운영체제보안시스템의 개념 및 운영 가정사항

김태훈, 김상호, 김재성

A Concept and Operational Assumptions of OS Security Enhancement System

Tai-hoon Kim[*], Snag-ho Kim[*], Jae-sung Kim[*]

Abstract

Trusted operating systems (OS) provide the basic security mechanisms and services that allow a computer system to protect, distinguish, and separate classified data. This paper proposes a new concept of operating system security enhancement system which uses loadabel security kernel module (LSKM) or dynamic link library (DLL) and specific conditions for operational environment should be assumed.

Key Words: Trusted OS, LSKM, OS Security Enhancement System

[*] 한국정보보호진흥원

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 [1-4]. 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 new concept of operating system security enhancement system which uses loadabel security kernel module (LSKM) or dynamic link library (DLL) 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.

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.

5. 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.

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.

6. OS security enhancement system

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.1 is the block diagram these products use.

So the new name of this product category is needed, and we propose the new name as Operating System Security Enhancement System.

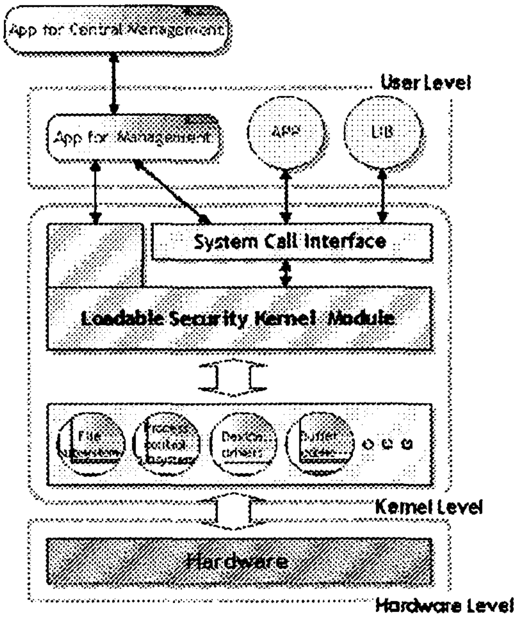

Fig.1 Block diagram of system

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.

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

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.

Reference

[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

● 저자소개 ●

김태훈
1995　성균관대학교 공과대학 전기공학과 학사
1997　성균관대학교 공과대학 전기공학과 석사
2002　성균관대학교 공과대학 전기전자및컴퓨터공학부 박사
1996~1999 신도리코 기술연구소 연구원
2002~현재 한국정보보호진흥원 선임연구원
관심분야: 보안공학

김상호
1994　명지대학교 전자공학과 학사
1997　연세대학교 전자공학과 석사
2002　연세대학교 컴퓨터・산업시스템공학과 박사수료
1994 ~1996 한국생산기술연구원 연구원
1996 ~현재 한국정보보호진흥원 선임연구원
관심분야: 정보보호제품 평가, 보안공학

김재성
1986　인하대학교 전산학과 학사
1989　인하대학교 전산학과 석사
1989 ~1990　LG 정보통신 중앙연구소 연구원
1990 ~1995　한국전자통신연구원(ETRI) 선임연구원
1995 ~1996　한화정보통신 중앙연구소 선임연구원
1996 ~현재　한국정보보호진흥원 지원기획팀장
관심분야: 정보보호제품 평가, 정보보호기술