SecuROS/FreeBSD 기반 다단계 사용자 인증 시스템

두 소 영[†] · 김 정 녀[†] · 공 은 배[††]

요 약

본 논문에서는 비밀번호 인증만을 사용하는 시스템의 취약점을 보완한 다단계 사용자 인증 시스템을 구현하였다. 제안된 다단계 사용자 인증 시스템은 사용자의 아이디/비밀번호, 스마트카드 그리고 접근제어 정보 등의 4단계 인증이 사용된다. 본 논문에서 제시하는 사용자 인증 시스템은 FreeBSD 커널에 접근제어 기능을 추가한 SecuROS/FreeBSD를 바탕으로 개발되었다. 사용자에 따라 시스템에 접근할 수 있는 범위를 제한하는 기능과 중요 정보를 입력할 때 그 요청이 시스템에서 요청한 것임을 확인할 수 있는 기능을 제공하여 신뢰성을 높였다. SecuROS/FreeBSD 시스템에는 강제적인 접근제어와 역할기반 접근제어가 사용되고 있어서 시스템에 접근하는 사용자는 접근하고자 하는 접근제어 정책에 대한 정보도 인증에 사용된다. 이때, 사용자가 요청한 접근제어 정보가 시스템에 정의된 접근제어 규칙에 모두 만족하는 경우에만 시스템 접근이 허가 된다.

Multiple User Authentication based on SecuROS/FreeBSD

Soyoung Doo[†] · JongNyeo Kim[†] · EunBae Kong[††]

ABSTRACT

This paper implements Multiple User Authentication System to which the system authenticating with password only has been upgraded. The 4-staged authentication including user ID, password, smart card and access control information, etc. is used at the suggested Multiple User Authentication System. The user authentication system that this paper suggests has been developed based on SecuROS/FreeBSD with the function of access control added to FreeBSD kernel. It provides both the function to limit access range to the system to each user and the function to check that when inputting important information the demand is the one of the system ; thus, the reliability becomes increased. In the SecuROS/FreeBSD system, MAC and RBAC are being used. So, in the case of users accessing to the system, the information about the policies of MAC and RBAC to which users would access is used in the authentication. At the time, the access to system is permitted only when the access control information that users demanded satisfies all the access control rules which have been defined in the system.

키워드 : 신뢰경로(Trusted Path), 사용자 인증(User Authentication), 강제적인 접근제어(Mandatory Access Control), 역할기반 접근제어(Role Based Access Control)

1. 서 론

다수의 사용자가 하나의 시스템에 접근하는 형태인 유닉스 계열의 시스템에서 공격자들은 자원과 정보를 오용하고자 시스템의 헛점을 계속 탐색하여 이를 이용하려고 한다. 대부분의 시스템에서는 사용자 인증의 수단으로 비밀번호를 사용하고 있는데 이것은 많은 사람들이 공감하는 문제점을 가지고 있다. 우선, 사용자가 기억하기에 용이한 전화번호, 생일, 취미, 이름과 관련된 단어들이 자주 비밀번호로 선택되는데 이것은 악의를 가진 사용자가 추측해 내거나 공격용 프로그램으로 쉽게 알아 낼 수 있다. 또한, 비밀번호는 실제서명과 달리 전달되는 문자만을 비교하게 되므로 개인의 고유성을 확인하기에는 부족함이 있다. 비밀번호의 이러한 위험성을 줄이고자 시스템에 접근할 때마다 비밀번호를 변경하는 일회용 비밀번호(one-time password)와 시스템이 랜덤한 값을 생성하여 주는 비밀번호 자동 생성기 등이 대안으로 제시되고 있으나 이렇게 생성된 비밀번호는 사용자가 기억하기에 어려움이 있다. 그 외에도 비밀번호로 문자열을 사용하는 방법(passphrase), 감사기능(Audit), 비밀번호 갱신 규칙, 최근 접속 시간을 배너로 보여주는 것 등이 비밀번호의 취약성을 보완하는 방법으로 제시되고 있으나, 그 효과는 만족스럽지 못하다.

사용자 인증을 강화하기 위한 또 다른 방안으로는 비밀번호와 함께 다른 인증방법을 사용하는 것이 있다. 은행에서 사용되는 현금 인출기와 같이 비밀번호와 마그네틱 카드를 통

† 정 회 원 : 한국전자통신연구원 보안운영체제연구팀
†† 정 회 원 : 충남대학교 컴퓨터공학과 교수
논문접수 : 2002년 5월 23일, 심사완료 : 2002년 12월 18일

해서 사용자를 확인하는 방법이 그 대표적인 예라고 할 수 있다. 스마트카드, 지문인식, 홍채인식, 음성인식, 화상인식 등이 인증에 활용할 수 있는 하드웨어이다. 하드웨어를 사용하는 방법은 복잡성을 높임으로써 인증의 강화 효과를 가지는 수단이 된다. 이 중 스마트카드는 저장 내용을 임의로 수정하기에 어려운 메모리를 가지고 있고, 프로세서를 포함하고 있어서 내부에서 연산이 가능하다는 장점을 가지고 있다

또한, 사용자 인증에서는 사용자와 시스템간의 신뢰경로가 보장되어야 한다. 신뢰 경로란 사용자에게 제공되는 인증 요청 메시지가 악의적인 프로그램에서 생성한 허위 메시지가 아닌 시스템에서 생성한 메시지임을 확인시킬 수 있는 방법과 사용자가 입력하는 내용이 시스템에게만 전달된다는 것이 보장되는 것을 의미한다. 현재 이러한 신뢰성이 보장되는 인증 시스템의 대표적인 예는 마이크로 소프트사의 윈도우 NT 로그인(login) 프로그램이다. 이 인증 프로그램은 동작되는 동안 다른 모든 프로세스를 멈추고 인증 처리 프로세스만을 동작시키는 방법으로 처리되고 있다. 다수의 사용자가 시스템을 사용하는 경우 로그인은 빈번히 발생할 것인데 로그인 프로그램이 동작하는 동안 모든 프로세스가 동작을 멈추는 것은 효과적인 처리라고 할 수 없다. 또한 제공된 로그인 프로그램이 시스템에서 발생된 명령어임을 증명하는 기능은 제공하지 못하고 있다. 본 논문에서 제안하는 인증 시스템은 역할기반 접근제어 정책을 이용하여 신뢰경로 기능을 제공한다.

본 논문에서는 사용자 인증을 강화하는 수단으로 다단계 인증 방법을 사용하고 있다. 다단계 인증 방법은 커널 수준의 접근제어 시스템을 바탕으로 기존의 유틸리티를 수정하여 개발 되었다. 다단계에 사용되는 다중인자로는 비밀번호, 스마트카드, 그리고, MAC(Mandatory Access Control)과 RBAC(Role Based Access Control) 속성값이 사용된다.

2장에서는 TCSEC B2 등급의 사용자 인증에 대한 내용을 설명하고, 3장에서는 접근제어 시스템SecuROS/FreeBSD에 대해 설명하고 4장에서는 다단계 인증시스템에 대해서 설명하고 5장에서 결론과 향후 연구방향을 설명한다

2. TCSEC에서의 B2 등급 사용자 인증

본 논문에서 개발된 다단계 사용자 인증 시스템은 현재 가장 널리 알려져 있는 표준안인 TCSEC(Trusted Computer System Evaluation Criteria)[1]에서 구분하고 있는 7단계의 보안등급 중 B2 등급에 맞춰져 있다.

TCSEC의 보안등급은 각 단계에 따라 보안 내용도 차이점을 가지는데 인증 방법은 다음과 같은 3가지 타입으로 분류되고 각 단계에 따라 한가지 타입 혹은 두 가지 이상의 조합을 통해 인증을 수행할 것을 요구하고 있다.

- 타입 1은 '사용자가 알고 있는 것' 즉, 비밀번호, 비밀문구, 개인식별번호 등을 사용하여 인증하는 방법을 의미한다.
- 타입 2는 '사용자가 가지고 있는 것' 즉, 실제 키 또는 전자적인 키를 사용하거나 마그네틱 카드, 또는 배지 등을 사용하여 인증하는 방법을 의미한다.
- 타입 3은 '사용자 자신을 나타내는 것' 즉, 지문인식, 망막, DNA 패턴 등을 사용하여 인증하는 방법을 의미한다.

다중 요소 인증은 이중 2가지 또는 3가지 인증을 혼합하여 강화된 인증기법을 제공하는 것이다. 2가지 요소 인증은 'ATM 카드 + 개인 식별번호', '신용카드 + 서명', '개인 식별번호 + 서명' 등의 조합을 예로 들 수 있고, 3가지 요소인증은 '스마트카드 + 비밀번호 + 지문'을 예로 들 수 있다.

본 논문에서는 TCSEC에서 어느 정도 강력한 보안이 보장된다고 평가되는 B2 등급 이상을 만족하기 위해서 위의 타입 중 2가지를 혼합하여 사용한다. 선택된 2가지 인증방법은 비밀번호와 스마트카드이다. 스마트카드에 저장된 데이터의 읽기, 쓰기는 접근 제한 규칙을 두어 조건이 맞는 경우에만 사용할 수 있도록 하였다. 또한, 스마트카드 리더기는 시리얼포트에 접속되는 외장형이고, 리더기에 전구가 부착되어 있어서 사용자는 전원이 켜지고 꺼지는 동작을 볼 수 있다.

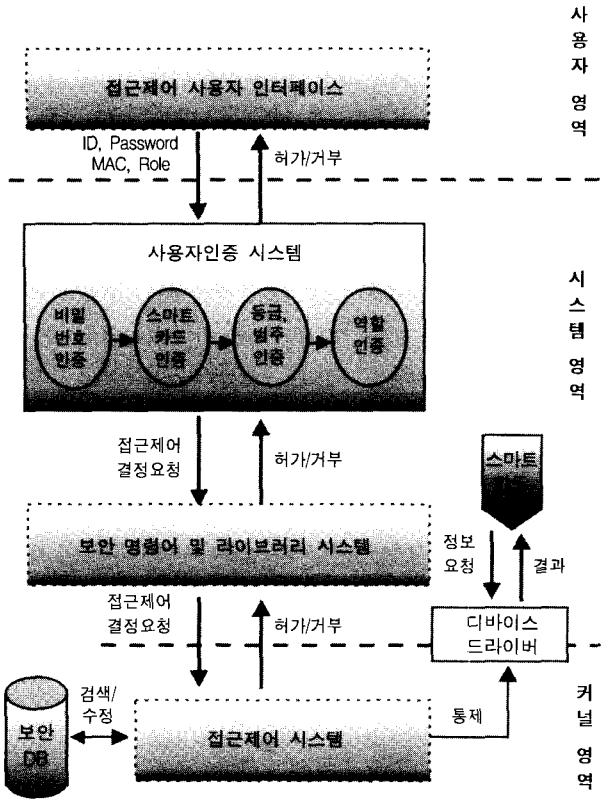
3. 접근제어 시스템

본 논문에서 제안하는 사용자 인증 시스템은 SecuROS (Secure & Reliable OS)/FreeBSD 시스템을 기반으로 하고 있다. SecuROS/FreeBSD는 FreeBSD 4.3 커널에 접근제어 관련 모듈을 추가한 보안운영체제 시스템이다.

보안운영체제란 운영체제 상에 내재된 보안상의 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템 보호를 위하여 기존의 운영체제 내에 보안기능을 추가한 운영체제를 말한다. 보안운영체제를 사용하여 얻을 수 있는 가장 큰 장점은 외부 공격자들 뿐만 아니라 내부 사용자들이 시스템 자원의 오용을 사전에 방지할 수 있다는 것이다.

구현된 보안운영체제 시스템의 자원과 정보에 접근하기 위해서는 접근제어 시스템의 허가를 얻어야만 한다. 즉, 관련

된 모든 시스템 호출은 접근제어 시스템을 통해서 허가된 경우에만 처리된다. (그림 1)은 보안운영체제 시스템의 구성도이다.



(그림 1) 보안운영체제시스템 구성도

사용자는 접근제어 사용자 인터페이스를 통해 시스템 자원에 설정된 접근제어 관련 정보를 설정하거나 확인할 수 있다. 접근제어 사용자 인터페이스는 접근제어 명령어 및 라이브러리를 통해서 커널에 접근제어 설정 및 확인 요청을 보낸다.

접근제어 시스템은 MAC(Mandatory Access Control)과 RBAC(Role Based Access Control)을 사용하고 접근제어 결정자와 접근제어 적용자로 구성되었다. 접근제어 결정자는 접근요청을 한 주체와 객체에 대한 설정 내용을 보안데이터베이스에서 검색하고 검색된 내용을 보안 규칙에 따라 적합한지 판단하게 된다. 접근제어 시스템은 MAC과 RBAC에 대한 주체의 접근 요청이 모든 조건에 대해 허가되는지 검사한다. 이 중 하나라도 거부되면 접근이 허락되지 않는다. 접근제어 시스템은 접근제어 처리를 수행할 때 보안데이터베이스를 참조하는데, 보안데이터베이스에는 MAC과 RBAC에 대한 속성값이 들어있다.

접근제어 결정자는 주체가 해당 자원에 접근권한이 있는지를 검사하여 그 결과를 접근제어 적용자에게 보낸다. 접근제어 적용자는 접근제어 결정자로부터 전달 받은 접근 결정 정보를 가지고 사용자가 해당 자원에 접근할 수 있게 이 내용을 보안데이터베이스에 추가하거나 또는 접근할 수 없음을 접근제어 명령어 및 라이브러리 시스템에 전달한다.

접근제어 명령어 및 라이브러리 시스템에서는 전달받은 내용을 주체 즉, 사용자에게 표준 입출력을 통해서 알린다[2]. 사용자가 객체에 대한 접근제어 권한을 검색한 경우, 결과가 허가였다면 사용자는 검색된 보안 정보 내용을 볼 수 있고, 그렇지 않은 경우 권한이 없음을 알리는 메시지를 전달 받는다. 또한, 사용자가 객체에 대한 접근제어 설정을 요청하였다면, 결과가 허가인 경우 정상적으로 설정되었다는 메시지를 받고 거부인 경우 오류메시지를 전달 받는다.

개발된 보안운영체제 시스템에서 사용되는 MAC과 RBAC에 관한 내용은 다음과 같다.

BLP 모델[3-5]의 ss-property와 *-property 원칙을 따르는 MAC에서는 주체(프로세스)와 객체(파일, 디렉토리, 디바이스 등의 시스템자원)들에게 등급과 범주를 주고 이 등급과 범주를 기준으로 낮은 수준의 등급과 범주를 갖는 주체가 높은 수준의 등급과 범주를 가지는 객체를 읽을 수 없도록 하거나 높은 수준의 등급과 범주를 갖는 주체가 낮은 수준의 등급과 범주를 가지는 객체를 쓸 수 없도록 하여 접근이 허가되지 않는 정보의 유출을 막아 기밀성을 보장한다.

RBAC[6]에서는 임의의 역할에 대한 접근 속성을 가지는 객체에 주체가 접근하기 위해서는 그 해당 역할의 멤버가 되는 주체 만이 접근 할 수 있다. 보안관리자 역할을 두어 시스템에 역할을 설정하거나 중요 정보의 속성값을 설정하는 것은 보안관리자 역할로 설정된 사용자 만이 가능하도록 하였다.

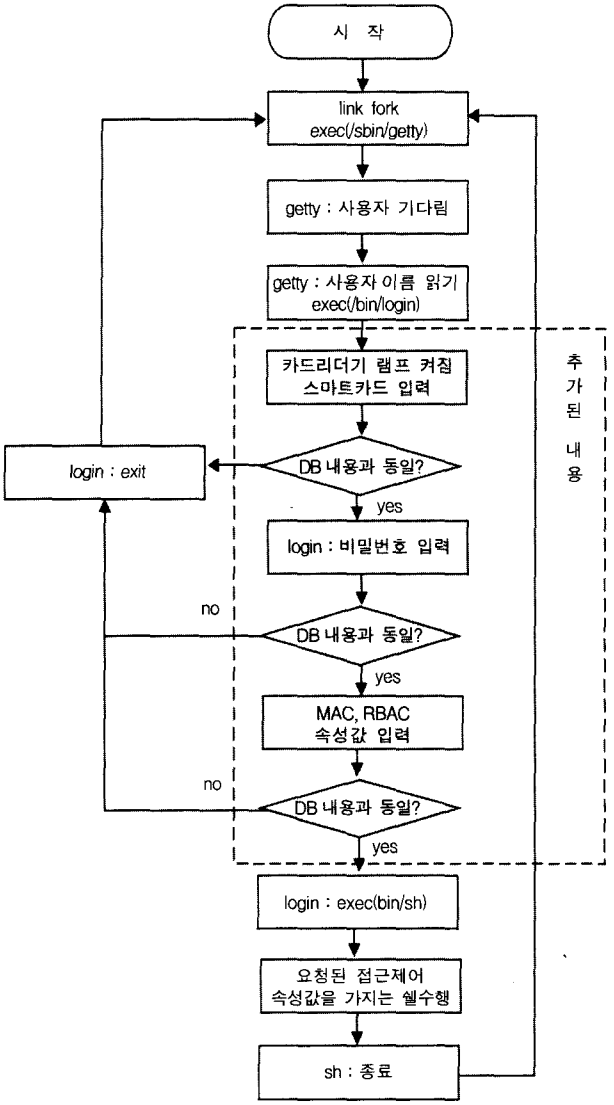
기존의 유닉스 계열 시스템에서 super user되면 모든 객체에 접근하거나 조작할 수 있던것과 달리 본 시스템에서는 super user일지라도 접근조건을 만족하는 경우에만 객체에 접근 또는 조작이 가능하다. 모든 보안 정보를 안전하게 관리하기 위해서 본 시스템에서는 보안 정보를 저장하기 위한 보안데이터베이스 파일을 사용하였고 이 파일들은 특정 위치에 저장한 후 보안 관리자만이 접근할 수 있도록 하였다.

4. 다단계 사용자 인증 시스템

다단계 사용자 인증 시스템은 사용자 아이디/비밀번호, 스마트카드, 그리고 접근제어 속성값 중 MAC의 등급과 범주, RBAC의 역할 정보로 구성되었다. (그림 2)는 시스템에 접

근하는 사용자 인증의 절차를 순서도로 나타낸 것이다.

init 프로그램이 getty 프로그램을 각각의 터미널 또는 콘솔에 실행시키게 되고 getty는 로그인 하려는 사용자가 있는지 살피며 기다리게 된다. 사용자가 아이디를 입력하면 getty는 login 프로그램을 수행시킨다.



(그림 2) login 프로그램 생성과 추가된 내용

본 논문에서는 FreeBSD의 login 프로그램을 수정하여 다단계 사용자 인증 시스템을 구현하였다. (그림 2)와 같이 login 프로그램에서는 먼저, 사용자에게 스마트카드 입력을 요청한다. 스마트카드 리더기는 접근제어 시스템에 의해서 접근이 제한된다. 보안관리자는 스마트카드 리더기 디바이스 드라이버에 'login_manager' 역할을 할당하고, login 프로그램에도 'login_manager' 역할로 상속(i---) 속성값을 할당하였다. 'login_manager' 역할이 할당된 디바이스 드라이버에는 'login_manager' 역할을 가지고 있는 주체만이 접근할 수 있다.

login 프로그램이 getty에 의해서 수행되면 login 프로그램이 가지고 있는 'login_manager' 역할이 프로세스에도 상속된다. 설정된 'login_manager' 역할은 login 프로그램이 종료되면 자동으로 삭제된다. 프로세스가 'login_manager'로 설정되어 있기 때문에 login 프로그램에서는 스마트카드에 입력된 카드의 데이터를 읽을 수 있고 카드리더기의 전구를 켜고 끌 수 있다.

사용자가 카드를 입력하면 카드리더기의 전구에는 불이 들어오게 된다. 스마트카드 인증이 완료되면 인증 시스템은 사용자의 비밀번호를 요청한다.

사용자는 카드리더기의 전구에 불이 켜진 것을 보고 메시지가 시스템으로부터 전달된 것임을 확인 할 수 있다. 만약 카드리더기의 전구가 켜지지 않은 상태에서 비밀정보를 요구하는 경우에는 가짜 login(fake login) 프로그램으로 의심해 볼 수 있다.

사용자는 리더기의 전구가 켜진 것을 확인한 후 비밀번호를 입력하게 된다. 입력된 비밀번호가 시스템에 보관된 내용과 같다면, 사용자 인증 시스템에서는 다음 단계로 접근제어 관련 정보를 요청한다. 접근제어 정보로는 MAC의 등급(class)과 범주(category)와 RBAC의 역할 정보를 사용한다. 사용자는 보안관리자로부터 미리 할당 받은 등급, 범주 그리고 역할 내에서 해당 속성값을 입력할 수 있다. 입력된 내용이 보안데이터베이스에 저장된 내용과 동일하거나 허가 범위 내에 있다면, 사용자에게는 요청된 접근제어 속성값을 가지는 프로세스가 할당된다. 만약, 사용자가 등급, 범주 그리고 역할 중 한

〈표 1〉 보안데이터베이스의 내용

사 용 자	최소 등급	최대 등급	범 주	역 할
sydoo	**0**	**5**	**1100111111001**	**backup_manager**
jnkim	2	3	0000000000001	-
ebkong	0	1	0000000000010	-
manager	0	5	111111111111	security_manager

가지라도 허가된 범주를 벗어난 속성값을 입력한다면 사용자 인증은 오류 메시지와 함께 종료되고 이 내용은 로그로 저장된다.

예를 들어 사용자 sydoo가 <표 1>과 같이 최소 0등급, 최대 5등급, 1100111111001 범주, backup_manager 역할로 보안데이터베이스에 설정되어 있을 때, 사용자 인증 단계에서 4등급, 11001 범주, backup_manager 역할을 입력하여 접근을 시도하였다면, 사용자의 접근은 허가된다. 이때 생성된 프로세스는 4등급, 11001 범주, backup_manager 역할의 속성값을 할당 받는다. 프로세스가 4등급, 11001 범주로 수행되었으므로 4등급 이하의 11001 범주 내에 있는 모든 객체에 접근이 가능하고 backup_manager 역할을 선택했으므로 시스템의 데이터를 백업할 수 있다.

만약, 사용자 sydoo가 1등급, 11111111111 범주, security_manager를 선택하였다면, 범주와 역할 속성값이 사용자에게 허가된 내용과 다르므로 접근이 거부된다.

사용자 인증 절차에서 비밀번호는 기존의 유닉스 시스템과 마찬가지로 3번의 재시도를 할 수 있고, 스마트카드, 등급, 범주, 역할 정보에 대한 것은 한번 실패하면 처음부터 다시 시도 하도록 하였다. 사용자 인증 시도는 모두 로그 파일에 기록된다.

6. 결 론

본 논문에서는 다수의 사용자가 접근하는 서버시스템을 위한 다단계 사용자 인증 시스템을 제안하였다. 제안된 인증 시스템은 커널에 구현된 접근제어 시스템을 바탕으로 개발되어 인증의 강화뿐만 아니라 사용자에 따라 보안등급이 다른 정보와 서비스를 제공할 수 있도록 구성되었다. 동일한 사용자라고 할지라도 역할에 따라 등급과 범주에 따라 접근 할 수 있는 정보와 서비스가 달라지게 하여 사용자에게 안전성과 함께 유연성을 제공한다.

본 논문에서는 비밀번호, 스마트카드, 등급과 범주, 그리고 역할 정보를 사용하여 다단계 사용자 인증 시스템을 구성하였다. 사용자와 시스템 간의 신뢰경로를 제공하여 비밀정보의 안전한 전달을 보장한다.

현재까지는 네트워크로 연결된 다른 시스템과의 접속을 배제한 로컬 시스템에서 처리되는 사용자인증 시스템에 대한 내용이 개발되었고 앞으로 원격 시스템에서 접근하는 사용자들을 위한 확장된 개념의 사용자 인증 시스템[9-11]에 대한 연구를 진행할 계획이다. 또한, 인증 단계에서 남긴 로그를 침입탐지 시스템에 적용시킬 수 있도록 하고, 감사추적 기록을 분석한 결과를 인증 단계에서 활용할 수 있는 기술도 지속적으로 연구할 예정이다.

참 고 문 헌

[1] http://www.radium.ncsc.mil/tpep/library/tcsec/index.html.

[2] Jong-Gook Ko, Jeong-Nyeo Kim, and kyo-Il Jeong, "Access Control for Secure FreeBSD Operating System," WISA2001, Vol.2, 2001.

[3] IEEE Std 1003.1e - Draft standard for Information Technology-Portable Operating System Interface (POSIX) Part 1 : System Application Program Interface (API)-Protection, Audit and Control Interfaces.

[4] IEEE Std 1003.2c - Draft standard for Information Technology - Portable Operating System Interface (POSIX) Part 2 : Shell and Utilities : Protection and Control Interfaces.

[5] Roos Lindgreen, Herschberg I. S, "On theValidity of the Bell-Lapadula model," Computer & Security, Vol.13, pp. 317-338, 1994.

[6] Rule Set Based Access Control, http://www.rsbac.de.

[7] David A. Wheeler, "Secure Programming for LINUX and UNIX HOWTO," http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/book1.html.

[8] Simon Wiseman, Phill Terry, Andrew Wood, "The Trusted Path between SMITE and the User," British Crown Copyright, 1988.

[9] Santosh Chokhani, "Trusted Products Evaluation," Communications of the ACM, Vol.35, No.7, July, 1992.

[10] Jeremy Epstein, John Mchugh, Rita Pascale, "A Prototype B3 Trusted X Window System," IEEE, 1991.

[11] Raymon M. Wong, "A Comparison of Secure UNIX Operating System," IEEE, 1990.

두 소 영

e-mail : sydoo@etri.re.kr

1992년 군산대학교 정보통신공학과(학사)

1994년 충남대학교 컴퓨터공학과(석사)

1994년~1997년 대우고등기술연구원

2000년~현재 한국전자통신연구원 보안운영체제연구팀

관심분야 : 접근제어, 시스템 보안, 암호프로토콜, 네트워크보안

김 정 녀

e-mail : jnkim@etri.re.kr

1987년 전남대학교 전산통계학과(학사)

1995년~1996년 Open Software Foundation Research Institute 파견

2000년 충남대학교 컴퓨터공학과(석사)

1988년~현재 한국전자통신연구원 보안운영체제연구팀장

관심분야 : 운영체제, 분산처리, 고장 감내, 시스템 보안

공 은 배

e-mail : keb@ce.cnu.ac.kr

1981년 서울대학교 계산통계학과(석사)

1987년 서울대학교 계산통계학과(학사)

1995년 Oregon State Univ. 전산학과 (박사)

1996년~현재 충남대학교 컴퓨터공학과 정교수

생물정보학 관심분야 : 암호학, 기계학습, 생물정보학