94-96.

[8].Yazar Z. A (2011), Qualitative risk analysis and management tool – CRAMM, SANS Institute InfoSec Reading Room. 2011.

[9] Al-Sawalha, A., & Al Smadi, T. (2018). Microstrip Patch Antenna Radiation Variation of Quality Factors and Bandwidth of a Conically Depressed. Journal of Advanced Sciences and Engineering Technologies, 1(1), 7.

[10]. Xinlan, Z., Zhifang, H., Guangfu, W., & Xin, Z. (2010, December). Information security risk assessment methodology research: Group decision making and analytic hierarchy process. In 2010 Second world congress on software engineering (Vol. 2, pp. 157-160). IEEE.

[11].56. Zhao D, Liu J, Zhang Z. (2009), ―Method of risk evaluation of information security based on neuralnetwork‖. IEEE international Conference on Machine Learning and Cybernetics, Vol. 1, No. 6,pp.1127-1132.

[12].Kijo, H. and Luo, J. (2012), ― Analysis on the competitiveness of Chinese steel and the southKorean‖, Software Computing in Information Communication Technology, Vol. 2, No. 1, pp. 451460.

[13].Manadhata, P. K., Karabulat, Y., & Wing, J. M. (n.d.). Report: Measuring the attack surfaces of enterprise software. Retrieved December 29, 2011, from Carnegie Mellon: School of Computer Science.

[14]. Al Smadi Takialddin, O. I. A., & Agha, K. A. A. (2018). Overview of Model Free Adaptive (MFA) Control Technology, Vol.7, No.4, December2018, pp. 165~169. http://doi.org/10.11591/ijai.v7.i4.pp165-169

[15]. Al-Wahshat, H., Al-Maitah, M., & Al-Smadi, T. (2017). Voice Quality for Internet Protocol Based on Neural Network Model. *Journal of Signal and Information Processing*, *8*(04), 195. https://doi.org/10.4236/jsip.2017.84013