전산 시스템 보안을 위한 자동화 위험분석 도구 (HAWK: Hankuk risk Analysis Watch-out Kit)의 개발에 관한 연구

o
윤정원* 신순자* 김기수* 이병만* 송관호*

한국전산원*

Development of Automated Risk Analysis Tools(*HAWK*) for Information System Environments

o
Jeong-Won Yoon* Soon-Ja Shin* Ki-Su Kim*
Byung-Man Lee* Kwan-Ho Song *

National Computerization Agency*

Abstract: Risk analysis is time-consuming and expensive process[1][6]. Automated risk analysis tools have been widely used in industry and government to support decision making process and reduce cost. However, difficulties in materializing impact of threats and fast-changing network environments make analysis process more complicated and less trusted since impacts are relative in network environments. HAWK system is developed to improve the accuracy of analysis result in network-oriented environment. It provides user-friendly environments and considers network environments as primary assets.

1. Introduction

The main goal of any risk analysis tools is to provide computation of impacts, performs cost-benefit analysis of controls, and evaluates suggested safeguards. However, most important role of automated tool is to provide decision support function to help human decision to save time and cost, and to reduce errors. Since the history of information systems risk analysis is relatively shorter than other areas such as insurance, stock market, power plants and etc, methodologies for IT system risk analysis were inherited from

conventional risk analysis. In 70s and 80s, information system was more independently operated than today, and network environment was less considerable as far as risk is concerned. Client/Server environment, real time system, distributed system, and many inter/intra networking system are adopted to share information, and the integrity of data is harder to preserve than before. Therefore, many conventional methodologies such as computation of ALE(Annual Loss Expectancy Value), Service Interrupt Cost, and etc is very difficult to measure in the networking environment. Moreover, due to advancing technology, controls have been getting complex and hard to implement. Therefore, importance of automated risk analysis is recognized more than ever. In this paper, we present HAWK system which is automated risk analysis tools specifically designed for network-oriented environments.

2. System Characteristics

2.1 Difficulties of Using Automated Risk Analysis Tools

Application of automated risk analysis tools to the risk management process requires user training and customization. Many users are often encountered with difficulties for the following reasons.

1) Only trained and experienced experts(usually IT auditors or risk analyst) may use the system with full strength.

2) The analyzed results need to be interpreted to make system users understand in practical terms.

3) The fixed questionnaires can hardly be adjusted in many dynamic information systems and network-oriented environments. In result, it is possible that the analyzed outcomes may misrepresent actual risk.

4) Even though current trend of the information systems moves toward the network-oriented environment, many risk analysis tools still don't reflect enough the trend or heavily depend upon the post analysis consulted by IT consultants.

5) There are difficulties to convert intangible values such as electronic data to currency values.

Since the risk analysis is core process before setting the contingency plan and disaster recovery, many systems users, not necessarily end-user, should involve the process to reflect the systems environment to the analysis process.

2.2 System Requirements

To determine accurate risk involved in target system, we must find out necessary information of target systems and its associated environments. If there are sufficient datum for target environment, decision-making process could be more precise and credible. This same principle applies to automated tools also. To make the system intelligent enough to help human experts, knowledge based approach is required. In brief, we decided our system requirements as followings.

- User Friendliness[1]
- Modeling Capabilities[1]
- Easy Customization for Dynamic Environment
- Saving time and cost
- Providing both Quantitative and Qualitative analysis[6]
- Producing ready-to-submit reports
- Assisting Risk Management Process
- Providing simple cost-benefit analysis
- Considering Network-oriented environments as priority factor

Most of automated tools require certain training to use efficiently. It is often encountered that user/security analysts have hard time to understand the analyzed results requiring expert's interpretation. Therefore, it is very important that user may easily understand the results of analysis, and apply it to the risk management process.

To measure risks, it is vital to consider as many threat scenarios as possible. Therefore, modeling capability must be needed in automated tools.

Network-oriented environments are very dynamic so the impacts upon the asset(either tangible or intangible) by same threat may be changed. Therefore, it is very vital to have

capability that reflects fast-changing target system environment.

2.3 The Overall Architecture of HAWK system

HAWK system is knowledge-based system which configures and rearranges the system's database to reflect the target system environment for accurate analysis. The design philosophy of HAWK system from the beginning is to consider network-oriented environment. Therefore, network domain is treated in priority and gives impact to every asset. HAWK system contains five different modules which are Expert, Preview, Survey, Analysis and Results modules.

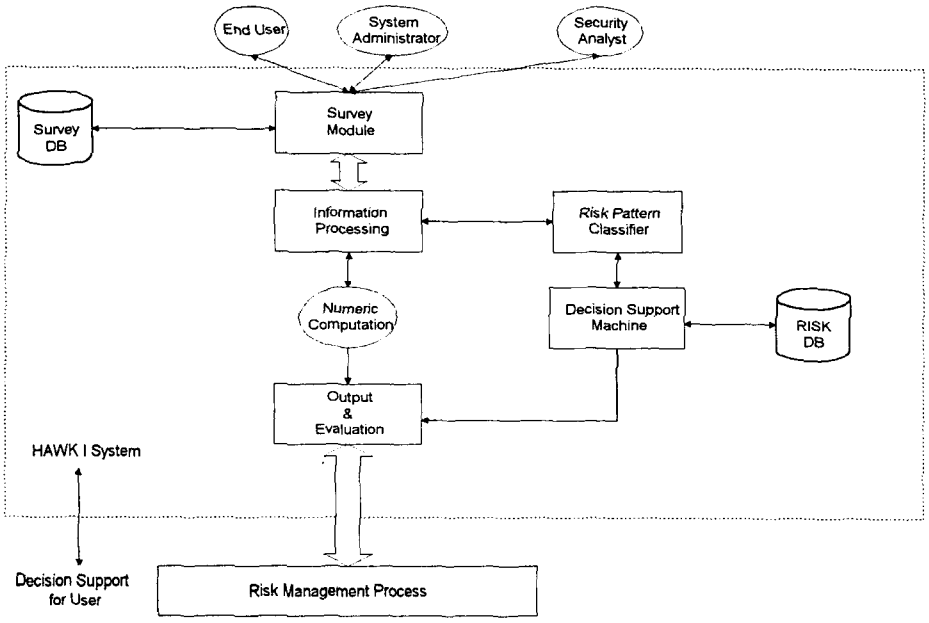

Figure 1. Overall Architecture of HAWK System

Expert module implants threat scenarios, gives weight values, edits assets, threats, vulnerabilities, and countermeasures, and performs mapping of relations between assets and others. Expert module must be carefully revised prior to analysis. Preview module performs pre-survey of target system environment to adjust HAWK Survey Module. During this process, only necessary information is extracted and applied. Each survey

question is designed to answer either by YES or NO to avoid misunderstanding and complication. As shown in Figure 1, surveyed information is stored in SURVEY DB for the purpose of retrieval and editing since survey process is the longest process in risk analysis. Another database, which is RISK DB, is maintained in Expert Module for the purpose of implanting threat scenario, editing asset, and etc as described above. After survey process is done, information from the survey process is used in Analysis Module to detect possible security breach by interacting with RISK DB for necessary information. All implanted threat scenarios and other knowledge stored in RISK DB is used to assist the analysis process.

3. System Design

Assets

Assets are main concern in risk analysis. In HAWK system, assets are divided by seven different domains. These seven different domains are followings.

Tangible Domains = { System, Operating System, Network, Application, Environment }
Intangible Domains = { Data, User }

System domain refers to physical entity with information processing capability of any kind such as CPU, Storage Devices, Back-up Devices, and etc.

Operating System domain refers to entity of Operating System of any kind such as UNIX, VMS, DOS, Windows, and etc.

Network domain refers to entity with network operating capability of any kind such as router, bridge, network communication software, cables, and etc.

Application domain refers to entity of software with data processing capability of any kind such as word processing, editors, compilers, and etc.

Environment domain refers to entity with supporting capability of information systems such as UPS, halon devices, air control systems, card reader system, and etc.

User domain refer to personnel resources involving in information system.

Data domain refers to entity of information.

Preview and Survey Module

HAWK System contains these seven different types of assets in its data base. Since information system environment is too dynamic and system dependent, applying risk analysis using automated tools without pre-survey may cause less accuracy of results. Therefore, to adjust automated tools to the target environments plays very important role to increase accuracy. HAWK systems contains preview module which pre-survey target system environments. Therefore, after processing data gathered through preview module, HAWK system adjust its data base to extract needed entities of domains, associated threats, applicable safeguards and vulnerabilities, and re-map the survey questions(Figure 2.2). HAWK recognizes the importance of network related assets which gives great impacts to the overall analysis results.

Security Analyst or Risk Analyst may add user defined regulation and comments by performing survey process for compliance evaluation and post analysis.

System flow in Figure 2.1 and 2.2 shows logical process of HAWK system.

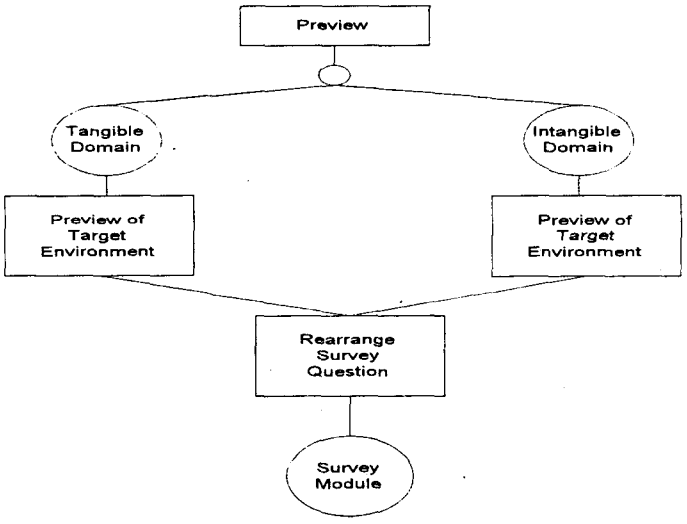

Figure 2.1 Preview Process of HAWK System

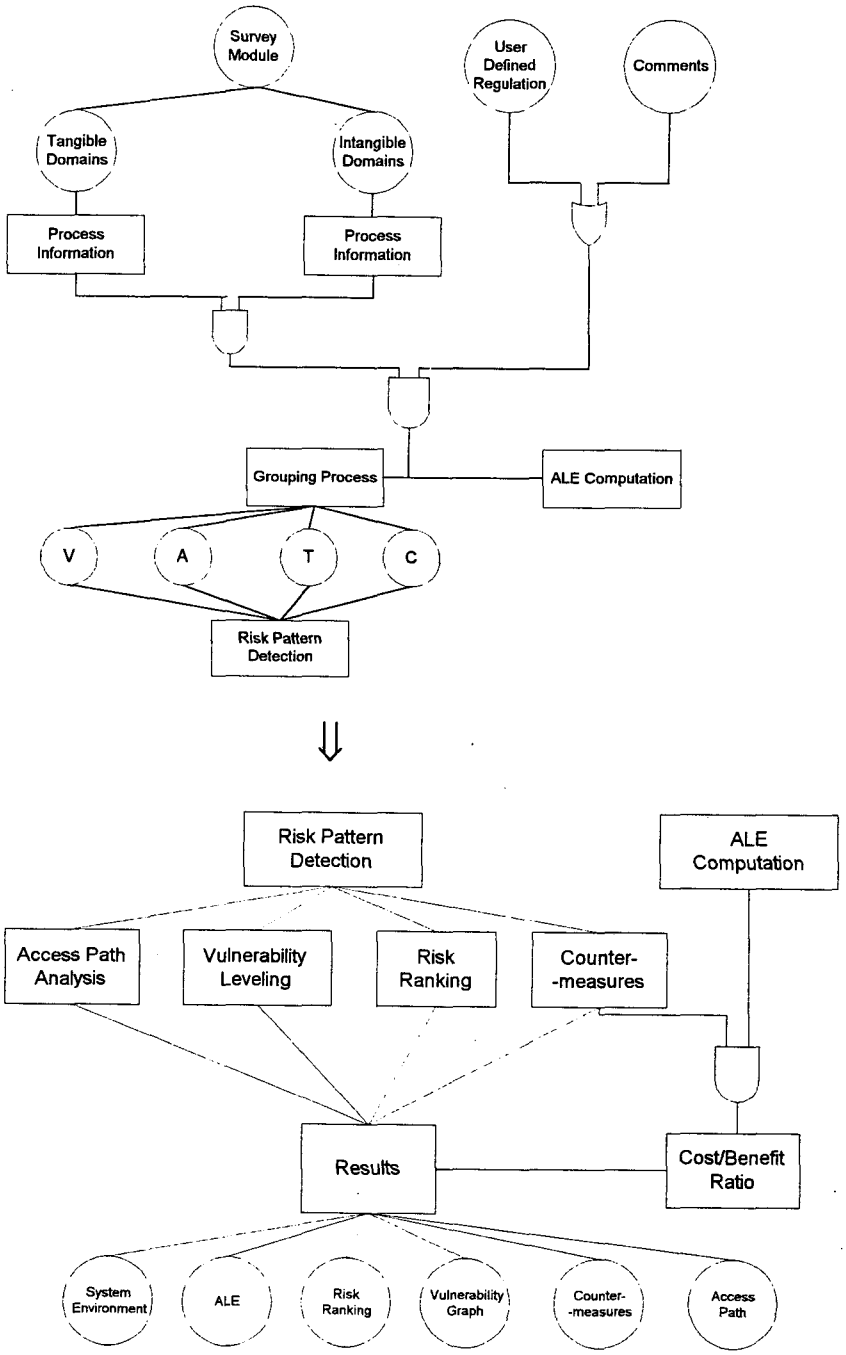

Figure 2.2 Survey, Analysis and Output Process of HAWK System

Vulnerability leveling and ALE

Most of qualitative analysis requires certain scale of numerical or verbal values to be assigned to each of assets and safeguards. In HAWK system, these scaling values are called "weight" and assigned in Expert module holding RISK DB. Each countermeasure is given weight value, and used to compute the vulnerability level.

VL : Vulnerability Level
C : Countermeasure suggested by HAWK
C* : Countermeasure implemented in Target System
W : Weight scaled by High/Medium/Low
P : Value of Asset
Tf : Threat Frequency

$$Sn = \sum_{n} Cn \bullet Wn, \qquad S^*n = \sum_{n} C^*n \bullet Wn$$

$$VL = \frac{(Sn - S^*n)}{Sn} \quad \text{where } 0 < VL < 1$$

Therefore, possible impact can't be greater than asset's value.

HAWK suggests two different types of ALE computation. One suggested by NIST FIBS PUB 65 is widely accepted. Therefore, HAWK system produce ALE suggested by NIST, and compute ALE of its own.

For reference, ALE suggested by NIST is following.

Loss valuation of an incident		Estimated frequency of occurrence	
$10	I = 1	Once in 300 years	f = 1
$100	I = 2	Once in 30 years	f = 2
$1,000	I = 3	Once in 3 years	f = 3
$10,000	I = 4	Once in 100 days	f = 4
•		•	
•		•	

The annualized loss expectancy is then approximated by

$$ALE(NIST) = 10(f + I - 3) / 3$$ [3][4]

Another ALE suggested by HAWK is the following.

$$ALE(HAWK) = VL \bullet P \bullet Tf$$

Since $0 < VL < 1$, total impact can not be greater than asset's value.

By computing two different ALEs, HAWK provides analyst to compare two values and make better decision. Because ALE provided by HAWK is dependent on the vulnerability level, computed value is more associated with the target environment, and gives fairely reasonable values.

4. Future Developments and Discussion

HAWK system is the first automated risk analysis tools developed in Korea. It is currently on-going project, and basic functions of Preview, Survey, Analysis and Output modules are implemented. However, RISK DB, which is used by Expert Module, are still being updated to give more precise knowledge to Analysis Module of HAWK system. In Expert Module, if we have enough risk analysis data and experience, Artificial Intelligence techniques such as Fuzzy Logic[8] and Neural Network could be used to provide more accurate weight value to decide importance of asset and countermeasures. These techniques are currently used in many financial risk analysis tools in U.S. Cost-benefit analysis capability is to be added by the beginning of the next year to assist risk management process. The security mechanism for SURVEY DB needs to be implemented by using either encryption or authentication.

5. References

[1] Frederick G. Tompkins, "How to Select a Risk Analysis Software Package", Datapro, McGraw-Hill, December, 1995

[2] Gunnar Wahlgren, "An Object-Oriented Approach to an IT Risk Management System", Proceedings of the IFIP TC11, Chapman & Hall, 1995

[3] Jackson K. M., Hruska J. and Parker, D.B., Computer Security Reference Book, CRC Press, 1992.

[4] Love Ekenberg, Mats Danielson, "Handling Imprecise Information in Risk Management", Proceedings of the IFIP TC11, Chapman & Hall, 1995

[5] Michael J. Cerullo & Virginia Cerullo, "EDP Risk Analysis", Computer Audit Journal, 1994

[6] Ozier, Will, "Issues in Quantitative Versus Qualitative Risk Analysis", Datapro, McGraw-Hill, Vol. 1, No. IS20-25, January, 1994

[7] Perry, William E. and Kuong, Javier F., EDP Risk Analysis and Control Justification, Management Advisory Publications, 1981

[8] W.G.de Ru and J.H.P. Eloff, "Risk Analysis Modelling with the Use of Fuzzy Logic", Computers & Security Vol. 15, No. 3, pp. 239~248, Elsevier Science Ltd. 1996

[9] Zenkins, Budddy, Security Analysis and Management Manual, Countermeasures Inc, 1994

[10] Description of Automated Risk Management Packages, NIST/NCSC Risk Management Research Laboratory, March 1991

[11] Guidelines for the Management of IT Security, ISO(International Organisation for Standardisation)/IEC(International Electrotechnical Commission) JTC 1 / SC27 / WG1(Work Group Meeting) N391, October 1993