제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

신뢰성이 보장되는 사용자 인증 프로토타입

두소영*, 김정녀*, 공은배**
*ETRI 보안운영체제연구팀
**충남대학교 컴퓨터공학과
e-mail : {sydoo,jnkim}@etri.re.kr, keb@ce.cnu.ac.kr

A Prototype of Trusted Authentication

So-Young Doo*, Jeong-Nyeo Kim*, Eun-Bae Kong**
*Secure Operating System Team, ETRI
**Dept. of Computer Engineering, Chung-Nam National University

요 약

본 논문에서는 로컬 또는 리모트에서 사용자가 서버 시스템에 접근하기 위해서 가장 먼저 거치게 되는 인증 절차 수행에 관련된 것으로 허가된 사용자의 접근만을 허용하고, 인증요청 메시지의 진위 여부를 확인시켜주는 기능과 사용자가 입력하는 중요 정보가 다른 사용자에게 유출되지 않도록 보장하는 기능을 추가한 신뢰성이 보장되는 인증방법을 소개한다. 본 논문에서는 역할기반의 접근제어 시스템을 커널 내부에 추가하고, 사용자인증에 비밀번호와 하드웨어 장치인 스마트카드를 사용함으로써 강화된 사용자 인증 시스템을 구현하였다.

1. 서론

사용자 인증은 시스템의 중요한 보안 요소 중의 하나이다. 그러나, 사용자 인증 프로그램만을 사용한 보안은 대문만을 단단히 잠그고 창문은 단속하지 않은 집과 같다고 설명할 수 있다. 집 안팎 곳곳으로 무언가 접근하는 것을 모두 감시할 수 있는 형태의 보안이 필요하다.

시스템에서도 이와 마찬가지로 인증하는 부분에만 보안을 위한 갖가지 장치를 수행하는 것 보다 전체 시스템의 접근제어를 총괄적으로 처리하는 보안 형태가 필요하다[1][2][3][4][5]. 본 논문에서는 커널 내부에 시스템에 접근하려는 모든 요구에 대해 판단할 수 있는 접근제어 모듈을 추가로 구성하여 만든 보안운영체제 시스템에서 사용자 인증에 대해서 설명한다.

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.

현재까지 시스템의 보안에 관련된 표준안 중 주로 참고되는 TCSEC[6] 에서 어느 정도의 안전성을 보장하는 B2 등급 이상을 만족하기 위한 사용자인증 시스템은 다음 3 가지 타입 중 2 가지 이상을 사용하여 인증 절차를 수행하여야 한다.

- what you know: 비밀번호, PIN 등
- what you have: 스마트카드, 열쇠, 배지 등
- what you are: 지문인식, 음성인식, 홍채인식 등

본 논문에서는 사용자인증을 강화하기 위한 방법으로 기존의 비밀번호 방식(what you know)과 스마트카드 방식(what you have)을 통합하여 구성하였다.

하드웨어를 사용하는 방법은 복잡성을 높인다는 점에서 인증의 강화 효과를 동일하게 가지고 있으나 보다 안전한 인증과 다양한 활용을 위해서 본 논문에서는 스마트카드를 사용하였다.

사용자 인증에서 또 한가지 고려되는 사항은 사용자와 시스템간의 신뢰경로를 제공하는 것이다. 신뢰

경로(Trusted Path)란 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.

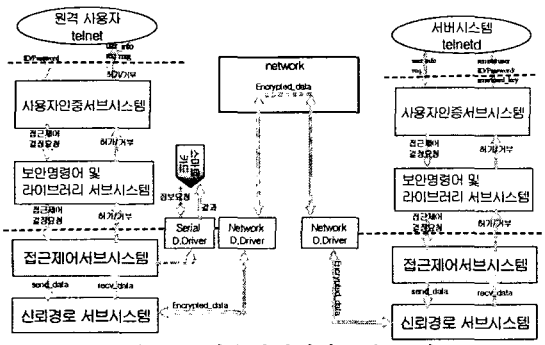
본 논문에서는 시스템의 동작에 영향을 주지 않으면서 사용자에게 시스템의 명령어임을 확인 할 수 있는 방법과 외부 또는 내부 사용자가 입력하는 중요 정보가 다른 사용자에게 유출되지 않도록 하는 방법을 제공하여 시스템의 자원과 정보를 보호하기 위해 구현된 사용자 인증 시스템에 대해서 설명한다.

2 장에서는 인증시스템을 포함하고 있는 전체 시스템에 대해서 설명하고 3 장에서 개발된 인증시스템에 대해서 설명하고 4 장에서 결론을 통해 정리한다.

2. 접근제어 시스템

본 논문에서 제안하는 사용자 인증 시스템은 유닉스 계열 시스템에 역할기반 접근제어[7]에 관련된 내용을 커널 내에 추가한 보안운영체제 시스템을 기반으로 한다[2].

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

보안운영체제시스템은 사용자인증에 관련된 처리를 수행하는 사용자인증서브시스템, 접근제어 서브시스템에 접근하기 위한 명령어와 라이브러리를 제공하는 보안명령어 및 라이브러리 서브시스템이 시스템영역에 구현되어 있고, 시스템에 접근하는 모든 요청을 받아서 허가/거부를 결정하는 접근제어 서브시스템과 시스템으로부터 전달되는 모든 메시지를 암호화해서 전달하고 복호화해서 시스템으로 전달하는 신뢰경로 서브시스템이 커널에 구현되어 있다.

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.

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 역할을 '인증역할' 이라고 하고, 이 역할을 인증 관련 프로그램 (예: login, telnet, ftp 등)프로그램에 읽기-쓰기-실행-상속 이라는 속성값과 함께 할당하였다. 또한, 스마트카드 디바이스(Serial Port, FreeBSD 의 경우 /dev/ttyd0)에도 '인증역할'을 읽기-쓰기-실행 이라는 속성값과 함께 할당하였다. 사용자가 인증 관련 프로그램을 수행하면 그 프로세스는 해당 프로그램에 할당되어 있는 '인증역할'의 '상속' 속성값에 의해 '인증역할'을 가지게 되고 이 역할을 가진 프로세스만이 스마트카드 드바이스를 통해 카드리더기에 입력된 카드 키 값을 읽을 수 있다.

'인증역할'은 보안관리자에 의해서만 할당되는 것이고 인증 관련 프로그램에만 설정될 것이므로 다른 프로그램이나 사용자에 의해서 이 카드리더기가 동작되는 일은 불가능하다.

3. 신뢰성이 보장되는 사용자 인증 시스템

본 논문에서 제안하는 사용자인증 시스템은 신뢰경로가 보장된다. 즉, 사용자가 중요정보(비밀번호)를 입력하기 전에 입력을 요청하는 메시지가 시스템에서 생성되었다는 것과 사용자가 입력하는 내용이 경우에만 읽을 수 있게 된다.

사용자의 중요 정보를 요청하는 메시지와 함께 스마트카드 리더기의 전구에 불이 켜지면 이것은 시스템에서 전달된 메시지임을 확인 할 수 있다. 이유는 스마트카드 디바이스가 '인증역할'로 설정되어 있기 때문에 시스템에서 인증한 프로그램만이 이 역할을 가지게 되고 그 프로그램만 카드리더기에 접근할 수 있기 때문이다. 사용자가 입력하는 중요정보는 시스템으로만 전달되고 해당 프로세스를 다른 프로세스가 접근할 수 없기 때문에 안전하게 전달 될 수 있다.

시스템에 저장된 스마트카드 키값과 읽어 들인 키값이 동일하면 비밀번호 입력을 요청하고 동일하지 않은 경우에는 오류메시지와 함께 인증관련 프로그램을 끝내게 된다.

스마트카드 인증이 정상적으로 처리된 경우라면 비밀번호를 요청하는 메시지가 출력된다.

사용자인증은 로컬 (콘솔)에서 수행되는 경우와 리모트에서 수행되는 경우로 나누어 생각할 수 있다. 이것은 스마트카드 처리 때문으로 리모트 시스템에서 처리되는 경우 리모트 시스템에 부착되어 있는 카드

리더기를 통해 카드 키를 읽어야 하기 때문이다. 현재 시스템에서는 카드리더기를 구동시키기 위한 리모트 시스템에서 서버시스템에 접근하는 클라이언트 프로그램 (예: telnet, ftp, rlogin 등)에 '인증역할'을 부여하였다. 현재 모든 시스템이 보안운영체제 시스템일 경우에만 적용된다. 그림 1 의 보안운영체제 시스템 처리 절차를 순서대로 설명하면 다음과 같다.

a. 리모트 시스템에서 서버시스템에 접근하고자 하는 리모트 사용자의 경우 사용자인증 서브시스템은 시스템에 접속하려는 사용자에게 연결하고자 하는 시스템의 주소를 입력 받는다. 이때 외부시스템의 운영체제가 보안운영체제인 경우 다음과 같은 절차로 수행된다.

b. 서버시스템에 연결 요청이 수락되면 서버시스템에서는 원격지 사용자에게 사용자 정보를 요청한다. 요청된 내용은 서버시스템의 사용자인증 서브시스템을 통해 보안명령어 및 라이브러리 서브시스템에서 접근제어 서브시스템을 거쳐 신뢰경로를 통해 암호화된 형태로 원격지 사용자 시스템으로 전달된다.

c. 원격지 사용자 시스템에서는 네트워크를 통해 전달된 내용이 신뢰경로 서브시스템으로 전달되어 암호화된 내용을 복호화 하고 접근제어 서브시스템의 허가를 받은 경우에만 사용자에게 전달된다.

d. 전달된 내용에 따라 사용자는 사용자의 패스워드, 스마트카드를 입력한다. 입력된 내용은 사용자 인증 서브시스템을 통해 보안 명령어 및 라이브러리 서브시스템을 거쳐 접근제어 서브시스템의 통제를 받으며 신뢰경로를 거쳐 암호화된 형태로 서버 시스템으로 전달된다.

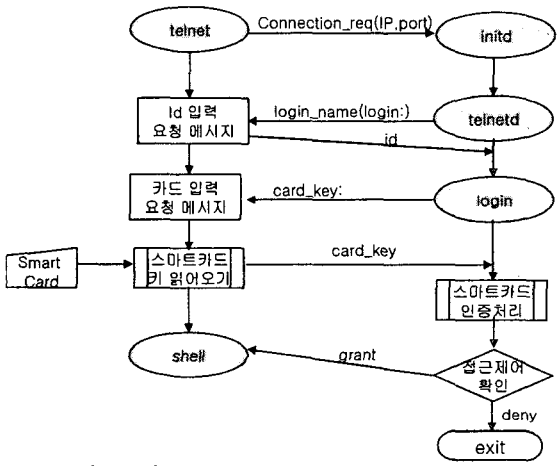
e. 서버시스템에서 전달된 데이터를 복호화 하여 사용자 인증 서브시스템으로 전달한다. 서버 시스템의 사용자 인증 서브시스템에서는 전달된 원격지 사용자 정보를 접근제어 서브시스템에 전달하여 접근 여부를 결정한다.

f. 서버시스템의 접근제어 서브시스템 결과는 서버시스템의 사용자 인증 서브시스템으로 전달된다. 전달된 결과가 허가 이면 원격지 시스템으로 허가임을 알리고 원격지 사용자가 사용할 수 있는 쉘을 수행한다. 전달된 결과가 거부이면 원격지 사용자에게 거부된 이유를 전달하고 연결을 종료한다.

g. 원격지 사용자 시스템은 서버시스템으로부터 전달된 데이터를 복호화 하여 사용자에게 접근 허가 또는 거부 결과를 알린다.

절차 a 에서 입력된 서버시스템 주소가 잘못되었거나 연결할 수 없는 상태이면 그 이유와 함께 접근 요청 프로그램이 종료된다

리모트 시스템 내부에서 외부 시스템으로 전달되는 내용은 암호화 되어 전달한다. 현재는 시스템에서 사용되는 전용 암호화 채널을 활용하고 있다. 추후 이것은 소켓에 접근제어 모듈을 추가하여 선택적인 암호화를 제공할 예정이다. 또한, IPSec 등의 표준화된 모듈과의 연동도 고려 중이다. 현재는 시스템에서 외부로 나가는 모든 내용에 대해서 암호화 되고 그 키는 미리 전달되는 형태를 가정한다.



(그림 2) 리모트 시스템의 사용자 인증 절차

그림 2 는 telnet 과 login 프로그램을 수정한 내용이다. 스마트카드 처리부가 추가되었다. telnet 의 경우에는 카드리더기에 접근하여 카드 키를 읽어오는 부분이 추가되었고, login 의 경우는 전달된 카드키를 접근제어 서브시스템에 전달하고 접근제어 서브시스템은 보안데이터베이스에 저장된 내용과 비교하여 동일한 경우 허가를 그렇지 않은 경우 거부를 login 프로그램에 전달한다. login 프로그램에서는 전달된 결과에 따라 허가인 경우 리모트시스템의 사용자에게 shell 을 생성시켜주고 거부인 경우 오류메시지를 전달하고 연결을 종료한다.

4. 결론

본 논문에서는 역할기반 접근제어 시스템이 구현된 보안운영체제시스템에서 사용자인증 시스템을 제안하였다. 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.
또한, 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.

역할기반 접근제어를 바탕으로 하는 보안운영체제 시스템은 Linux Redhat 6.2 커널 1.1.15 와 FreeBSD 4.3 을 기반으로 구현되어있다. 각 시스템에 대해 신뢰성이 보장되는 인증처리 서비스는 C 로 구현하였다.

참고문헌

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