International Journal of Research in Social Sciences
Vol. 7 Issue 4, April 2017,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A SECURITY ANALYSIS TO BE TECHNOLOGY ARCHITECTURE FOR MINISTRY OF REGIONAL MUNICIPALITIES AND WATER RESOURCES (MRMWR) SULTANATE OF OMAN

BoumedyenShannaq[*]

Richmond Adebiaye[**]

Abstract

The proposed work developed critical strategy to solve basic problem; the Violation performance of individual services by constructing attack graphs, and automatic extraction and verification (analysis) properties of this graph allows to partially solve such problems .Furthermore describes the security architecture, processes and organization structure of security analysis system (SAS), for the Ministry of Regional Municipalities and Water Resources (MRMWR) in sultanate of Oman. The proposed architecture is derived based on the current state assessment of the IT infrastructure, the future strategic direction and leading practices principles that consider the development of architecture, models and security analysis system (SAS), based on the formation of attack graph and the calculation of a variety of security metrics.

Keywords:

Security analysis;

Security architecture;

Models and security;

Attack graph;

Security metrics.

[*] **Dr. Boumedyen Shannaq Ministry of Regional Municipalities and Water Resources ,Sultanate of Oman**

1. Introduction

The Ministry of Regional Municipalities and Water Resources (MRMWR) wishes to develop an IT Strategic Plan for the next five (5) years which will help the management align IT objectives & goals to the Ministry and eOmanobjectives & goals and align with IT leading practices. Security is a key domain which have to take into account while developing the IT applications, services, platforms, infrastructure and managementfunctions [1] .The proposed work focus to design general architecture to improve security analysis based on defense analysis at the stage of designing computer networks. One of the basic requirements to develop procedures of security analysis sensitivity is to develop network configuration and implemented security policies [2]. Considering, damage of information security in computer networks, It can be caused by many different factors: the existence of vulnerabilities operating systems (OS) and applications; incorrect configuration of hardware and software ; errors made when setting access control; presence of vulnerable or easily attacked services and malicious software, etc. Using a combination of existing vulnerabilities and weaknesses in network configuration and the applied security policy , violators (Both external and internal), depending on their goals, may to implement a variety of attack strategies. These strategies aimed at various critical network resources and include multistep chain attack. As part of these chains it can be compromised different hosts and different implementation on personal security threats[3].

2. Problem Definition

The design and operation of network [4],basically initiating a big challenge for verifying whether the planned development mechanisms such as network configuration, security policy and protection mechanisms are the correct required level of security. Moreover, in step of operation computer networks quite often there is a change in its configuration and composition , particularly When using software and hardware , so it should be constantly intelligent mechanism to monitor the network, i.e. analysis of existing vulnerabilities and assess the level of security .

During the design phase the main source of data for security analysis process , are the specifications of the designed network considering the security policy, and the operational phase – i.e. the actual parameters of the network.Figure 1 describes the main scope of security needs

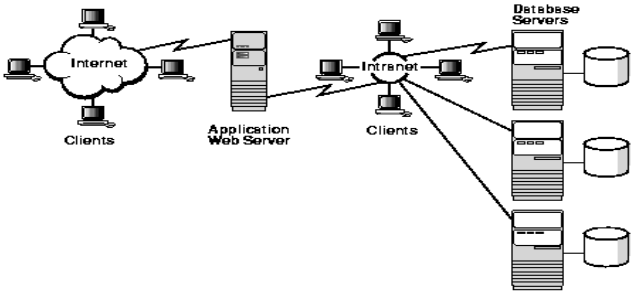


Figure 1.*Scope of Data Security Needs[5]*

The increasing complexity of computer networking and security mechanisms [5], increase the number of vulnerabilities and potential errors in their use, as well as opportunities for the implementation of the attacks necessitates, the development of powerful automated tools (systems) security analysis. These systems are designed to perform tasks for detecting and correcting errors in a network configuration, the identification of possible attack paths of various categories of offenders (On the implementation of the various security threats), the definition of critical network resources and the selection of adequate security threats policy that uses the most appropriate in the given circumstances defense mechanisms[6][7].

At the design stage the proposed work used a variety of methods of security analysis and determine the overall level of security, for example, based on quantitative and qualitative basis risk analysis techniques, including on the basis of a mathematical apparatus ; Probability Theory, Bayesian networks, possibility theory, fuzzy sets [8,9,10,11], and so on. A promising trend in the level of assessment security approaches are based on the construction representation possible actions violators as trees or graphs attacks and subsequent verification of the properties of the tree (graph) based on the use of various methods, such as methods for verification model (Checking model), as well as the calculation on the basis of the presentation of various security metrics.

3. Proposed Solution

Vulnerability analysis can be performed by passive and active methods for vulnerability analysis[12]. Passive methods implemented on the basis of the analysis of event logs, settings software and hardware and so on. Active methods are reduced to "Testing Network penetration", which is performed by implementation of various attack. Passive methods do not allow us to estimate the possible route of penetration of offenders, such methods cannot always be used, since they lead to a violation performance of individual services or the entire system. Combination passive method (to obtain relevant data on the current configuration and implementation security policy), procedures constructing attack graphs, and automatic extraction and verification (analysis) properties of this graph allows to partially solve such problems.

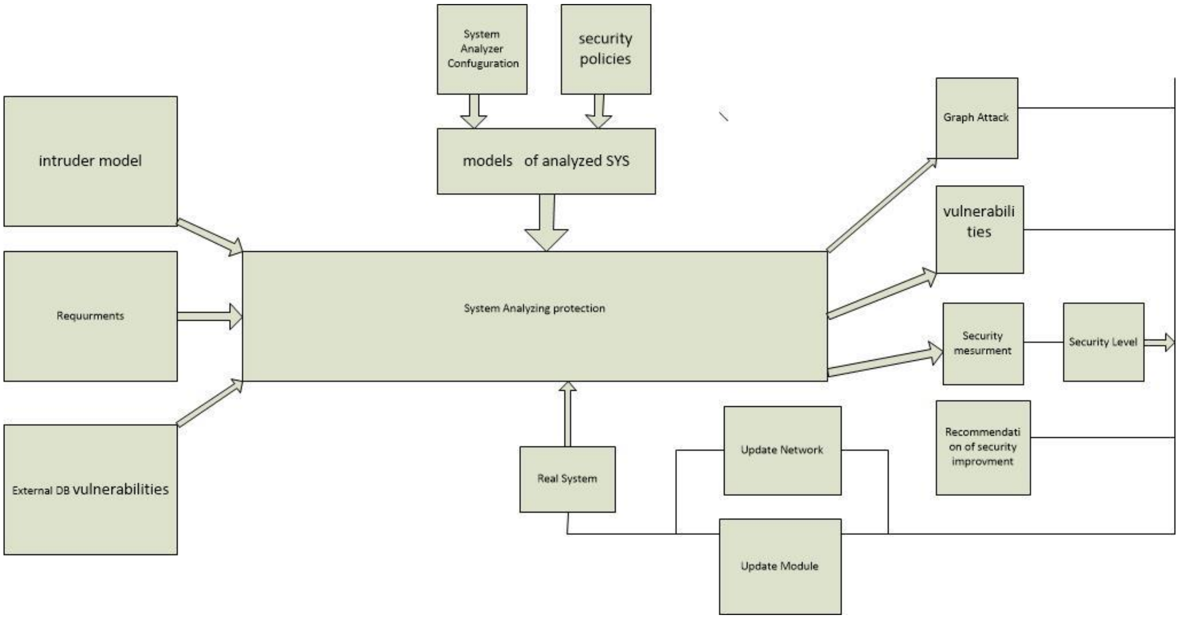
currently there are a lot of research done on the development of methods, techniques and analysis of security systems ,Proposed in this work , an approach to security analysis in computer networks is based on a thorough analysis of possible violators of action for the implementation of the various security threats and violations of construction of graphs of these actions Total attack graph describes the various embodiments of the intruder attack. It is assumed that such a graph is based on modeling violator given network configuration and Rules implemented security policies, as well as the goals, the level of knowledge and skills, as well as the diversity of the offender location that allows explore how the actions of external and internal intruders.

Thus, this work propose the implementation of a detailed assessment of the security techniques based on the analysis of attack scenarios and the processes occurring in the test network.

This approach allows security team to assess the level of protection computer networks in an environment where there is no possibility to obtain information about all aspects of their operation. Analysis in terms of resistance to hacking attempts can also supplement the results of the analysis of specific examples of the base security, and allows to focus on the private and the most important aspects of the individual applications.

The main difference in the approach proposed by other research approaches is in the process of constructing attack graph (used multi-level, hierarchical view of the attacker's action strategies) and use of a common attack graph constructed to define a family of different indicators (metrics) security,Intended for the qualitative analysis of a given network configuration and implementation current security policy.

Security analysis system using the proposed approach is designed to function at different stages of the network lifecycle, including the phases of design and operation (Fig. 2).



Figuer2. General representation of analysis of security systems

4.The architecture of security analysis system

The proposed SAS architecture which projected for action during the design and maintenance of computer networks, is presented in Fig. 3.

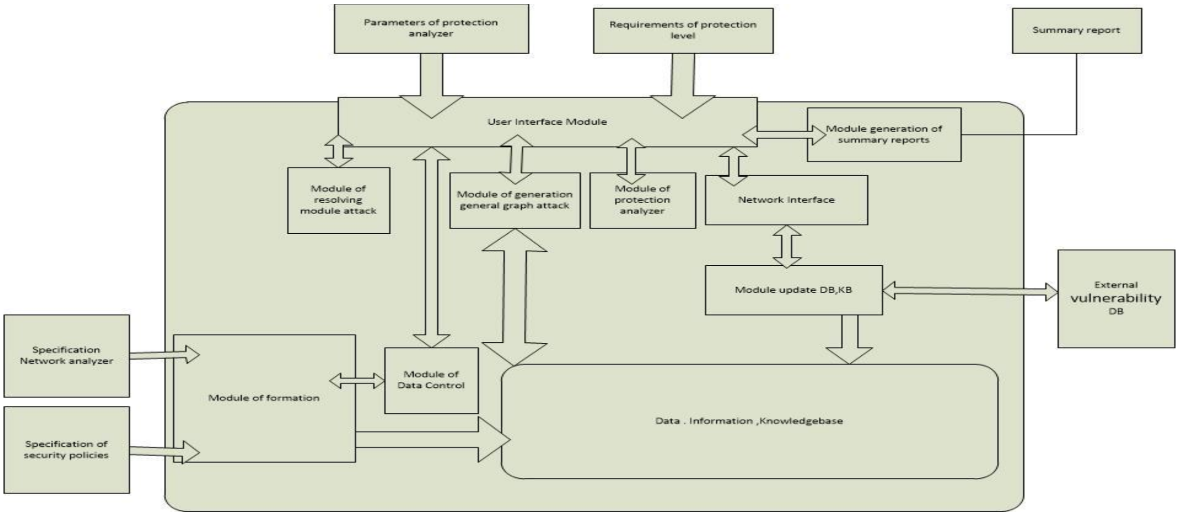

Parameters of protection analyzer
Requirements of protection level
Summary report
User Interface Module
Module generation of summary reports
Module of resolving module attack
Module of generation general graph attack
Module of protection analyzer
Network Interface
Module update DB,KB
External vulnerability DB
Specification Network analyzer
Specification of security policies
Module of formation
Module of Data Control
Data . Information ,Knowledgebase

Figure 3.General architecture of SAS

SAS includes the following elements: a user interface module; a network interface; module of the internal representation of the models analyzed network and security policies; data control unit; data store; module updates the database (DB) and knowledge bases(KB); generating unit of general attack graph; module implementation intruder model; Module security analysis; reporting module.

During the design phase, SAS operates with a model of analyzed computer network that is based on predetermined specifications analogous of analyzed network configuration and network security policy.

During the operational phase for the construction of the analyzed network model , used subsystem of collecting information on the analyzed computer network, consisting of the following components: The various data sources (host software agents, security units of information system components containing security settings, proactive security monitoring components); Assembling information.

Considering the function of the main modules of the proposed SAS, user interface module allows the user (administrator, designer) to control the operation of all system components, the input data set, view reports on security analysis, and so on. Network interface provides interaction with outer SAS

environment: an appeal to external databases vulnerabilities for updates; communication with the information collection sub-system. The module of the internal representation of the analyzed network security policy and converts the analyzed data of network and implemented security policy derived from the collector of information (at the stage of operation of the network), or on a user-defined language computer network configuration and software specifications and hardware SDL (System Description Language) language and security policy specification SPL (Security Policy Language) (in the design phase) into an internal representation.

Input in SAZS system specifications and security policy , should describe the components of the protected system (network) with the necessary details ,need be set to software used security (in the form of software titles and versions).

If required for the analysis of the data protection level is not enough (for example, the user did not specify the version of the network service), the system should prompt the user to enter the necessary information on the basis of database software. In order to detect incorrect or underdetermined data, which are necessary for the analysis of security, is the control module data. For example, the user may make a mistake in the name of the service or indicate that port 31 is open on the server, but does not determine what application processes incoming requests on this port. For troubleshoot when entering the specifications of the control module provides the user the choice of the necessary data, using a database of software titles.The data warehouse consists of the following groups of data bases and

Knowledge base :

(1) Group of knowledge base of the network implemented in Security Policy;

(2) A group of database operations;

(3) A group of other databases.

Databases and knowledge [13,14] differ in terms conditional on the submission of information to the prevailing view. In the first case , a factual information, in the second , the information in the form of rules.

Group of knowledge and database about the network consists of four bases:

(1) knowledge base configuration of the analyzed network ;

(2) The knowledge base of the implemented security policies to the Constitutional Rules;

(3) The knowledge base offending configuration of the analyzed network

(4) The knowledge base offender implemented in Security Policy.

Structural data (base configuration and database about The knowledge base) mutually coincide and contain information about the architecture and the specific parameters of a computer network (e.g., the type and version of the OS, the list of open ports and so on.) and the rules that describe its operation.

First knowledge base configuration of analyzed network is actually the internal representation of the specification of the analyzed network that It is used to form an attack action in the construction of a general attack graph.

knowledge base offending configuration , is an internal representation of the analyzed network specification as it is currently the offender, i.e. As a result of the implementation of a sequence of attack.

knowledge base implemented a security policy contains general rules the functioning of the network, for example, "local user host is cannot run the application A “. Based on the information from the knowledge base offender . The implementation on the network security policy it is possible to plan a sequence of actions performed by the infringer (for example, according to the security policy, access to the file is permitted only if local administrators, so read the file offender must obtain the required rights, to implement certain critical sequence of actions).

Group databases action consists of the following bases:
(1) database actions and vulnerability exploits;
(2) a database of intelligence activities;
(3) The database user of common action.
DB action, vulnerability exploits (in contrast to other databases this group) is based on the external vulnerability database. Offensive actions in this database are divided into the following groups:

(1) The actions to obtain the rights of the local user;
(2) actions to obtain administrator rights;
(3) actions aimed at the violation of privacy;
(4) actions aimed at violation of integrity;
(5) actions aimed at violation of accessibility.
DB intelligence activities includes actions aimed at remote receiving information about a host or network. Description of intelligence activities is not contained in external databases

vulnerabilities. Information on methods and means of implementing the infringer intelligence ,Action can be obtained only by an expert.

Base user actions common database contains information on possible user actions carried out in accordance with his existing authority. Such actions may include, for example, the preparatory actions for the attack, as well as activities such as "read file", "file copy" "File Delete", "delete directory" and so on. Which may be used to implement the threat of a violation of the confidentiality, integrity and availability of facilities. For each attacking action DB stored condition of successful implementation of the action (for example, a version of the vulnerable software security), and the result of its impact on the object of attack (for example, emergency stop network service).

Group additional database consists of the following bases:
(1) database to security requirements ;
(2) The database by name.

DB to the security demands contains predefined security expert method sets the values of the metrics, each of which meets the requirements for a certain class of systems of security, regulated by international standards and other regulatory documents.

Database name is used by the data control to detect errors in the use of computer network specification

and forming recommended to use software means, in the absence of the specification required for analysis data protection. The module updates the database and knowledge base downloads open database vulnerabilities , and transmits them to the base Information attack. The module generating total attack graph construction produces a graph Attacks by simulating the possible actions of the offender in the test network, using available information about the actions of various types (offensive, intelligence, common), and network configuration used security policy. During the formation of the attack graph , This module puts at the vertices of security metrics elementary objects, on the basis of which the general graph analysis module calculates metrics attacks composite objects.

The module provides an implementation of intruder model definition of the original offender status, the level of knowledge and skills, primary knowledge of the analyzed network. The level of knowledge and skills It defines a set of actions used by the infringer. Security analysis unit generates a plurality of composite general object graph attacks (trails, threats), calculates metrics security-related data objects, evaluates the overall level of network security, compares the results with the requirements defined by the user (if requirements have been specified), identifies weaknesses in the security space, and generates recommendations to improve the overall level of security computer networks.

Reporting module displays information about the user vulnerabilities found in the software and hardware security, weaknesses, recommendations for improving the level of computer network security, and so on.

5.Conclusion

This work demonstrated a concreate approach by Constructing attack graph (used multi-level, hierarchical view of the attacker's action strategies) and use of a common attack graph constructed to define a family of different indicators (metrics) security .The proposed approach involves implementing a set of functions ,such as modeling of malicious actions; construction of a graph of possible attack, carried out various points of the network and aimed at implementation of various security threats with regard to the qualifications offender; identifying vulnerabilities and "bottlenecks" in the defense (the most Critical components of a computer network);calculation of the various security metrics and the definition of general security level; comparison of the metrics with the requirements and development recommendations to enhance security. Thus, this work propose the implementation of a detailed assessment of the security techniques based on the analysis of attack scenarios and the processes occurring in the test network. This approach allows security team to assess the level of protection computer networks in an environment where there is no possibility to obtain information about all aspects of their operation. Analysis in terms of resistance to hacking attempts can also supplement the results of the analysis of specific examples of the base security, and allows to focus on the private and the most important aspects of the individual applications.

References(10pt)

[1] Boumedyen Shannaq , Richmond Adebiaye," Schemes for Distributed Computing Environment Based on Cloud Computing Technology for Ministry of Regional Municipalities and Water Resources (MRMWR) Oman", International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 6, Issue 1 (Jan 2017) PP: 01-06.

[2] Security Awareness Program Special Interest Group PCI Security Standards Council, October 2014.

[3] Peng Ning and Dingbang Xu," Learning Attack Strategies from Intrusion Alerts", Cyber Defense Laboratory.

[4] Martin P. Clark," Networks and Telecommunications: Design and Operation, 2nd Edition ", SBN: 978-0-471-97346-1,1997

[5] Oracle9i Security Overview Release 2 (9.2) Part Number A96582-01, Data Security Challenges,2002.

[6] Cyber attack techniques and defense mechanisms, institute for security technology studies at dartmouth college investigative research for infrastructure assurance group,2002

[7] Haifeng Zhou, Chunming Wu, Ming Jiang, Min Huang," Evolving Defense Mechanism for Future Network Security ", IEEE Communications Magazine 53(4):45-51 · April 2015

[8] Boumedyen Shannaq," Methods and Algorithms for Searching Arabic Name Entity", International Journal of Computer Applications, Volume 82 - Number 8, 2013.

[9] Boumedyen Shannaq, Devanshi Thakkar ," On the Development of Neural Network Models Using Data Mining Tools", Asian Journal Of Computer Science And Information Technology, 2012

[10] P.P.Kokorin , Boumedyen A.N. Shannaq ,"Methods of texts normalization and ontological clustering of texts" , ,VAX UDC ,information-measuring and operating systems Journal, http://www.radiotec.ru/catalog.php?cat=jr.(2010)

[11] Vasilios Zarikas1 , Nick Papanikolaou2 , Michalis Loupis3 , Nick Spyropoulos," Intelligent Decisions Modeling for Energy Saving in Lifts: An Application for Kleemann Hellas Elevators", Energy and Power Engineering, 2013, 5, 236-244

[12] KIzz,"Guide to Computer Network Security, Security Assessment, Analysis, and Assurance",2017.

[13] Boumedyen , John ,Richmond, "BWA_Thesaurus as knowledge management strategy for Arabic and English Tourism Webpage's " WCAS the international Conference ICKMARS-2012.

[14] Boumedyen ,John ,Jambak , "Taxonomic Knowledge Management Strategy for Managing Market Basketing " presented in WCAS the international Conference ICKMARS-2012, published in Journal of Current Computer Science and Technology ,Vol 3, No 1 (2013). This paper awarded the appreciated paper out of 51 papers