A Study on Assumptions for Operational Environment of OS Security Enhancement System

Tai-Hoon Kim, Min-Chul Kim, Nam-Kyun Baik and Jae-Sung Kim

78, Garak-Dong, Songpa-Gu, Seoul, Korea

(Tel : +82-2-405-{5323, 5345, 5367, 5420}; E-mail: {taihoon, mckim, namkyun, jskim}@kisa.or.kr)

Abstract: Trusted operating systems (OS) provide the basic security mechanisms and services that allow a computer system to protect, distinguish, and separate classified data. Trusted operating systems have been developed since the early 1980s and began to receive National Security Agency (NSA) evaluation in 1984. The researches about trusted OS are proceeding over the world, and new product type using the loadable security kernel module (LSKM) or dynamic link library (DLL) is being developed. This paper proposes a special type of product using LSKM and specific conditions for operational environment should be assumed.

Keywords: Common Criteria, Protection Profile, OS security product, Assumption for environment

1. INTRODUCTION

Trusted operating systems (OS) provide the basic security mechanisms and services that allow a computer system to protect, distinguish, and separate classified data. Trusted operating systems have been developed since the early 1980s and began to receive National Security Agency (NSA) evaluation in 1984.

Trusted OS may lower the security risk and the threat to the security holes of implementing a system that processes classified data. Trusted OS can implement some security policies and accountability mechanisms in an OS package via integrated or micro kernel type. A security policy is the rules and practices that determine how sensitive information is managed, protected, and distributed [1-2]. Accountability mechanisms are the means of identifying and tracing who has had access to what data on the system so they can be held accountable for their actions.

In these days, the trusted OS is not used widely as a commercial purpose. But the researches about trusted OS are proceeding over the world, and new product type using the loadable security kernel module (LSKM) or dynamic link library (DLL) is being developed and some of such products are introduced.

This paper proposes a special type of product using LSKM and specific conditions for operational environment should be assumed.

2. TRUSTED OPERATING SYSTEM

Trusted OS may be used to implement mandatory access control (MAC) via multi-level security (MLS) systems and to build security countermeasures that allow systems of different security levels to be connected to exchange mutual data. Using of a trusted OS may be the way that a system can be connected to other high security systems. Department of Defense (DoD) security regulations define what evaluation criteria must be satisfied for a multi-level system based on the lowest and highest classification of the data in a system and the clearance level of the users of the system. Using an NCSC-evaluated system reduces accreditation cost and risk. The security officer identified as the Designated Approving Authority (DAA) for secure computer systems has the responsibility and authority to review and approve the systems to process classified information. The DAA will require analysis and tests of the system to assure that it will operate securely. The DAA can accept the NCSC evaluation of a system rather than generating the data. For a B3 or A1 system, which can represent a savings of 1 to 2 years in schedule and the operating system, will provide a proven set of functions.

This technology has been implemented by several vendors for commercial-off-the-shelf (COTS) use in secure systems. As of September 1996, the NCSC Evaluated Product List indicated that fourteen OS have been evaluated as level C2, B1, B2, and B3 systems in the last three years [3]. The number of OS evaluated by class (excluding evaluations of updated versions of OS) is included in the table 1 [4]. Using of one of the approved trusted OS can result in substantial cost and schedule reductions for a system development effort and provide assurance that the system can be operated securely.

The heavy access control and accounting associated with high security systems can affect system performance; as such, higher performance processors, I/O, and interfaces may be required. Trusted OS have unique interfaces and operating controls that require special security knowledge to use and operate. Frequently COTS products that operate satisfactorily with a standard operating system must be replaced or augmented to operate with a trusted operating system [5].

Table 1 NCSC Evaluation criteria classes.

Class	Title
A1	Verified Design
B3	Security Domains
B2	Structured Protection
B1	Labeled Security Protection
C2	Controlled Access Protection
C1	Discretionary

3. USAGE CONSIDERATIONS AND CONSTRAINTS

Some systems included in the level C1 and C2 provide limited discretionary access controls and identification and authentication mechanisms. Discretionary access controls (DAC) identify who can have access to system data based on the need to know. But mandatory access controls (MAC) identify who or what process can have access to data based on the requester having formal clearance for the security level of the data. A low-level system is used when the system only needs to be protected against human error and it is unlikely that a malicious user can gain access to the system.

Some systems included in the level B2, B3, A1 provide

complete mandatory and discretionary access control, thorough security identification of data devices, rigid control of transfer of data and access to devices, and complete audit of access to the system and data. These higher level systems are used when the system must be protected against a malicious user's abuse of authority, direct probing, and human error [2]. The portion of the trusted OS that grants requesters access to data and records the action is frequently called the reference monitor because it refers to an authorization database to determine if access should be granted. Higher level trusted operating systems are used in MLS hosts and compartmented mode workstations.

4. EVALUATION CRITERIA AND EVALUATION

The multipart standard ISO/IEC 15408 defines criteria, which for historical and continuity purposes are referred to herein as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use is tolerable.

The CC is presented as a set of distinct but related parts as identified below.

4.1 Part 1 Introduction and General Model

Part 1, Introduction and general model, is the introduction to the CC. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. In addition, the usefulness of each part of the CC is described in terms of each of the target audiences.

4.2 Part 2 Security functional requirements

Part 2, Security functional requirements, establishes a set of functional components as a standard way of expressing the functional requirements for TOEs (Target of Evaluations). Part 2 catalogues the set of functional components, families, and classes.

4.3 Part 3 Security assurance requirements

Part 3, Security assurance requirements, establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance components, families and classes. Part 3 also defines evaluation criteria for PPs (Protection Profiles) and STs (Security Targets) and presents evaluation assurance levels that define the predefined CC scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

In support of the three parts of the CC listed above, it is anticipated that other types of documents will be published, including technical rationale material and guidance documents.

5. PROTECTION PROFILE

5.1 Overview of Protection Profile

A PP defines an implementation-independent set of IT security requirements for a category of TOEs. Such TOEs are intended to meet common consumer needs for IT security. Consumers can therefore construct or cite a PP to express their IT security needs without reference to any specific TOE [5-7].

The purpose of a PP is to state a security problem rigorously for a given collection of systems or products (known as the TOE) and to specify security requirements to address that problem without dictating how these requirements will be implemented. For this reason, a PP is said to provide an implementation-independent security description. A PP thus includes several related kinds of security information (See the Fig. 1).

A description of the TOE security environment which refines the statement of need with respect to the intended environment of use, producing the threats to be countered and the organisational security policies to be met in light of specific assumptions.

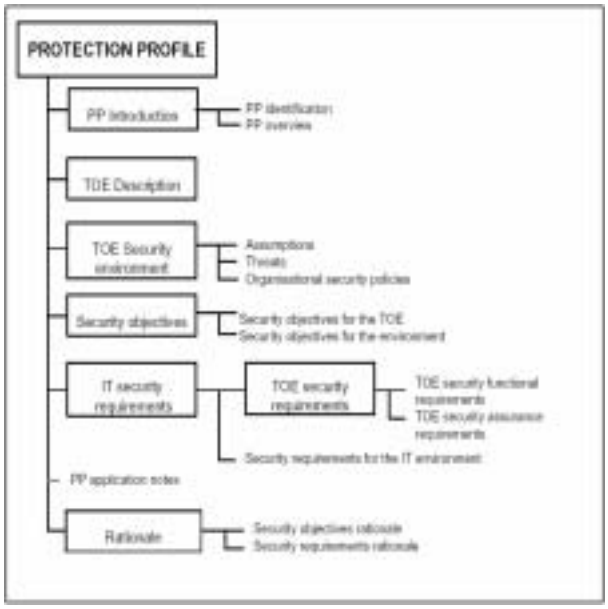

Fig. 1 Protection Profile content

5.2 TOE Security Environment

ISO/IEC 15408 defines the requirements for the content of this part of a PP in [15408-1], subclause B.2.4 and C.2.4. The wording of these two sections is identical, which can be taken as an indication that the expected content of the TOE Security Environment section does not differ greatly between a PP and an ST.

The purpose of the TOE Security Environment section is to define the nature and scope of the definition of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed, i.e. the security concerns, to be addressed by the TOE.

TOE security environment will therefore involve a discussion of:

a) assumptions made regarding the TOE security environment, thereby defining the scope of the security concerns;

b) the assets requiring protection (typically information or resources within the IT environment or the TOE itself), the identified threat agents, and the threats they pose to the assets;

c) any organisational security policies or rules with which the TOE must comply in addressing the security concerns.

Subsequent sections of the PP show how the security concerns will be addressed by the TOE, in combination with its operating environment. It is therefore important to ensure that the security concerns are clearly and concisely defined - otherwise you may end up with a PP that addresses the wrong concerns.

5.3 How to Identify and Specify the Assumptions

ISO/IEC 15408 requires the TOE Security Environment section of a PP to contain a list of assumptions about the TOE security environment or the intended usage of the TOE. To compile such a list, we first need to ask the following question:

"What assumptions are we making about the TOE security environment and the scope of the security concerns?"

For example, it may be necessary to make some assumptions in order to ensure that a potential threat to an asset is not, in practice, relevant in the TOE security environment. The following types of assumption should be included:

a) aspects relating to the intended usage of the TOE;
b) environmental protection of any part of the TOE;
c) connectivity aspects;
d) personnel aspects.

Other assumptions may be included where these have had a material effect on the PP content, for example assumptions which led to the choice of the assurance requirement. However, it must be remembered that ISO/IEC 15408 requires that the formally identified assumptions have to be shown to be upheld by the security objectives. General assumptions which cannot be traced to security objectives may nonetheless be usefully included within the descriptive (informative) text in the PP.

It is unlikely that we will be able to completely identify all the assumptions we are making in a single attempt. Rather, we should expect to be identifying additional assumptions throughout the development of the PP. In particular, when constructing the PP rationale, we should consider whether we are making any assumptions that have not been stated in the PP.

When adopting this iterative approach to identifying assumptions, it is important to avoid the inclusion of any assumptions relating to the effective use of specific TOE security functions that we identify in the process of constructing the rationale. Such detail would be more appropriately included as security requirements for the non-IT environment.

It is, however, reasonable to state as a personnel assumption that the TOE has one or more administrators who are assigned responsibility for ensuring the TOE security functions are configured and used appropriately.

For ease of reference, it is recommended that each assumption is numbered or otherwise uniquely labeled.

6. NEW PRODUCT TYPE

There are some products may use the loadable security kernel module or dynamic link library to enhance the security for operating system. But these products are not the trusted OS because the target of evaluation is not the OS itself. Next Fig. 2 is the block diagram these products use.

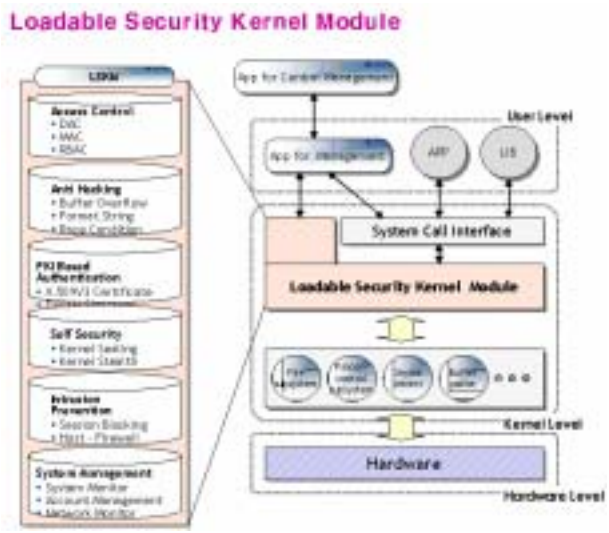

Fig. 2 Block Diagram of these Products

So the new name of this product category is needed, and we propose the new name as “Operating System Security Enhancement System(OS SES).”

7. ASSUMPTIONS FOR OPERATION ENVIRONMENT

Even though there may be very many assumptions for operation environment of OS SEP, next items may be some of them. These assumptions are related to the Labeled Security Protection Profile.

7.1 Physical Assumptions

TOEs (from now on, TOE is OS SES in this paper) intended for application in user areas have physical control and monitoring. It is assumed that the following physical conditions will exist:

A.LOCATE : The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorised physical access.

A.PROTECT : The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

7.2 Personnel Assumptions

It is assumed that the following personnel conditions will exist:

A.MANAGE : There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NO_EVIL_ADM : The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and

abide by the instructions provided by the administrator documentation.

A.COOP : Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

7.3 Procedural Assumptions

About the Mandatory Access Controls, MAC is dependent upon the establishment of procedures. It is assumed that the following procedural controls exist.

A. CLEARANCE : Procedures exist for granting users authorization for access to specific security levels.

A. SENSITIVITY : Procedures exist for establishing the security level of all information imported into the system, for establishing the security level for all peripheral devices (e.g., printers, tape drives, disk drives) attached to the TOE, and marking a sensitivity label on all output generated.

7.4 Connectivity Assumptions

It is assumed that the following connectivity conditions exist:

A.PEER : Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. OS SES-conformant TOEs are applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain.

A.CONNECT : All connections to peripheral devices reside within the controlled access facilities. OS SES-conformant TOEs only address security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

8. CONCLUSION AND FUTURE WORK

For the Evaluation of IT products or systems, ISO/IEC 15408 (Common Criteria) requires PP or ST, and the TOE Security Environment section of a PP or ST contains a list of assumptions about the TOE security environment or the intended usage of the TOE.

In this paper, we proposed a new product type and specific conditions should be assumed to exist in OS SES environment and the meaning of those conditions.

REFERENCES

[1] Russel, Deborah & Gangemi, G.T. Sr. Computer Security Basics. Sebastopol, CA: O'Reilly & Associates, Inc., 1991.

[2] Abrams, Marshall D., Jajodia, Sushil and Podell, Harold J. Information Security An Integrated Collection of Essays. Los Alamitos, CA: IEEE Computer Society Press, 1995

[3] Trusted Product Evaluation Program Evaluated Product List [online]. Available WWW <URL: http://www.radium.ncsc.mil/tpep/index.html> (1996).

[4] White, Gregory B.; Fisch, Eric A.; & Pooch, Udo W. Computer System and Network Security. Boca Raton, FL: CRC Press, 1996.

[5] Trusted Operating Systems, Software Technology Review, SEI, CMU. Available WWW <URL : http://www.sei.cmu.edu/str/descriptions/trusted_body.html>

[6] ISO. ISO/IEC 15408-1:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[7] ISO. ISO/IEC 15408-2:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[8] ISO. ISO/IEC 15408-3:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements