Network Security Evaluation Based on Information Security

Nayunipatruni Suman
Department of Computer Science
GMRIT, Rajam, Andhra Pradesh
INDIA
E-mail-suman1986@hotmail.com

Abstract:

The Network security Evaluation is a In development of computer and network hot issue in present research of Network technology brings us convenience to gether security. After acquiring each host's web-based threat exists everywhere, and to attack. Therefore, study and evaluation of the network security will be important practical significance: finding out network vulnerabilities,enhancing network security and improving network survivability. The Method of network security evaluation develops from manual to automatic, from partial to overall, from regulation-based with network security vulnerabilities: the confidentiality, Integrity and availability evaluation index by attacking the network. we can directly evaluate the network security. But for the Network security involves the security of data transmission, the Confidentiality of communications, the legitimacy of key management. It is a comprehensive application of information security. An information security incident that might be difficult to manage and mitigate. Hence, the objectives of the research are to determine the information security risk factors, consisting of threats and vulnerabilities and to discuss their criticalness. The findings of the research show that the most critical threats are system error and Information Communication Technology (ICT) failures and the most critical vulnerability is insufficient attention to human factors in system design and Implementation

Keywords :- network security; Information Communication Technology, vulnerability, information security, threats, outsourcing, Risk Factor

I. Introduction

In development of computer and network technology brings us convenience together with network security vulnerabilities: the web-based threat exists everywhere, and computer networks are important targets to attack. Therefore, study and evaluation of the network security will be important practical significance: finding out network vulnerabilities, enhancing network security and improving network survivability [1]. The Method of network security evaluation develops from manual to automatic, from partial to overall, from regulation-based to model-based, from stand-alone to distributed [2], from qualitative to quantitative plus qualitative [3].This issue to the field of information Technology (IT)Security as information technologies constitute merely component of information systems. It is crucial to view information system security in its complexity and aim to secure IS of the organization in all its components and across all interfaces [4]. Secyrity of information system is an essential part of its conception and development. It would, however, be misleading to narrow this issue to the field of information Technology (IT) security as information technologies constitute merely one component of information systems. It is crucial to view information system security in its complexity and aim to secure IS of the organization in all its components and across all interfaces [4].

Information security threats, enterprises improve their information security system by polishing their information security policies and reconfiguring their operation system. Therefore, the automatic management of information security will become one of the most important issues in the near future. In the field of information security, many of the Researches discuss and investigate the laws, e.g., BS7799 and ISO27001, and the relevant theory aspects.

Enterprises should construct a sound information managing technique and integrate the information security systems at the end hosts into one standardized information security management platform. Thus, distributed independent protection functions can be ntegrated into one service-oriented module that satisfies the security standard and the needs of enterprise in the future.

Evaluating and extending concepts:

Objective quantitative evaluation of the output of this clustering stage isn't easy. Apart from an impressionistic idea of general quality, more sophisticated quantitative evaluation is difficult. The obvious possibilities - such as comparing extracted concepts to existing ones in terms of computation of recall, overlap, precision, and so on-give us some indication but are limited because our approach is intended to evaluate and extend existing concepts anyway. More progress in evaluating text-based information security concept learning might come from carefully constructing a gold standard information security concept on the basis of manually analyzing a corpus. By tuning the pattern matching to ontological relations such as part-whole relations and specialization generalization relations, we can easily extend concepts. However, both in the clustering step (which you could interpret as extending or evaluating the extension of concepts) and in the pattern-matching step (which you could interpret as populating the information security concept with selected relations), human intervention is essential to evaluate the system proposals. The difference with purely handcrafted information security concept development is that recognizing and evaluating proposed ontological structure is much easier, more complete, and faster than inventing ontological structures. Language method tools have advanced to such a level of accuracy and efficiency that it's now possible to Automatically analyze huge amounts of text. Like most researchers in this field, we believe that this approach will solve some hard problems in information security concept Content creation, adaptation, and evaluation but will always require human interaction.

II. Security Policy

Security policy is a set of measures covering formal and normative frame of information security in a company or an institution. It also describes implementation process of technical and administrative measures for daily operations of a company.

First step in creation of IS security policy of a company is an elaboration of information security study, which describes current status of information security in a Specific company. Subsequently, a risk analysis is to be performed. People who are well familiar with company's environment should be involved in the risk analysis study. Information obtained by risk analysis are fundamental for company's information security, therefore, it must be kept confidential and accessible to strictly defined audience Only.

Based on the result of the risk analysis, security policy is Created .It consists of two parts:

1)General security policy: description of the Organization and its processes, security policy Objectives, security infrastructure, identification of Assets, confidential data and general threats, Description of present status and description of Security measures, contingency plans.

2)System security policy: that defines implementation of security policy in a specific system of a company. With security mechanisms based on security policy being in place, it is essential to monitor their actual functionality

III. A Formal Network Security Evaluation Based on Information Security Concept Quality.

Before evaluation for computer network information security, evaluation indexes of computer network information security should be constructed.

We construct two layers evaluation indexes of computer network information security, which is The first class assessment index includes three indexes: environmental safety, hardware and software safety, data security. There are 12 indexes in the second class assessment index. In environmental safety, defence against electromagnetic leakage, defense against wiretap and safe power supply is included. In hardware and software safety, firewall, intrusion detection, software flaw analysis and anti-virus software are included. In data security, digital signature, data recovery, data encryption, data backup and access Controls are included. Evaluation result is

established on the weight of these assessment indexes.

IV. Approaches on Security Engineering

(1) Security architecture

In security engineering context, *security architecture design* is a problem described below: Given a set of security component or module (e.g., firewall, VPN, and so on) that performs unit security function (e.g., access control, authentication, and so on), and their costs, evaluated assurance levels (EAL) and security strength, we must integrate, organize and construct an optimal *security architecture* that has maximal security by using minimal cost. *Security architecture design* is comparable to Lego block. Quality of architecture can be measured by means of evaluating *coupling* (i.e., interface complexity) between components and *cohesion* of internal of a component

(2) Security pattern

Security pattern is application of conventional research of *software pattern* (a subject in component base software engineering). There are many research results on security pattern in (http://www.securitypatterns.org/). Major subjects of security pattern are ①development of an efficient security pattern description language (e.g., UMLsec inhttp://www4.in.tum.de/~umlsec/), ②development of efficient security pattern repository(data base) and pattern mining method, ③development of new andreusable security patterns [16].

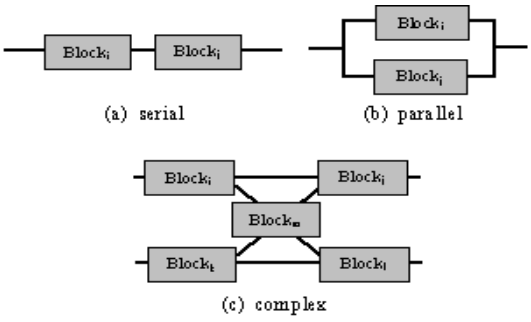

Fig. 1. Element structure of Security Block Diagram

In modern general purpose high level programming language such as Java and C#, there are many functional structures such as exception handling and monitor structure. They are useful for concurrent programming and fault tolerant programming those are necessary problems in modern computing environments (e.g. parallel,concurrent, distributed, high availability, real-time).

Security monitor and *security exception handler* are possible extensions of conventional monitor and exception handler. Recall that monitor is a modular unit to implement concurrency control function (e.g., mutual exclusion and synchronization). Security monitor is a new modular unit to implement security function (e.g., data/variable level information flow control and access control). Security exception handler is another extended exception handling structure that has security exception.

(2) Secured programming

Recall that Dijkstra's "structured programming" was influenced to software engineering (especially structured programming). Pascal, C and Java are typical structured programming languages. We can research *secured programming* is by extending the structured programming concept. One of the successful research result is "secure programming for Linux and Unix" of David A. Wheeler [29]. He provides a set of design and implementation guidelines for writing secure programs for Linux, Unix systems and C, C++, Java, Perl, PHP, TCL and Ada95 (e.g. preventing buffer overflow). Such programs include application programs used as viewers of remote data, web applications (including CGI scripts), network servers, and setuid/setgid programs.

(3) Runtime security

Security mechanism (e.g., byte code verifier) in Java is regarded as "white box" run-time security monitoring mechanism. That is more secure than Microsoft's activeX control authentication approach (i.e., "black box" approach) even Java has lower usability than authentication approach. Further research is needed in this area.

V. Security assurance

(1) Security test and verification

Security testing is an activity of demonstrating that a security system or product is not incorrectly developed in conformance to a Security Functional Requirement Specification (SFRS) (or

PP, ST) by using the 'test case' or penetration test scenario. We need *testing engine* that automatically generate the test case or penetration test scenario from SFRS and test and analyze.

(2) Security validation

Security validation is an activity of demonstrating that a SFR (or PP, ST) is really reflected security requirements and environment. PP and ST evaluation in CC evaluation are example of the security validation. Acceptance test, system level evaluation, operational evaluation, certification and authentication are can be regarded as the security validation.

(3) Security evaluation model

A scheme of information security evaluation consisted of evaluation criteria, deliverables, and evaluation tools as shows in Figure 3. For each atomic (i.e., non dividable) criteria *ci*, deliverable *di* and tool *ti* are inputs of an atomic evaluation method *mi*. Results of all *mi* are merged to final result *R*. Result of RL is a function of DL, CL as show Below

RL = MT(DL, CL)

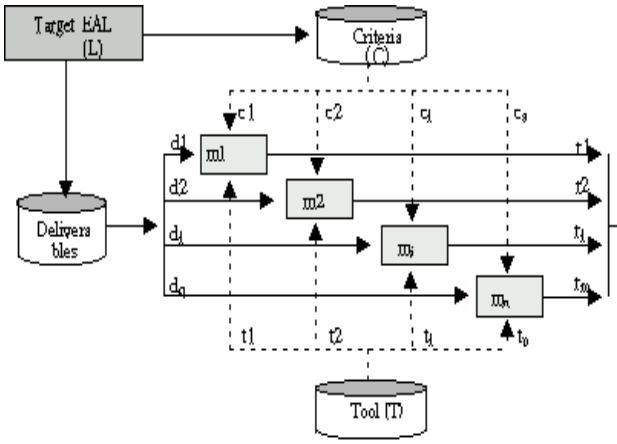

Fig. 2. A security evaluation model

- RL = {*r1, r2, r3... rm*} : set of result of evaluation (*RI* = path, fail, unconclusion) (Example of verdict rule: If at least an *ri* is 'unconclusion', then R ='unconclusion', else If at least an *ri* is 'fail' then R='fail' else R = 'pass'.
- M = {m1, m2, m3... mn}: a set of evaluation method
- T = {t1, t2, t3... tp}: a set of evaluation tools (e.g., static analyzer, verifier, test tools)
- D = {d1, d2, d3... dq}: a set of deliverables (e.g., structure design, source code, security target)
- C = {c1, c2, c3... cs}: a set of evaluation criteria (e.g., ITSEC, TCSEC, CC)
  DL ⊆ DL+1⊆.... DLmax = D
  CL ⊆ CL+1 ⊆.... CLmax = C
  L ∈ {level1, level2... levelLmax}: set of evaluation levels

It is important to note that, in some security product and system evaluation schemes, all set of criteria and deliverables are not used, but subset of them are used for each specific Target evaluation assurance level (e.g., EAL1 ~ EAL7 in CC) [20]. However, in scheme of information security management system such as ISO/IEC 17799 and ISO/IEC 21827 (SSE-CMM), whole set of criteria and deliverables are needed. Optimal and cost-effective evaluation criteria, evaluation tool, and form and contents of deliverables as well as evaluation methods should be developed in context of security engineering paradigm [7], [21].

(4) Dependability evaluation

As a user of real information system, he should concurrently consider not only security, but also availability, reliability and safety. Thus evaluation method of the dependability is needed [23]. The *dependability* is a property of the system that equates to its trustworthiness. Trustworthiness essentially means the degree of user confidence that the system will operate as they expect and the system will not 'fail' in normal use. Dimensions to the dependability are *reliability* (correctness, precision, and timeliness), *safety* and *security* (confidentiality, integrity, availability). Repair-ability, maintainability, survivability and error tolerance are other system properties can also be considered under the heading of dependability. Technologies on dependability engineering should be developed in context of the engineering of security, reliability, safety engineering.

VI. LITERATURE REVIEW **OF** RISK ASSE**SSME**NT

Literature Review In the field of risk assessment, Roehl and Fesenmaier (1992) have categorized information security risk into seven items: equipment risk, financial risk. physical risk, psychological risk, satisfaction risk, social risk, and time risk. Halliday(1996) develop **an** effective information technology risk analysis and management method, which is a business-oriented approach from an IT perspective. Lichtenstein(l996) discusses requirements for ideal risk assessment, and developsand evaluate risk factors to be considered in the selection methods. Crmes(l991) have developed schema for risk ranking to specify the items that contribute significantly to program risks, named it risk ranking and filtering(RRF1 methodology. RRF prioritizes the risks considering multiple factors, such **as** reliability estimates, and qualitative factors. Ward(1998) examines the shortcomings of common approach to the rank risks in terms of probability and impact, and guide the analysis of risks to consider the multiple factors include size of impacts, probability of impacts, inter-dependent between risks and response and the time available for response. The nature of the study is a investigative research, focused on information security management of the organization.Risk Assessment Methods The general approach to risk assessment usually based on **assetlthreatlvulnerability** model which refers to the investigation of assets, threats,vulnerabilities and to find out risks. followed by the implementation of effecrive safeguards. Risk assessment is usually classified **as** quantitative risk analysis and qualitative risk analysis. Quantitative risk assessment, general speaking, rely on probability and statistics which builds **on** the existence of probabilities that describes the likelihood of outcomes, such as consequences. We common refer to probabilities that are derived from this process **as** "objective probability". In general, probability are derived **on** the basis of historical records, statistical analysis. systematic observation and experimentation. Some authors have studied **on** probability of threats and proposed many well-known methods, such as the fractile method, the triangular distribution method. Nerveless, in many cases evaluators always proceeds to assess the likelihood of Thread vulnerability lacking of prior information situation. **In** this situation, the other approach is used---the qualitative risk analysis.

it's a descriptive ranking risks, for example, "very high risk". In this study, we adopts the qualitative risk analysis since deficient of prior information about threats and vulnerability. The concept of perceived risk most often used by consumer researchers defines risk in terms of the consumer's perceptions both of the unceltainty and the magnitude of the possible adverse consequences (Con 1967, **Cox** and Rich 1964; Dowling and Staelin 1994). As the risk can be defined of possible loss and the risk itself is not known certainty I the process of risk assessment might be conducted in uncertainty and fuzzy environment. Therefore, this study includes Fuzzy MCDM theory to reinforce the fullness and rationality of the risk-determining process.

VII. AWARENESS OF SECURITY STATUS

In the latter part of the **1990s** the USA set up a Presidential Commission to look into the security of critical infrastructures - one of the key infrastructures being energy. The commissioners delivered an eye-opening report [11 including observations:

It is the cyber threat that is new – networked information systems present fundamentally new security challenges.

We found ... **today, the right command sent illicitly over a network to a power generating plant could be just as effective as a backpack full of explosives - with the perpetrator harder to identify and harder to apprehend.**

We observed ... **within government and among industry decision-makers awareness is limited. Several believe that there is not yet cause for concern or sufficient to demand action.**

We conclude ... **it is clear that infrastructure assurance must be a high priority in the Information Age. They are vulnerable in new ways - we must protect them in new ways. Both public and private sectors share this responsibility.**

So - are our Utility's communications infrastructures secure? Can the Utility recognise that **an** attack has occurred (or is occurring)? Can the Utility record details of the attack? The suspicion is that in most cases the Utility's physical properties are secure, but what about their communications infrastructure?

Consider the Utility's telecontrol and Network Management Systems. Information **is** the lifeblood of these systems - the Utility cannot operate if it is starved of information. Security for these systems doesn't just happen ! and security is never complete ! So if we recognise that there is no way to prevent the security attacks we must develop mechanisms to counter these attacks. This means that we must:

VIII. Conclusions

In the network security testing and evaluation process, some hosts in the network with the read and write management privilege to boot directory have the Relationship of Information Security Management System is the term being used for a system of management concerned with Information Security.

If we directly assess the network security from the test value, the assessment can't really reflect the network security situation. After the transition of the network security confidentiality vector and integrity vector by the mechanism of continuous analysis, Implementation, control, maintenance and improvement of Information security system aiming to prevent systematically incidents occurrence. The network security assessment will be feasible and also can provide a scientific basis for the network insecurity detection and resolution.

REFERENCES :

1. Research on Information Security in Modern Network Ning Zhang 1, 2 1. Institute of Information Technology 2. Faculty of Information and Engineering, Flinders University, Adelaide, 5001 Hong Bao., School of Information.,Beijing Union University
2. Evaluation Model for Computer Network Information Security Based on Analytic Hierarchy Process XI Zhen-yuan, CHEN He, WANG Xiang-zhong, SHENG Jian-ling, FAN Yu-tao
3. An Information Security Engineering Paradigm for Overcoming Information Security Crisis., Yeun-hee Jei, Ick-whan Bae, Sung-ja Choi and Gang-soo Lee D*ept of Computer Engineering, Hannam University, Dae-jeon, 306-791, KOREA gslee@eve.hannam.ac.kr*
4. INFORORMATION SECURITY - WHO CARES ? B Shephard Schneider Electric, UK
5. Information Security Risk Assessment & Pointed Reporting: Scalable Approach D.S. Bhilare.,School of computer science , Dr. A.K. Ramani.,School of computer scienceDr. Sanjay Tanwani.,School of computer science,Devi Ahilya University,Indore, India
6. Network Security Platform Design Based on WWW Information System Xi Jianrong, Department of Computer Science, Weinan Teachers University,Weinan, China