2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

사용자와 시스템간의 신뢰경로가 보장되는 인증시스템

두소영, 고종국, 은성경, 김정녀
한국전자통신연구원 보안운영체제연구팀
e-mail : sydoo@etri.re.kr

The Trusted Path Authentication System between the User and the Secure OS

So-Young Doo, Jong-Gook Ko, Sung-Kyong Un, Jeong-Nyeo Kim
Secure Operating System Team, ETRI

요 약

인증시스템은 보안운영체제시스템을 구성하기 위한 중요한 서브시스템 중의 하나이다. 본 논문에서는 사용자가 시스템에 접근하기 위해서 가장 먼저 거치게 되는 인증 절차 수행에 있어서 허가된 사용자의 접근만을 허용하고, 인증요청 메시지의 진위 여부를 확인시켜주는 기능과 사용자가 입력하는 중요 정보가 다른 사용자에게 유출되지 않도록 보장하는 기능을 추가한 다 단계 사용자 인증방법을 소개한다. 본 논문에서는 역할기반의 접근제어 시스템을 커널 내부에 구성하고, 사용자인증에 비밀번호와 하드웨어 장치인 스마트카드를 사용함으로써 강화된 사용자 인증 시스템을 구현하였다.

1. 서론

유닉스 계열의 시스템은 여러 명의 사용자가 하나의 시스템을 사용하게 되어 개인용 시스템보다 시스템의 자원과 정보에 대한 공격이 빈번히 발생한다. 사용자 인증은 시스템에 허가된 사용자 접근만을 허용하여 시스템 자원의 오용과 남용을 줄이는 목적을 가지고 있다. 현재 유닉스 계열의 시스템에서 가장 흔히 사용되는 사용자 인증 방법은 비밀번호 인증이다. 비밀번호는 다른 사용자에게 유출되거나 유추될 가능성이 높아 시스템에 접근할 때마다 비밀번호를 변경하는 일회용 비밀번호(one-time password)를 사용하는 방법과 시스템이 랜덤한 값을 생성하여 주는 비밀번호 자동 생성기 등이 대안으로 제시되고 있다.
사용자 인증을 강화하기 위한 또 다른 방안으로는 비밀번호와 함께 하드웨어를 사용하는 것이다. 은행에서 사용되는 현금 인출기와 같이 비밀번호와 마그네틱 카드를 통해서 사용자를 확인하는 방법이 그 대표적인 예다. 그 외에도 스마트카드, 지문인식, 홍채인식, 음성인식, 화상인식 등이 마그네틱 카드 대신 고려되는 하드웨어 들이다. 하드웨어를 사용하는 방법은 복잡성을 높인다는 점에서 인증의 강화 효과를 동일하게 가지고 있으나 보다 안전한 인증과 다양한 활용을 위해서 본 논문에서는 스마트카드를 사용하였다.

스마트카드는 저장 내용을 임의로 수정하기에 어려운 메모리를 가지고 있고, 프로세서를 포함하고 있어서 어느 정도 내부적인 연산이 가능하다. 현재 선금식 전화 카드, 핸드폰, 은행, 교통, 인터넷 지불 방식등에 활발히 사용되고 있다.

사용자 인증에서 또 한가지 고려되는 사항은 사용자와 시스템간의 신뢰경로를 제공하는 것이다. 신뢰경로란 사용자에게 제공되는 인증 요청 메시지가 악의적인 프로그램에서 생성한 허위 메시지가 아닌 시스템에서 생성한 메시지임을 확인 시킬 수 있는 방법과 사용자가 입력하는 내용이 시스템에게만 전달된다는 것이 보장되는 것을 의미한다. 현재 이러한 신뢰성이 보장되는 인증 시스템의 대표적인 예는 마이크로소프트사의 윈도우 NT 로그인(login)을 예로 들 수 있다. 이 인증 프로그램은 동작되는 동안 다른 모든 프

로세스를 멈추고 인증 처리 프로세스만을 동작시키는 방법을 사용하고 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 발생한 명령어임을 증명하는 기능은 제공되지 않고 있다.

본 논문에서는 시스템의 동작에 영향을 주지 않으면서 사용자에게 시스템의 명령어임을 확인 할 수 있는 방법과 사용자가 입력하는 중요 정보가 다른 사용자에게 유출되지 않도록 하는 방법과 사용자 인증을 다단계로 하여 보다 강화된 인증 방법을 제공하여 시스템 자원과 정보를 보호하기 위해 구현된 사용자 인증 시스템에 대해서 설명한다.

2 장에서는 표준안에서 제시하고 있는 인증 시스템이 갖추어야 하는 구성 내용을 설명하고 3 장에서 인증시스템을 포함하고 있는 전체 시스템에 대해서 설명하고 4 장에서 개발된 인증시스템에 대해서 설명하고 5 장에서 결론을 통해 정리한다.

2. 표준에서 제안하는 인증시스템의 보안

인증은 사용자 식별을 증명하는 절차를 의미한다. 현재까지 가장 널리 알려져 있는 표준안인 TCSEC (Trusted Computer System Evaluation Criteria)[1]에서 5 단계의 보안등급을 두고 있다.

각 단계에 따라 신뢰성 보장을 위한 방법도 차이점을 가지는데 인증 방법은 다음과 같은 3 가지 타입으로 분류하고 각 단계에 따라 한가지 타입 혹은 두 가지 이상의 조합을 통해 인증을 수행할 것을 요구하고 있다.

타입 1 은 비밀번호, 비밀문구, 개인식별번호 등을 사용하여 인증하는 방법을 의미한다.

타입 2 는 실제 키 또는 전자적인 키를 사용하거나 마그네틱 카드, 또는 배지 등을 사용하여 인증하는 방법을 의미한다.

타입 3 은 지문인식, 망막, DNA 패턴 등을 사용하여 인증하는 방법을 의미한다.

TCSEC 에서 어느 단계이상의 강력한 보안이 보장된다고 평가되는 B2 등급 이상을 만족하기 위해서는 위의 타입 중 2 가지 이상을 혼합하여 사용할 것을 명시하고있다. 예를 들어 마그네틱 카드와 비밀번호를 지원하거나, 질의-응답 시스템을 사용하여 시작되는 개인식별번호나 생체인식장비가 조합적으로 사용되어야 한다.

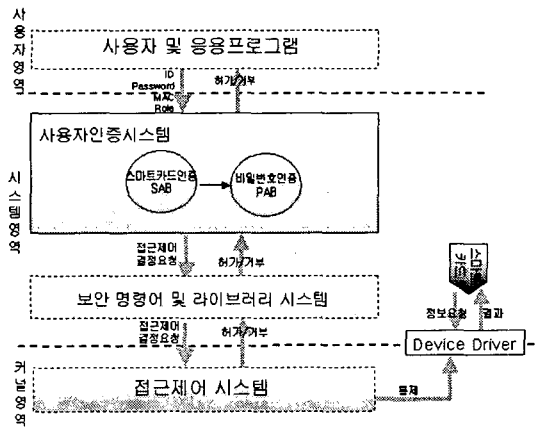
본 논문에서는 B2 등급 이상의 안전성을 보장하기 위해서 기존에 사용되어온 비밀번호와 다양한 활용이 가능한 스마트카드를 이용하여 사용자 인증하는 방법을 소개하고자 한다.

사용된 스마트카드에 저장된 데이터는 비밀번호를 사용하여 읽기, 쓰기에 대한 제한을 두어 임의의 사용자가 접근하여 카드 내의 정보를 읽을 수 없도록 한다. 또한, 스마트카드 리더기는 시리얼포트에 접속되는 외장형을 사용하며 외부에 전원을 켜고, 끄는 동작을 보여 줄 수 있는 전구가 부착 된 것으로 선택하였으며 시리얼 포트 디바이스 드라이버에 대한 접근을 접근제어 시스템에서 제한하도록 하였다.

3. 접근제어 시스템

본 논문에서 제안하는 사용자 인증 시스템은 유닉스 계열 시스템의 접근제어에 관련된 커널을 일부 수정하고 추가한 보안운영체제 시스템을 기반으로 한다.

구현된 보안운영체제 시스템은 시스템의 자원과 정보에 접근하기 위해서는 접근제어 시스템의 허가를 얻어야만 가능하다. 즉, 관련된 모든 시스템 호출을 접근제어 시스템을 통해서 허가된 경우에만 처리하도록 하였다. (그림 1)은 보안운영체제 시스템에서 사용자인증 처리 동작을 간략히 나타낸 것이다.



(그림 1) 보안운영체제시스템 구성도

보안운영체제 시스템에서는 16 개의 역할(role)을 정의할 수 있다. 이 역할은 보안관리자에 의해서 부여 받을 수 있다. 객체의 경우 역할과 읽기(r),쓰기(w),실행(x),상속(i)이라는 속성값의 조합을 할당 받는다. 상속이라는 속성값은 해당 객체를 실행하는 주체에게 동일한 역할을 상속해주는 것을 의미한다. 주체에도 역할이 할당된다[2].

역할이 할당된 주체는 해당 역할이 할당된 객체를 접근할 수 있는 권한을 얻게 되고, 역할이 할당되지 않은 주체는 이 객체에 접근할 수 없게 된다.

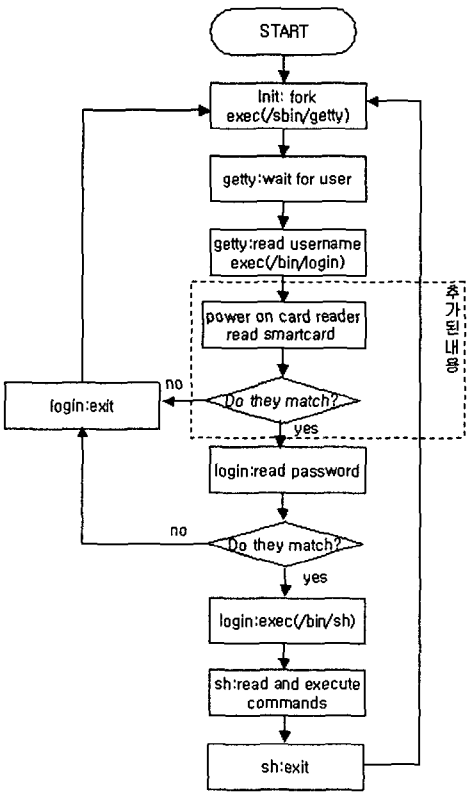
인증 시스템에서 사용되는 역할은 '인증역할' 인데 이 역할을 login 프로그램에 읽기-쓰기-실행-상속 이라는 속성값과 함께 할당하였다.

또한, 스마트카드 드라이버(Smart card Driver)에도 '인증역할'을 읽기-쓰기-실행 이라는 속성값과 함께 할당하였다.

사용자가 login 프로그램을 수행하면 그 프로세스는 '로그인역할'을 가지게 되고 이 프로세스에서 동작하는 login 프로그램은 스마트 카드 드라이버를 통해 카드 리더기에 입력된 카드값을 읽을 수 있게 된다. '인증역할'은 보안관리자에 의해서 할당되는 것이고 login 프로그램(또는 인증에 관련된 프로그램)에만 설정될 것이므로 다른 프로그램이나 사용자에 의해서 이 카드리더기가 동작되는 일은 불가능하다.

4. 신뢰경로가 보장되는 인증 시스템

본 논문에서 제안하는 사용자인증 시스템은 신뢰경로(*Trusted Path*)를 보장한다. 즉, 사용자가 중요정보(비밀번호)를 입력하기 전에 입력을 요청하는 메시지가 시스템에서 생성되었다는 것과 사용자가 입력하는 내용이 시스템에만 전달되고, 다른 사용자에게는 유출되지 않는다는 점을 보장하는 것이다[3][4].



(그림 2) init, getty, login, shell 의 처리 내용

먼저, 사용자에게 시스템에서 전달된 메시지인지 증명하기 위해서 스마트카드 리더기를 활용한다. 화면에 메시지를 출력하는 형태의 소프트웨어적인 방법은 어떠한 방법이라도 프로그래머들에 의해서 흉내낼 가능성이 있다. 때문에 본 논문에서는 스마트카드 리더기를 외장형태의 전원표시가 가능한 전구가 달린 제품을 선택하여 카드리더기의 전구를 켜서 시스템에서 전달된 메시지임을 확인시키는 방법을 사용하였다. 카드리더기를 조작할 수 있는 것은 진짜 login 프로그램만이 가능하므로 카드리더기의 전구에 불이 들어오고 비밀번호를 요청한다면 시스템에서 전달한 메시지라고 할 수 있다.

(그림 2)는 시스템에 접근한 사용자의 인증 처리를 순서도로 나타낸 것이다. *init* 은 *getty* 프로그램을 각각의 터미널 또는 콘솔에서 실행시킨다. getty 는 로그인하려는 사용자가 있는지 살피며 기다리게 되고, 사용자가 있다면 getty 는 login 프로그램을 수행시킨다. login 프로그램에서는 비밀번호를 받아들이기 전에 카드리더기의 전구에 불을 켜서 시스템에서 입력된 메시지임을 확인할 수 있게 한다. 또한, 카드리더기에 입력된 카드 내에 정해진 위치에서 키를 읽어오게 된다. 카드에서 데이터를 읽어올 때는 미리 비밀번호를 확인하게 되고 그 비밀번호가 맞는 경우에만 읽을 수 있게 된다. 시스템에 저장된 스마트카드 키값과 읽어들인 키 값이 동일하면 비밀번호 입력을 요청하고 동일하지 않은 경우에는 오류메시지와 함께 login 프로그램을 끝내게 된다.

스마트카드 인증이 정상적으로 처리된 경우라면 비밀번호를 요청하는 메시지가 출력된다.

사용자가 입력하는 메시지가 시스템에만 전달된다는 것은 사용자가 입력하는 동안 다른 프로세스가 현재 프로세스에 대해 접근할 수 없다는 의미와 동일하다. login 프로그램에서는 비밀번호가 입력되는 동안 현재 tty 에 접근하는 프로세스가 tty 를 실행 중인 프로세스와 동일한지 확인하게 된다. 따라서 다른 프로세스들은 사용자가 입력하는 내용을 볼 수 없게 된다.

입력된 비밀번호를 시스템에 저장된 비밀번호와 비교하여 동일한 경우 사용자 인증이 정상적으로 완료하게 되어 쉘을 수행하게 되고, 동일하지 않다면 오류메시지와 함께 login 프로그램이 종료된다.

5. 결론

본 논문에서는 역할기반 접근제어 시스템이 구현된 보안운영체제시스템에서 사용자인증 시스템을 제안하였다.

본 논문에서 제안된 사용자인증 시스템은 신뢰경로가 보장된다.

사용자가 중요정보를 입력하기 전에 시스템에서만 전달할 수 있는 표시로 시스템으로부터 전달된 메시지임을 확인할 수 있게 하였고, 사용자가 중요정보를 입력하는 동안에는 다른 프로세스가 현재 입력하는 프로세스에 접근할 수 없도록 하는 방법을 사용하였다.

현재 데이터 보호에 가장 널리 사용될 것으로 예측되고 있는 스마트카드와 비밀번호를 활용하여 다단계 사용자인증을 수행하여 인증 절차를 강화 하였다.

강화된 사용자 인증은 보안운영체제 시스템에 접근하는 사용자를 보다 강력하게 제한하여 사전에 시스템의 자원과 정보를 오용하거나 남용하는 사용자를

차단하고자 함이다.

본 논문에서는 네트워크로 연결된 다른 시스템과의 접속을 배제한 로컬 시스템에서 처리되는 사용자인증 시스템에 대한 내용을 설명하였다. 현재 원격 시스템에서 접근하는 사용자들을 위한 확장된 개념의 사용자 인증 시스템[5][6][7]에 대한 연구가 진행중이다.

참고문헌

[1] http://www.radium.ncsc.mil/tpep/library/tcsec/index.html
[2] Rule Set Based Access Control, http://www.rsbac.de
[3] David A. Wheeler, "Secure Programming for LINUX and UNIX HOWTO", http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/book1.html
[4] Simon Wiseman, Phill Terry, Andrew Wood, "The Trusted Path between SMITE and the User", British Crown Copyright, 1988.
[5]Santosh Chokhani, "Trusted Products Evaluation", Communications of the ACM, Vol.35, No.7, Jury. 1992.
[6] Jeremy Epstein, John Mchugh, Rita Pascale, "A Prototype B3 Trusted X Window System", IEEE 1991.
[7] Raymon M. Wong, "A Comparison of Secure UNIX Operating System", IEEE, 1990.