通信情報保護學會論文誌
第 8 卷 第 3 號, 1998. 9

Security Evaluation Criteria for Firewalls in Korea

Cheol Won Lee*, Ki Yoong Hong*, Hak Beom Kim*, Kyeong Hee Oh*,
Hyun Jo Kwon*, Joo Geol Sim*

Abstract

Recently, to use the evaluated firewall is recognized as a solution to achieve the security and reliability for government and organizations in Korea. Results of firewall evaluation using ITSEC (Information Technology Security Evaluation Criteria) and CCPP (Common Criteria Protection Profile) have been announced. Because there are problems to apply ITSEC or CCPP for the firewall evaluation in Korea environment, Korea government and Korea Information Security Agency (KISA) decided to develop our own security evaluation criteria for firewalls. As a result of the efforts, Korea firewall security evaluation criteria has been published on Feb. 1998. In this paper, we introduce Korea security evaluation criteria for firewalls. The criteria consists of functional and assurance requirements that are compatible with CC Evaluation Assurance Levels (EALs).

Keywords : criteria, evaluation, firewall, security functional requirements, assurance requirements, evaluation level

I. Introduction

Information security measures to protect information in network environment is divided into three categories: computer security (COMPUSEC), communication security (COMMSEC), and network security (NETSEC). COMPUSEC include computer security, database security, and a single security function product. These measures may be considered from legal and institutional aspect, management aspect, and technical aspect.

Examples of information protection measures from legal aspect are US's Computer Security Act, Germany's Federal Data Protection Act, and Korea's Framework Act on Informatization Promotion. Examples of information protection from institutional aspect are US's TPEP (Trusted

* Korea Information Security Agency

Product Evaluation Program) and Great Britain's UK IT Security Evaluation and Certification Scheme. Information protection from the management point of view is carried out through means of security planning, risk analysis, and audit trail to provide efficient protection of an organijation's important information. Information protection from technical aspects refers to information protection application technology such as identification and authentication, access control, integrity, encryption, audit trail, key management, and firewall[1].

Nowadays, security evaluation is becoming more and more important in order to guarantee performance and reliability of an information system's security functions. For evaluation of information security products, there are TCSEC, ITSEC, and CTCPEC developed by U.S., Europe, and Canada respectively.

In this paper, we introduce firewall security evaluation criteria developed by Korea Information Security Agency (KISA) to establish Korea information security evaluation scheme.

The paper comprises 5 chapters. The first chapter is an introduction, the second chapter looks at information technology security evaluation criteria of various countries, and the third chapter describes Korea firewall security evaluation criteria. The fourth chapter compares Korea firewall security evaluation criteria with those of other countries and the last chapter puts forward the conclusion.

II. Evaluation Criteria of other countries

A. The United States

The U.S. TCSEC (Trusted Computer System Evaluation Criteria), also commonly known as the Orange Book, in 1983 and adopted DoD 5200.28-STD after making a few revisions in 1985[2]. TCSEC has divided secure computer system into 7 classes (D, C1, C2, B1, B2, B3, and A1) which enables DOD to distribute secure and reliable computer systems to DOD and sub-agencies. Also, DOD has recommended to each organization to adopt and operate secure computer system that satisfies their requirements. Fundamental computer security requirements for TCSEC are security policy, marking, identification, accountability, assurance, and continuous protection.

TCSEC has defined requirements for each level by four categories: security policy which defines the system must perform, accountability that support the security policies, and assurance, and documentation.

In order to evaluate every diversifying information security systems, the U.S. has created TNI (Trusted Network Interpretation of the TCSEC) which is the evaluation criteria for information security system on the network[3], TDI (Trusted DBMS Interpretation of the TCSEC) which is the evaluation criteria for databases[4], and Computer Security Subsystem Interpretation of the TCSEC which is the evaluation criteria for subsystems that only satisfy TCSEC evaluation criteria partially[5]. The U.S. has also created FC (Federal Criteria) to compile 4 types of evaluation criteria into single evaluation criteria through joint efforts with NSA (National Security Agency) and NIST (National Institute of Standard and Technology) in 1992[6]. But, FC was not enacted and was instead included in the overall effort to create CC (Common Criteria).

B. Europe

Great Britain, Germany, France, and the Netherlands agreed to create so called Harmonized Criteria in order to reduce time, labor, and cost caused by different evaluation criteria and recognition methods for information security products. They created ITSEC (Information Technology Security Evaluation Criteria) version 1.2 in 1991[7]. Unlike TCSEC, ITSEC aimed to evaluate all information security products according to a single set of criteria. ITSEC urged developers to develop security functions with consideration of the environment in which the products will be used or to use security functions already defined by TCSEC or Germany's ZSIEC (Criteria for the Evaluation of Trustworthiness of Information Technology System). Evaluation of the products is carried out with only assurance portion of criteria.

Security functions defined by ITSEC are made up of 5 types of functions such as F-C1, F-C2, F-B1, F-B2, and F-B3 for the compatibility with TCSEC and additional 5 types of functions such as F-IN (integrity), F-AV (availability), F-DI (data integrity during data exchange), F-DC (confidentiality of data during data exchange), and F-DX (confidentiality and integrity of the information to be exchanged) that use security function of Germany's ZSIEC.

ITSEC's assurance requirements are based on effectiveness and correctness of criteria. Refer to reference[7] for more information.

ITSEC has 7 levels, namely E0, E1 (the lowest), E2, E3, E4, E5, and E6 (the highest) and level E0 represents inappropriateness.

C. International CC(Common Criteria)

Six countries, the U.S., Canada, France, Germany, the Netherlands, and Great Britain recognized the need to integrate various evaluation criteria such as TCSEC, ITSEC, CTCPEC, and FC as well as the need to reduce the cost and time spent by the different evaluation criteria. These six countries agreed to develop Common Criteria in 1993. Currently version 2.0 is released and, based on this version, efforts for standardization are underway by ISO/IEC JTC1 SC27 WG3. CC is composed of 5 parts. Part 1 gives introduction and general models. Part 2 describes security functional requirements, Part 3 describes assurance requirements, Part 4 describes already defined protection profile and Part 5 includes procedure to register protection profile [8,9,10,11].

Security function requirements include security audit (FAU), non-repudiation of origin or receipt (FCO), user data protection (FDP), cryptographic support(FCS), identification and authentication (FIA), security management (FMT), privacy (FPR), protection of trusted security functions (FPT), resource utilization (FRU), TOE (Target of Evaluation) access (FTA), and trusted path/channels (FTP). Assurance requirements include configuration management (ACM), delivery and operation (ADO), development (ADV), guidance documents (AGD), life-cycle support (ALC), tests (ATE), vulnerability assessment (AVA), and maintenance of assurance (AMA).

The rating scales, from assurance perspective, in CC include the following levels; EAL1, EAL2, EAL3, EAL3, EAL4, EAL5, EAL6, and EAL7. EAL0 means inappropriateness. Detailed infor-

mation on each level is described in reference [8, 9, 10].

III. Korea's Firewall system Evaluation Criteria

Korea is preparing evaluation of information security systems based on Article 15 of The Framework Act on Informatization Promotion, which was enacted in 1995, and Enforcement Ordinance 16 of the same Act. As a part of this attempt, KISA has developed evaluation criteria for firewall and evaluate firewall in the February of 1998. The reason that Korea has developed independent firewall evaluation criteria instead of using ITSEC or CCPP is as follows.

- Required hierarchical rating scale on firewall security functions.
- There are problems in adopting ITSEC or CCPP in Korea.
- Cumulate know-how related to information security evaluation system by operating its own evaluation criteria.

KISA has defined security requirements (identification and authentication, access control, confidentiality, integrity, audit trail, security management) and assurance requirement (development process, configuration management, test process, operational environment, guidance document, vulnerability) for each level. Defined security and assurance requirements are developed into 7 levels to be compatible with information security evaluation criteria, to be developed in near future, and CC.

The firewall evaluation criteria will be the first of such case along with CC but it will be different from CC in that it pursues to have hierarchical rating scales, not the protection profile that CC has adopted.

A. Background of the Development of Firewall evaluation criteria

In the mid 1990s, Internet became very popular in Korea. As a result people started to apply Internet to various field including collecting and processing information, and analyzing collected information. However, unauthorized copying, modifying and deleting information stored in system through computer crimes and Internet hacking caused serious problems to users. As a result, securely operating and maintaining of National computer network and Industry network has been highlighted. Also for Internet users, measures to protect systems and stored information from illegal activities such as hacking has became a necessity.

Government organizations including government-affiliated organizations realized that it is necessary to provide information to people through Internet and started to provide web services. At the same time they are collecting information in the web and using collected information to process given tasks on the Internet. As the Korea Information Infrastructure(KII) is being established, national public network would be integrated and Electronic Commerce in KII is applied, computer incidences such as hacking, unauthorized modifying, unauthorized access and unauthorized destroying information will be increased as expected. Therefore, organizations planning to establish KII and organizations trying to provide information services by integrating many organizations computer network is requiring a method to protect their systems from illegal activities such as hacking and computer

crime.

To fulfill some requirements mentioned above, Korea government and KISA decided to use evaluated firewalls. We tried to apply ITSEC and CCPP to evaluate firewalls for Korea networks environment. However, it was unlikely to apply each of them for the firewall evaluation due to the different requirements in Korea. Thus, Korea Evaluation Criteria and Evaluation Manual for firewalls have been developed to test confidence of the firewall security functions.

B. Structure of the Firewall evaluation criteria

The evaluation criteria for the firewall is created to meet Korean environment with consideration to the factors described in Figure 1.

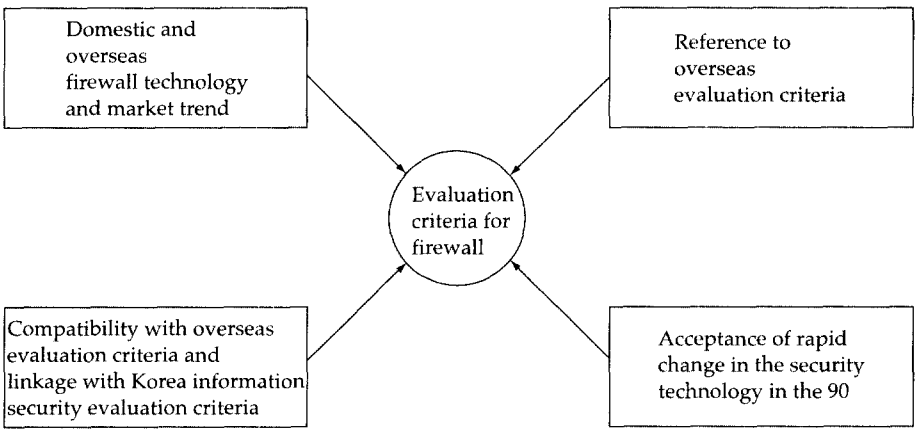


Figure 1. Evaluation criteria considerations

The evaluation criteria for the firewall propose the barometer for evaluating security functions required of a firewall. The security functional requirements and assurance requirements defined in the evaluation criteria of the firewall for each level are the minimum requirements that must be satisfied in order to be evaluated to that specific level.

B.1 Security functional requirements

Security functions provided by the firewall can be categorized into 6 classes; identification and authentication, access control, integrity, confidentiality, audit trail, and security management.

- **Identification and Authentication**

  Identification and authentication is a function that certifies the identity of the user that tries to access the objects in and out of the network through the firewall.

- **Access control**

  Access control is a function that controls the access by a subject to an object according to access control rules. It is formed by discretionary access control, mandatory access control, and sensitivity label. Discretionary

access control is a function that controls access by a subject to object based on the access authority and identity of a subject or an object when an access is tried on the internal and external network through the firewall. Mandatory access control is a function that controls access by a subject to an object based on the sensitivity label of the subject and object when access to the object is tried either in the internal or external network through the firewall. The security label here represents the security level of the subject and object and is the basis for the application of mandatory access control rules.

- **Integrity**

  Integrity is the protection of important security related data inside the firewall and the data transmitted through the firewall from unauthorized changes. It is composed of requirements for data integrity of data inside the firewall and transmitted data. With the integrity function, it must be possible to detect the unauthorized change to the data that was transmitted through the firewall or the unauthorized change to the security related data inside the firewall.

- **Confidentiality**

  During the transmission, data is exposed to the users that do not have the necessary authority but the confidentiality function prevents exposure of information in the transmitting process. However, organizations using firewall in Korea could decide whether to use confidentiality function or not. Therefore, confidentiality function is provided as an option. But, when the confidentiality function is provided, regardless of the level, source code or the drawing of the hardware must be submitted.

- **Logging and audit trail**

  Logging and audit trail records, investigates, and reviews the user's security-related events and activities. The logging audit trail function is composed of recording of events, management of audit record file, process of security infringement activities, and intrusion detection.

- **Security management**

  Security management function comprises security functions that only certified administrator can carry out and that are needed to securely manage security-related data within the firewall.

B.2 Assurance requirements

Objective of assurance requirements is to measure the confidence level of the security function that is implemented by the firewall. Assurance requirements include development, test, configuration management, operation environment, guidance document, and vulnerability which is generated during the life cycle of the firewall.

B.2.1 Development Process

Development process of a firewall system is composed of functional specifications, basic design, detailed design, and implementation processes. The person requesting the evaluation must submit materials for each step of the devel-

opment process.

- **Functional specifications**

  The functional specification step is the first step in the development of a firewall. This step includes creation of security target document for the firewall and the functional specification documents that can satisfy the security requirements that are described in the security target document. The functional specification document must describe external interfaces and operation of the security functions that the firewall possesses.

- **Basic design**

  The basic design step deals with designing and defining the higher level of the firewall. Definition and design of the higher level refers to specifying of basic structure, interface, and important hardware and software components of the firewall.

- **Detailed design**

  Detailed design step includes design details of the firewall that are used in implementation in terms of hardware and as well as the basis for the software programming. The components specified during this process are called modules. Software and hardware are made based on these modules. The specification of the firewall is defined in more detail as the detailed design process continues and the detailed design must be done in a way that preserves the intention of the architectural design.

- **Implementation**

  Detailed design of the firewall is realized both in terms of hardware and software programming during the implementation process. During the implementation process of the firewall, the verification for the consistency among various documents produced during each process of development must be provided.

B.2.2 Test Process

The developer of the firewall tests the security functions in order to confirm whether all the security functions and mechanism work the way they are supposed to in order to be able to respond to potential risks listed in the security target document. At the same time, the developer tests whether the system works efficiently as a whole security system.

B.2.3 Configuration management

Configuration management is a management method used to control the changes made to software in the development, production, and maintenance process. It must be required to prove integrity of the developed firewall.

B.2.4 Operational environment

Operational environment is composed of installation process and operational procedure requirements of the firewall.

- **Installation process**

  The installation process of the firewall is made up of installation procedures to construct the firewall. This process must be pro-

vided to guarantee there has been no change in the provided security functions during installation.

- **Operational procedure**

  Operational procedure carried out by a system administrator in order to operate firewall securely. Procedures for system administrator's routine jobs and special task must be defined. Routine job includes start-up, back-ups and maintenance of firewall. Special task includes restart of system by unexpected breakdown and recovery of lost data. Also, for the maintenance and up grade of a system, replacement, addition and revision procedure must be specified.

B.2.5 Guidance document

The guidance document is an important means of communication between developers and users of the firewall. Assurance requirements for the guidance document can be broken down into user guidance document and system administration guidance document.

B.2.6 Vulnerability

Assurance requirements for the vulnerability are composed of vulnerability analysis and misuse analysis of the firewall.

- **Vulnerability analysis**

Various vulnerabilities such as deactivating, bypassing, corrupting, or circumventing of the security functions and mechanisms can take place during the development of a firewall. Therefore, the developer must carry out the vulnerability analysis of known vulnerabilities and prove that the developed firewall is protected from such vulnerabilities. Known vulnerabilities refer to those that are published in the public domain such as various hacking methods against the firewall and other methods that can subvert the security functions of the firewall by infiltrating the system.

- **Misuse analysis**

  Misuse analysis is used to evaluate whether the firewall can be configured, installed, or used in a manner that is insecure. The purpose of the misuse analysis is to minimize the possibility of human or other errors that can negatively affect the security functions of the firewall and to minimize the possibility of wrongly constructing or installing the firewall without the users and administrators knowing about it.

C. Characterization of Evaluation Levels

The level of firewall evaluation is determined according to the implemented security functions in the firewall and according to the degree of confidence of the firewall's development process, test process, configuration management, operational environment, guidance document, and vulnerability. Depending on the security functional requirements and assurance requirements, evaluation level is divided into 7 levels: K1, K2, K3, K4, K5, K6, and K7. K1 represents the lowest level and K7 represents the highest. As mentioned before, confidentiality can be provided optionally at all evaluation levels. Letter E is attached to represent provision of confiden-

tiality; K1E, K2E, K3E, K4E, K5E, K6E, and K7E.

The following are the characteristics of each level.

- **Level K0**

  Level K0 means that the firewall evaluation result does not satisfy the requirements of the level.

- **Level K1**

  Level K1 must provide the minimum level of security functions of firewall such as identification and authentication for the system administrator and discretionary access control for all connection requests. Level K1 also requires security management mechanism to protect internal data of the firewall such as administrator's identification and authentication data and discretionary access control rule. For assurance requirements, level K1 also requires informal security target document, functional specification, test document, configuration management document, and manuals for user and administrator must be provided. Test document should state test plan, test procedures, and test results for security functions. Configuration management document should state configuration items and configuration identification method.

- **Level K2**

  Level K2 should satisfy the requirements of the level K1. Level K2 requires capability to create and maintain audit records on security related activities. Level K2 also requires discretionary access control on the all the data packets transferred through firewall. Security management function for logging and audit trail is also required. Developer is required to submit informal basic design document. And if there are many different installation methods, developer must specify each installation method and its effect on system security including secure startup, backup and maintenance. For analysis of obvious vulnerabilities, developer must perform vulnerability analysis. Evaluator also must conduct penetration test based on each obvious vulnerability. Developer must analyze if the firewall installation, startup, and operation documents are contradict or inconsistent to each other. Evaluator should repeat any procedures based on developer's analysis.

- **Level K3**

  Level K3 must satisfy the requirements of the level K2. Level K3 requires ability to check whether there has been any modification to the important data inside the firewall and transmitted data. Also, it must be possible to summarize and print audit records. Developer must submit detailed design document for security mechanisms. Developer also must submit configuration management document which states configuration management system and configuration change control method which was applied in the development process of the firewall. Evaluator should conduct penetration test based on the evaluator's analysis results on known vulnerabilities.

- **Level K4**

  Level K4 should satisfy all the requirements of the level K3. Level K4 requires the identification and authentication function that

protects the system from the reply attacks. Level K4 also requires integrity of the security label and mandatory access control for all connection requests through the firewall. Developer must submit source code and/or hardware drawing. Also, developer must submit the document to verify that the source code and/or detailed specification is correspondence to each other. For level K4, evaluator should conduct all the test procedures stated in the test document to see if all the security functions meet the K4 level requirements. One of the special characteristics of the K4 level is that the evaluator should analyze all the submitted documents and conduct penetration test by himself. Evaluator also should try to install and operate all the procedures stated in the documents to perform misuse analysis of the firewall.

- **Level K5**

  Level K5 should satisfy all the requirements of the level K4. At the same time, mutual authentication function and mandatory access control for transmission must be provided for level K5. Formal model of system security policy must also be provided. Functional specification, basic design, and detailed design must be written in semi-formal. Developer must track following three issues. Firstly, for each development phases, developer must prove that every documents created during each phase corresponds with each other. Secondly, audit information must be maintained for every change in the configuration. Lastly, a method to control configuration change using configuration management tool must be provided.

- **Level K6**

  Level K6 must fulfill the requirements of the level K5. Level K6 require a function that can detect intrusion by an outsider. Developer must describe detail design specification using layering, abstraction and data hiding techniques.

- **Level K7**

  Level K7 must satisfy all the requirements of level K6. At this level, functional specification and architectural design must be written in the formal so it is synchronized with formal model of system security policy. Also, all the tools used during the development phases must be subject to configuration control. In level K7, security functional requirement does not exist.

D. Evaluation Criteria Summary

The summary of the requirements for each level of the evaluation criteria is shown in the figure 2.

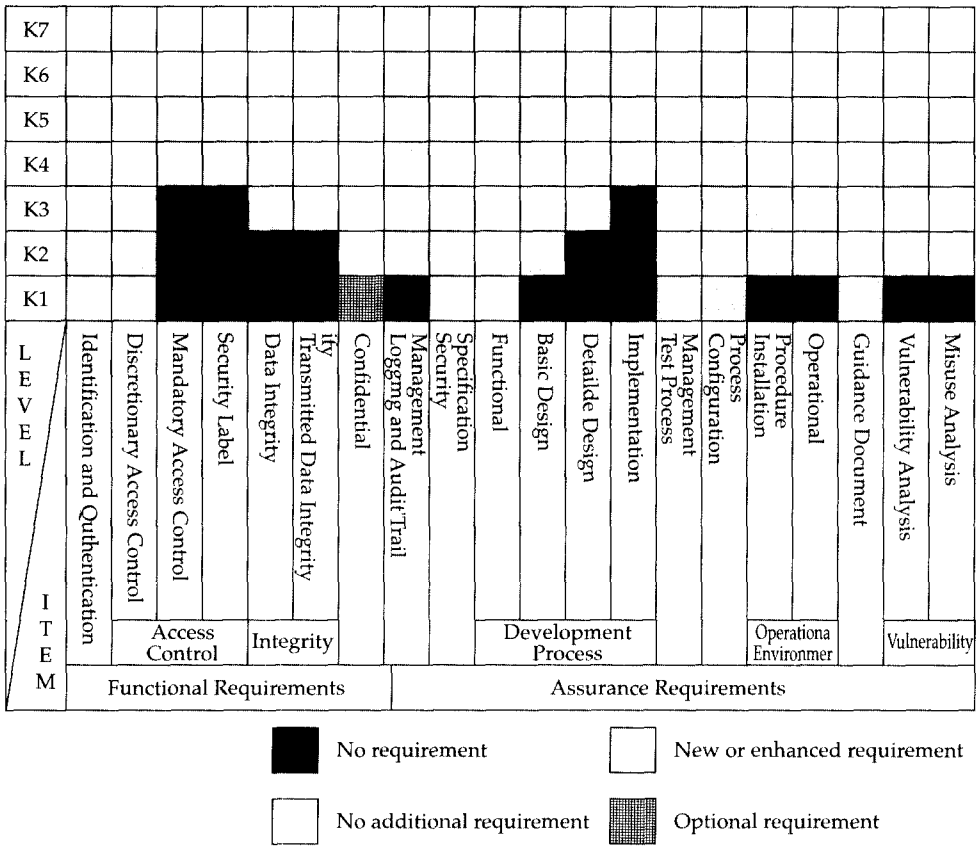


Figure 2. Summary of the firewall evaluation criteria

IV. Comparison between domestic and overseas information technology security evaluation criteria

In this chapter, we will analyze and compare the evaluation criteria of Korea and other countries described in the prior chapters. Depending on the perspective of the one who make analysis and comparison, the result might be different from what we have stated on this chapter. And depending on where one puts more emphasis on between evaluation criteria and evaluation scheme, the result also might differ. Figure 3 shows the comparison on assurance between US TCSEC and FC, Canada's CTCPEC, Europe's ITSEC, CC that is currently being standardized as an international standard, and Korea's firewall evaluation criteria.

The U.S.				Canada	Europe	International		Korea	
TCSEC		FC / PP		CTCPEC	ITSEC	Common Criteria		Firewall Evaluation Criteria	
D	Minimal protection				E0 Inadequate Assurance	EAL0 EAL1	Inadequate Assurance / Functionally Tested	Inadequate Assurance / Minimal Protection	K0 / K1 (E)
C1	Discretionary Security Protection				E1, F-C1	EAL2	Structurally Tested	Audit Trail Enhanced	K2 (E)
C2	Controlled Access Protection	CS-1	T1	T1	E1, F-C2	EAL3	Methodically Tested and Checked	Intergrity Enhanced	K3 (E)
B1	Labelde Security Protcction	LP-1 CS-2 CS-3	T1 T2 T3	T2 T3	E3, F-B1	EAL4	Methodically Designed,Tested , and Reviewde	Identification and Authentication Enhanced	K4 (E)
B2	Structure Protection	LP-2	T5	T4	E4, F-B2	EAL5	Semiformally Designed and Tested	Access Control Enhanced	K5 (E)
B3	Securtiy Domain	LP-3	T6	T5	E5, F-B3	EAL6	Semiformally Verifide Design and Tested	Intrusion Detection Enhanced	K6 (E)
A1	Verified Design	LP-4	T7	T6 T7	E6, F-B3	EAL7	Formally Verifide Design and Tested	Verifide Protection	K7 (E)

Figure 3. Comparison of evaluation criteria from various countries

As can be seen from Figure 3, Korea's evaluation criteria for firewall is the most unique firewall evaluation criteria in the world which has the 7 levels of hierarchical rating scale structure. Of course, organizations (such as Canada's CSE, UK's CESG, US's NSA, and CC) in other countries are also developing the firewall evaluation criteria with the protection profile method. But, these criteria do not have hierarchical rating scale structure and can only determine whether the evaluation has succeeded or failed. Therefore, it is very difficult to choose a firewall that can be suitable for various users requirements in various information network environments such for unclassified information, SBU (Sensitive But Unclassified) information, or for classified information. It is also very difficult to satisfy different security requirements of various users. However, Korea's firewall evaluation criteria have 7 levels by accepting various security require-

ments and assurance requirements and therefore are able to provide the basis for provision of adequate firewall that befits the required security level of a user. Korea's firewall evaluation criteria have also given consideration to compatibility with CC that is being standardized by international organizations for standardization (ISO).

V. Conclusion

Some countries have outstanding results to evaluate information security products such as TCSEC (U.S), ITSEC (Europe), and CTCPEC (Canada). These countries (U.S, Canada, U.K, France, Germany, and Netherlands) are currently leading the world in the fields of security evaluation by developing harmonized common criteria as an international standard.

past some years, Korea government and organizations had necessities to use evaluated security products for their own purposes. Korea government and Korea Information Security Agency (KISA) decided to develop our own security evaluation criteria after deep consideration on previously developed security evaluation criteria. As a result of efforts, we developed Korea Security Evaluation Criteria and Manual to apply them to evaluate firewalls for Korea environments. On Feb. 1998, we have set up the Korea evaluation scheme by publishing the firewall security evaluation criteria and manual to start evaluation activities for firewalls.

In this paper, we introduced the background, structure, characteristics, and brief summary of Korea Firewall Security Evaluation Criteria. Also, comparison among all existing security evaluation criteria was presented.

Currently, we are trying to build Korea Information Security Evaluation Criteria (KISEC) based on the accumulated knowledge and experience gained from the evaluation activities.

We will pay close attention to security worldwide trends in standardizing evaluation criteria and actively participate in the activities of International Organizations for Standardization.

References

[1] K. Y. Hong, The Evaluation and Certification System of Information Security Systems, 2nd Symposium on Information Security, 1997.

[2] National Computer Security Center, Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, Dec., 1985.

[3] National Computer Security Center, Trusted Network Interpretation of The TCSEC, NCSC-TG-005, Jul., 1987.

[4] National Computer Security Center, Trusted DataBase Management System Interpretation of the TCSEC, NCSC-TG-02, Apr., 1991.

[5] National Computer Security Center, Computer Security Subsystem Interpretation of the TCSEC, NCSC-TG-009, Sepl., 1988.

[6] National Institute of Standard and Technology and National Security Agency, Federal Criteria for Information Technology Security, Vol. I, Dec., 1992.

[7] France, Germany, The Netherlands, and The United Kingdom, Information Technology Security Evaluation Criteria, Version 1.2, Jun. 1991.

[8] Common Criteria Implementation Board, Common Criteria for Information Technology Security Evaluation, Part 1 : Introduction and General Model, Version 2.0, May 1998.

[9] Common Criteria Implementation Board, Common Criteria for Information Technology Security Evaluation, Part 2 : Security Functional Requirements, Version 2.0, May 1998.

[10] Common Criteria Implementation Board, Common Criteria for Information Technology Security Evaluation, Part 3 : Security Assurance Requirements, Version 2.0, May 1998.

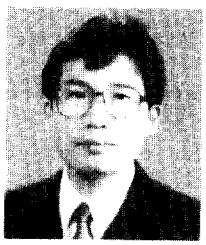
[11] Common Criteria Editorial Board, Common Criteria for Information Technology Security Evaluation, Part 4 : Predefined Protection Profiles, Version 1.0, Jan. 1996.

□ 著者紹介

이 철 원

1987년 2월 충남대학교 수학과(학사)
1989년 8월 중앙대학교 대학원 전산학과(석사)
1989년 9월 - 1996년 6월 한국전자통신연구소 선임연구원
1996년 6월 - 현재 한국정보보호센터 선임연구원

※ 주관심분야 : 컴퓨터 · 네트워크 보안, 정보보호시스템 평가체계, 정보보호기술 표준화



홍 기 웅

1985년 2월 전남대학교 전자계산학과(학사)
1990년 2월 중앙대학교 대학원 전자계산과(석사)
1994년 4월 정보처리기술사
1996년 2월 아주대학교 컴퓨터공학과(박사)
1985년 9월 - 1995년 10월 한국전자통신연구소 선임연구원
1992년 - 1993년 이태리, Alenia Spazio사 Senior Researcher
1995년 10월 - 1996년 4월 한국전산원 선임연구원
1996년 4월 - 현재 한국정보보호센터 책임연구원, 기술기준팀장

※ 주관심분야 : 컴퓨터 · 네트워크 보안, 정보시스템 위험분석 · 평가, 정보보호 표준화

김 학 범

1988년 2월 경기대학교 전자계산학과(학사)
1990년 2월 중앙대학교 대학원 전자계산학과(석사)
1996년 3월 - 현재 아주대학교 대학원 컴퓨터공학과 박사과정 재학중
1991년 10월 - 1996년 6월 한국전산원 주임연구원
1996년 7월 - 현재 한국정보보호센터 선임연구원

※ 주관심분야 : 컴퓨터 · 네트워크 보안, 정보보호시스템 평가체계, 정보보호 표준화

오 경 희

1988년 2월 서강대학교 전자계산학과 (학사)
1992년 2월 한국과학기술원 전자계산학과(석사)
1995년 11월 CISA
1992년 10월 - 1996년 12월 한국통신 멀티미디어연구소 전임연구원
1996년 12월 - 현재 한국정보보호센터 주임연구원

※ 주관심분야 : 정보보호시스템 평가체계, 정보시스템 감사, 위험분석 및 관리

권 현 조

1997년 2월 성균관대학교 정보공학과(학사)
1998년 3월 - 현재 성균관대학교 정보통신대학원 재학중
1995년 11월 CISA
1997년 1월 - 1997년 7월 (주)나라계전 연구소, 연구원
1997년 7월 - 현재 한국정보보호센터 연구원

※ 주관심분야 : 정보보호시스템 평가체계, 네트워크 보안, 전자서명

심 주 걸

1957년생
중앙대학교 전자공학과(학사)
건국대학교 대학원 전자공학과(석사)
성균관대학교 정보공학과 박사과정재학중
현재 한국정보보호센터 근무

※ 관심분야 : 정보보호시스템 기준·평가 암호이론