Review of methodologies on network defects and vulnerability

Wonjoo PARK*, Dongil-SEO**, Daeyoung KIM***

* Information Security Development Division, ETRI, Daejeon, Korea
(Tel : +82-42-860-5351; E-mail: wjpark@etri.re.kr)
** Information Security Development Division, ETRI, Daejeon, Korea
(Tel : +82-42-860-3814; E-mail:bluesea@etri.re.kr)
*** Dept. of Information Communications Engineering, CNU, Daejeon, Korea
(Tel : +82-42-821-6862; E-mail: dykim@cnu.ac.kr)

Abstract: Security defects occurring within corporate networks and the Internet may be abused by internal or external malicious attackers. Such abuses cause a financial toll through expenditures on additional human resources, the impact of down-time as problems are fixed, as well as damage from divulging corporate informational assets. Hence, through the precise analysis of the possible defects in network security and the identification of risks, preventative policy should be established to ensure maximum security. This report reviews methodologies that calculate and analyze levels of network security in order to resolve these problems, and generates appropriate test steps, test methods, and test items.

Keywords: Risk analysis, network vulnerability

1. INTRODUCTION

Security defects occurring within corporate networks and the Internet may be abused by internal or external malicious attackers. Such abuses cause a financial toll through expenditures on additional human resources, the impact of down-time as problems are fixed, as well as damage from divulging corporate informational assets. Hence, through the precise analysis of the possible defects in network security and the identification of risks, preventative policy should be established to ensure maximum security. However, with regard to applying safeguards in actual working environments, there currently is neither a precise standard to measure the level of network security (AS-IS) nor a standard to measure the extent of safeguards to improve security levels (TO-BE).

To resolve this issue, it is time that a methodology to measure and analyze current levels of network security be established, including adequate test steps, test methods, and test items.

2. MET ODOLOG REVIEW

Corporations themselves rarely perform analysis for detecting security defects in their information systems, and generally carry out by themselves only internal checks of their systems by using defect detection solutions or simple checklists. Also, institutions contract out information security to consulting companies - which evaluate their current level of security and establish systematic solutions - because of legal requirements like the Information Security Act, the establishment of information protection systems, and the existence of security threats. Consulting companies perform risk analysis, which is the essential component of the security analysis.

Internationally, there are many methodologies for analyzing risks. They differ depending on the field and the circumstances of the information system of the targeted items. Each model for security analysis can be configured, regardless of the user s specific circumstances or purpose, and according to the specifications of the users requiring security analysis.

2.1 ritish RA methodology (SI)

RA(Risk Analysis) is a security analysis model that has been developed specifically for BS7799 compliance. It assists in the application of Part 1 and 2 of BS7799, to improve corporate information security management. This includes support for establishing an Information Security Management System (ISMS), as per Part 2 of BS7799. Hence, the outcomes of RA s risk analysis have merit in their ability to present to the BS7799 inspector proof that all the processes specified in Part 2 of BS7799 are carried out. RA is performed according to the following 5 steps:

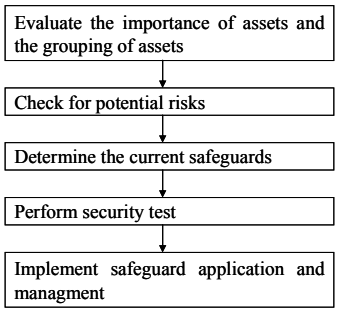

Fig. 1 RA methodology

RA methodology contains the basic concepts of risk analysis, and because of its simplicity is adequate for first-time risk analysis in small-sized institutions. However, for institutions that have numerous information systems and network assets, this risk analysis system provides limited functionality and effectiveness : RA can only be effective if it is adapted to the organization s specific circumstances.[1]

2.2 ritain s (CCTA) CRAMM Model

CCTA Risk Analysis and Management Method (CRAMM) was developed by the Central Computer and Telecommuni -cations Agency(CCTA) for the purpose of risk analysis of the information systems of British governmental agencies. As CRAMM evolved into an automated tool, it expanded into private use. It has been through several reviews and

modifications since 1988. In addition to the established merits of the method, automation for analysis and verification process and risk management have been added, and the use of CRAMM has increased.

Each stage requires a Stage Agreement, in which the outcomes measured from each step are verified by the managers to improve their accuracy. All the managers, including the system and security managers, should participate in the risk analysis process. Moreover, the merit of the automated CRAMM lies in the fact that risk analysis can be applied during the security system design. Of course many other automated tools have this useful function, but CRAMM s function is particularly powerful. To maximize the effect of risk analysis, the application of risk analysis is recommendable from the system design stage. However, this methodology has a disadvantage, which is its difficulty in detecting mistakenly implemented countermeasures at stages 1 and 2 of the security solution review. [2]

Phase 1: Identification and evaluation of physical assets, software, and data assets
- Identification of system assets and the measurement of their value
- Determination of items requiring security for the targeted organizations

Phase 2 : Threat analysis, defects analysis, and risk testing
- Measurement and evaluation of the degree of defects and threat for the asset groups
- Determination of items requiring security and analysis of all system risks

Phase 3 : Identification and selection of the countermeasures for the current systems
- Perform risk management to maximize the effect of risk analysis
- Implement the countermeasures and improvement plans to reduce risks

2.3 US NIST Methodology

The National Institute of Science and Technology (NIST) established the foundation of quantitative analysis by publishing in 1979 the " FIPS PUB 65, Guideline for Automatic Data Processing Risk Analysis . " FIPS PUB 191, Guideline for the Analysis of Local Area Network Security " and " Special Publication 500-174, Guide for Selecting Automated Risk Analysis Tools " present the risk analysis models and security mechanisms . The features of NIST s risk analysis model include the determination of overall security mechanisms and the application of versatile methods for multiple circumstances, in which the users are able to liberally select a risk analysis method. The procedure for risk analysis proposed by NIST contains 7 steps as figure.

The risk analysis method proposed by NIST:

Risk = Likelihood of threat occurring **X** Loss measured

The above method has been widely adopted as a fundamental risk analysis formula. It helps to satisfactorily quantify outcomes for both events of high likelihood but low loss and events of low likelihood but high loss.[3]

2.4 US OCTAVE Methodology

OCTAVE is a risk analysis methodology developed in 1999 by SEI of Carnegie Mellon University. It concentrates on risk analysis for information assets and practical solutions to alleviate risk factors

Phase 1: Write an asset-based profile of the level of risks
- Critical assets
- Security requirements for protecting the critical assets
- Threat factors for the critical assets
- Measures for current security
- Current defects of institutions

Phase 2: Discern defects in infrastructure
- Main components
- Current technical defects

Phase 3: Develop Security strategy and planning agenda
- Identify risk factors of the critical assets
- Measure risks
- Defensive strategy
- Plans to alleviate risks

through overcoming the previously discovered security defects. OCTAVE s accessible method is comprised of 3 phases:

OCTAVE risk analysis is targeted to all organizations including IT divisions and business sectors, and has merit in carrying out multi-perspective evaluations of relevant divisions and for all company personnel. [4]

2.5 CISCO SAFE Model

SAFE is a blueprint for network security proposed by Cisco Company. It is based on Cisco Architecture for Voice, Video, and Integrated Data (AVVID), and defines which security solutions to deploy for the whole networks by using modules that simplify network design, practical rollout, and management. Each module includes security and VPN factors that can reduce the specific threats discovered from each network area.

SAFE acts as a guide in protecting network architecture. It divides network architecture roughly into: large-scale campus network, enterprise network including e-commerce and extranets; small and medium-scale network; and remote-user networks. By defining each module, it can determine the types of threats and can propose countermeasures for alleviating them.[5]

Phase 1: Security based on network security policies
Phase 2 : Security for the entire infra-network
Phase 3 : Thorough security management and reporting system
Phase 4 : Mechanism for authorization and certification
Phase 5 : Detection of intruders into the critical resources and sub-networks

3. Measurement of levels network security

The methods for assessing the level of network security are largely categorized in two ways. First, network security can be measured by using network defect analysis tools. Such tools as

Retina and NetRecon show levels of security by using various reports or graphs after the investigation of the target area. This analysis tool has merit for the convenient and simple investigation of networks but is only able to show partial outcomes and still has many limits in assessing the security level of the global network. [6][7]

Second, network security can be measured by using personnel for diagnostic purposes. This method quantifies the outcomes by using checklists for individual categories to assess the level of network security. At the stage of risk analysis, the outcomes obtained by the risk analysis of individual areas are integrated and quantified again, thus enabling an in-depth assessment of the level of network security. Presently, almost all the information-security consulting companies apply this diagnostic method for determining levels of network security except for the some areas.

This paper presents various quantification methods for assessing the levels of network security by practically applying the outcomes obtained using the checklists. There are disadvantages in that for organizations with numerous assets this requires a great deal of time to perform the practical check for information assets, and it is inconvenient to manage separately each risk. For example, in organizations that want to manage only technical risks, not physical and managerial risks, this method is not appropriate for instant and timely management due to the excessive time required and inconvenience. In particular, for an initial application of safeguards for information security, this method has many barriers to evenly improve the security for all areas - managerial, physical, and technical.

In most cases, the first aim of security is to block all unauthorized outsiders from hacking, and the next aim is to block any threats by authorized insiders and outsiders through the expansion of the scope of the application. So a flexible management methodology is required for controlling managerial, physical, and technical risks. Moreover, this system is more suitable for the domestic context where it is appropriate to apply safeguards to the selected areas that require security systems stage by stage. Therefore, effective and efficient risk management can be achieved by adopting objective and quantitative methods in performing risk analysis for information assets.

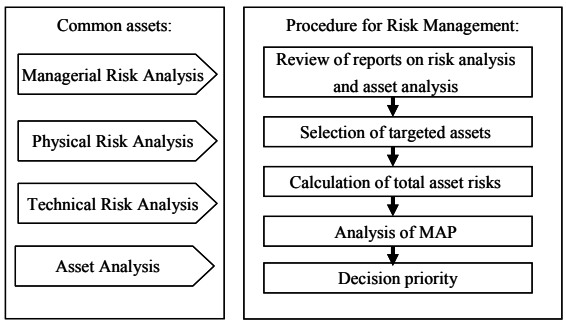

Fig. 2 Procedure for effective Risk management

3.1 Review of outcomes of risk analysis (managerial, physical, technical) and of outcomes of assets analysis

Summarize the list of assets, risk assessment by asset, and details in the test for the degree of importance of assets by reviewing each asset s importance in terms of the relevant risks and the outcomes of asset analysis that are achieved from the process of the managerial, physical, and technical risk analysis.

3.2 Selection of targeted assets

Out of the assets reviewed from Stage A, determine the managerial, physical, and technical assets reviewed from the risk analysis and test of the degree of importance of assets (asset priority). Then take the common assets as the targeted assets. For this selection and analysis of the targeted assets, the preceding steps should be followed: for risk analysis of the managerial, physical, and technical assets, the specific management division, physical locations, technical check details and defects of individual assets must be derived (and a risk analysis should be performed in advance).

3.3 Calculation of total asset risks

Calculate the weighted average of managerial, physical, and technical risks of the prior-derived target assets and their degree of importance based on the total asset risks formula. In the formula for the weighted average of the managerial, physical and technical risks, use the simple weighted average, which is derived by first ascribing points to H, M, L (the levels of risks measured in each report), 3 points, 2 points, and 1 point, respectively, and then dividing the sum of the points by 3. The formula for the weighted average is as follows:

Weighted average of risks
= (Managerial risks x W1 + Physical risks x W2 + Technical risks x W3)/ W1+W2 +W3

Calculate the total asset risks to reflect the degree of importance of individual assets into each asset s weighted average of individual asset risks by using the following formula:

Total asset risks
= Weighted average of individual asset risks × The degree of importance of individual assets

Calculate total asset risks for the degree of importance of individual assets by ascribing 3, 2, and 1 points for degrees of importance 1, 2, and 3, respectively.

3.4 Analysis of MAP

Make axes for the weighted average of managerial, physical, and technical risks and the degree of importance of assets, and analyze the degree of importance of assets and the weighted average of risks on the two dimensional plane. Make the axis for the weighted average of managerial, physical, and technical risks and the axis for the degree of importance of assets calculated from the previous stage, and then analyze by asset.

For instance, let us suppose that system A, system B, and system C have the values shown in Table 1. The correspond -ing map analysis is described in Figure 3.

Table 1. Weighted average of risks and the degree of importance of assets by system (example)

Description	System A	System B	System C
Weighted average of risks	M	L	H
Degree of importance of assets	M	M	H

3.5 Decision Priority

Based on the location on the graph shown through the analysis of MAP, and considering the degree of importance of assets and the weighted average of risks, the top right side is the area of greatest priority. In Figure 5, System C is the first priority, followed by Systems A and B. By carrying out the above procedure, the managerial, physical, and technical risks and the degree of importance of each asset can be reflected collectively. Consequently, the security solutions will be determined for all institutional divisions according to the security priorities for each asset.

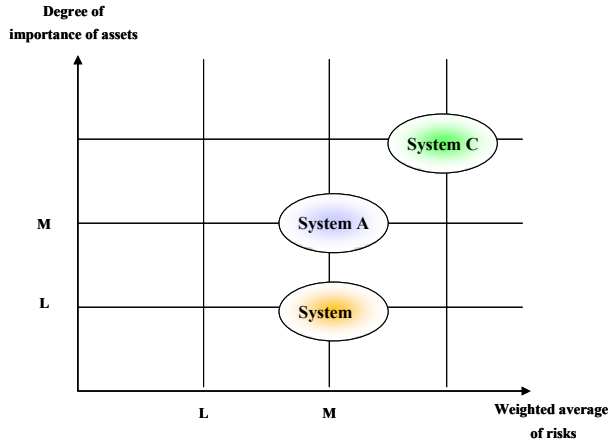

Fig. 3 Analysis of MAP (Example)

4. Conclusion and Future work

Until recently, for security management of information systems, defect analysis of individual information systems and establishment of solutions has been the main focus, but from now on, risk analysis and management integrated with individual defect analysis will be essential to security management. Furthermore, tool-based methodologies will become mainstream by developing automated tools for risk analysis. Additionally, it will be important to appropriately apply to the risk analysis tools such as the merits of the foreign methodologies reviewed and the key contents of risk analysis methodologies suitable to each country s circumstances.

REFERENCES

[1] British Standards Institution (BSI), BS-7799, 1999
[2] CCTA, CCTA Risk Analysis and Management Methodology (CRAMM), Datapro Reports On Information Security, 1992
[3] Edward Roback, NISTIR 4325, Risk Assessment Methodology, 1990
[4] OCTAVE, OCTAVE Criteria, Version 2.0 Carnegie Mellon Software Engineering Institute, 2001
[5] http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking solutions package.html
[6] http://enterprisesecurity.symantec.com
[7] http://www.eeye.com