신뢰 인증 시스템과 안전성 분석

두소영, 김정녀, 손승원

한국전자통신연구원 정보보호연구본부

Trusted Authentication System and Security Analysis

So-Young Doo, Jeong-Nyeo Kim, Sung-Won Sohn

Network Security Department, Information Security Division, ETRI

요 약

본 논문은 비밀번호 인증의 신뢰성 강화에 관한 연구로서 비밀번호 인증의 취약성과 공격방식을 살펴보고 이에 대한 신뢰성 강화 방안을 제시한다. 본 논문은 비밀번호 인증 처리에 있어서 사용자와 시스템간의 상호인증 방법을 제시하여 사용자가 알아차리지 못하는 사이에 중요 정보가 유출되는 것을 방지하며, 커널 수준에서 접근제어 기능을 제공하여 트로이 목마 유형의 공격으로부터 인증 처리 프로세스를 보호함으로서 기존의 비밀번호 인증 처리의 신뢰성을 향상하였다. 본 논문은 비밀번호 인증의 신뢰성을 강화하기 위해 비밀번호 자체의 보호를 강조하던 기존의 연구들과 달리 인증 처리 프로세스를 보호할 수 있는 메커니즘을 제안한다. 또한, 실험을 통한 검증을 이용하여 연구 결과의 정당성을 뒷받침하였다

I. 서론

비밀번호 기반의 인증은 몇 가지 취약점을 가지고 있음에도 불구하고 컴퓨터 사용자들을 식별하는 방법으로 널리 사용되고 있다. 비밀번호 인증 방법이 이렇게 범용화 되어 사용되는 이유는 인증 절차가 간단하고 처리비용이 적기 때문이다. 본 논문은 비밀번호 인증의 신뢰성 강화에 관한 연구로서 비밀번호 인증의 취약성과 공격방식을 살펴보고 이에 대한 신뢰성 강화 방안을 제시하려는 것이다.

지난 20년 동안 비밀번호 인증 방식의 보안성은 많은 연구에 의해서 분석, 평가되었다[1,2,3,4]. 이러한 연구에 의해 밝혀진 바에 의하면, 일반 사용자들이 생성한 비밀번호는 특히 유추공격에 약하며 가로채기 공격과 재연공격에 취약성을 드러내고 있다.

비밀번호 유추를 위한 온라인 공격의 위험은 로그인 실패 횟수를 제한하는 것으로 어느 정도 감소시킬 수 있으나, 강력한 사전을 사용하는 오프라인 공격은 놀라운 효과를 가지고 있다[1,2]. 시스템 관리자는 자신이 가지고 있는 사전을 이용한 역행(reactive) 비밀번호 검사기를 수행하거나[3], 사용자가 처음으로 시스템에 접근하거나 비밀번호를 변경할 때 선택한 비밀번호가 공격당하기 쉬운지 미리(proactive) 검사해 보는 방법[4]을 사용하고 있다. 비밀번호 검사기는 사용자의 비밀번호를 공격자가 예측할 수 없게 만들 수 있도록 도와줘서 유추 공격을 어느 정도는 방지할 수 있으나 그렇게 만들어지는 비밀번호는 사용자가 기억하기에 쉽지 않다는 단점이 있다. 비밀번호 유추 공격은 위와 같은 방법을 사용하는 경우에도 불구하고 아직까지 대량의 비밀번호를 관리해야 하는 시스템의 경우에는 쉽게 성공하고 있다.

가로채기 공격은 프로그램 오류를 이용하는 해킹 기법을 바탕으로 끊임없이 시도되고 있는데 해커들의 프로그래밍 기술이 발전하고 해킹을 수행하는 코드(exploit)가 인터넷에 공개되면서 최근 그 심각성이 더 커지고 있다[5,6]. 사용자의 아이디와

비밀번호에 대한 표준 프롬프트를 보여주고 입력된 내용을 획득한 후 파일에 저장하고 화면에 '시스템 오류; 종료' 메시지를 내보낸 후 종료하는 프로그램을 작성하는 것은 매우 쉽다. 이러한 트로이 목마형 공격을 수행하는 사람들은 순진한 희생자를 기다리며 터미널을 떠나지 않는다. 이런 종류의 공격을 방지하기 위해서 사용자는 시스템을 사용할 때 마다 다시 초기화하는 방안을 이용할 수 있다. 어떤 시스템에서는 시스템의 초기화를 위해서 모든 신호를 없애고 처리 중인 프로세스를 중단하는 핫키 (마이크로 소프트의 경우는 이러한 이유로 안전한 인증 처리 경로로 <CTRL><ALT> <DELETE> 키를 선택하고 있다)를 사용하기도 한다. 이 방법은 인증 처리가 필요할 때 마다 다른 프로세스의 작업을 중단 시켜야 하고 원격 접속의 경우에는 네트워크 모듈까지 중단해야 하므로 모든 경우에 적합하지는 않다. 또 다른 방법으로는 사용자가 로그인 할 때 가장 최근에 접속했던 시간, 예를 들면 ' 5월 20일 09:47에 마지막 로그인 했었습니다' 라는 사용자 로그오프 시간을 알려줘서 이 내용이 맞을 경우에만 비밀번호를 입력할 수 있게 하는 방법도 있다. 인증 처리에 관한 공격 방법 중 비밀번호를 유추하는 공격은 사소한 공격이라고 판단되고 있고 더 세련되고 심각한 공격은 가로채기 유형의 공격이다[5]. 그림1에 인증 처리 단계와 공격 유형을 분리하여 정리하였다.

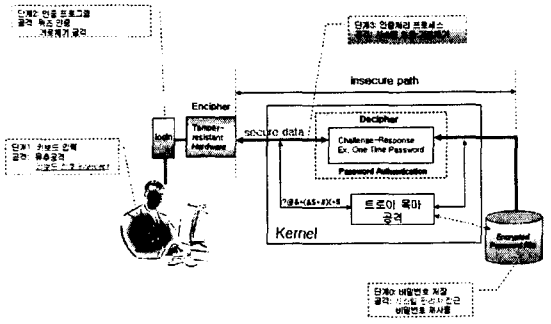

그림1: 공격 유형 분리

재연 공격은 공격자가 어떤 경로를 통해서 비밀번호를 얻은 경우 이 내용을 저장하거나 기억하고 있다가 이것을 이용하여 시스템에 접근하는 방법이다. 재연 공격은 비밀번호가 시간이 지나도 변하지 않기 때문에 가능한 공격이다. 한번 사용한 비밀번호는 다시 사용하지 않는 일회용 비밀번호 같은 방법을 사용하면 해결할 수 있다.

비밀번호 인증 방식에 취약점이 존재하는 근본적인 이유는 다음과 같다. 첫째는 비밀번호 인증 절차가 사용자에게 시스템의 정당성 여부를 확인 할 수 있는 방법을 제공하지 못한다는 것이다. 사용자는 자신의 아이디를 입력한 후 자신의 비밀번호를 입력하라는 메시지를 전달 받게 되는데 사용자는 이 메시지가 시스템에서 전달된 것인지, 불법적인 사용자가 전달한 것인지 확인 할 수 없다.

두 번째는 UNIX 계열의 시스템에서는 슈퍼유저 권한으로 모든 자원에 접근이 가능하다는 문제점이 있는데 해킹 프로그램을 이용하여 슈퍼유저 권한을 획득한다면 인증 처리가 수행되는 프로세스를 공격하거나 사용자가 입력하는 모든 정보를 가로채기 할 수 있는 위험이 존재한다.

본 논문은 비밀번호 인증 처리에 있어서 사용자와 시스템간의 상호인증 방법을 제시하여 사용자가 알아차리지 못하는 사이에 중요 정보가 유출되는 것을 방지하며, 커널 수준에서 접근제어 기능을 제공하여 트로이 목마 유형의 공격으로부터 인증 처리 프로세스를 보호함으로써 기존의 비밀번호 인증 처리의 신뢰성 향상과 이에 대한 검증방법을 보여주고자 하는 것이다.

II. 신뢰 인증 제공 방법

본 논문에서 제안하는 사용자 인증 시스템은 유닉스 계열 시스템의 접근제어에 관련된 커널을 일부 수정하고 추가한 보안커널을 기반으로 한다. 구현된 보안커널은 시스템의 자원과 정보에 접근하기 위해서는 접근제어 시스템의 허가를 얻어야만 가능하다. 즉, 관련된 모든 시스템 호출을 접근제어 시스템을 통해서 허가된 경우에만 처리하도록 하였다. 그림2는 보안커널에서 사용자 인증 처리 동작을 간략히 나타낸 것이다.

보안커널은 역할기반 접근제어[7]를 포함하고 있는데 현재 시스템에 16개의 역할(role)을 정의할 수 있다. 이 역할은 보안관리자에 의해서 부여받게 된다. 객체의 경우 역할과 읽기(r),쓰기(w),실행(x),상속(i)이라는 속성값의 조합을 할당받는다. 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 login프로그램에 상속-읽기-쓰기-실행(irwx) 이라는 속성값과 함께 할당하였다.
또한, 스마트카드 디바이스에도 '인증역할'을 읽기-쓰기(-rw-) 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 login프로그램(또는 인증에 관련된 프로그램)에만 설정될 것이므로 다른 프로그램이나 사용자에 의해서 이 카드리더기가 동작되는 일은 불가능하다.

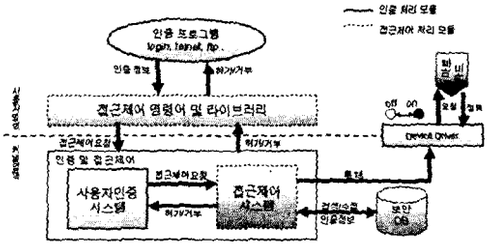

그림2: 보안커널 구성도

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].

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 login프로그램만이 가능하므로 카드리더기의 전구에 불이 들어오고 비밀번호를 요청한다면 시스템에서 전달한 메시지라고 할 수 있다.
시스템에서 사용자 인증 처리를 수행하는 절차는 다음과 같다. init은 getty프로그램을 각각의 터미널 또는 콘솔에서 실행시킨다. getty는 로그인 하려는 사용자가 있는지 살피며 기다리게 되고, 사용자가 있다면 getty는 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 함께login프로그램을 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. login프로그램에서는 비밀번호가 입력되는 동안 인증처리 프로세스에 접근하는 프로세스가 동일한 역할을 가지고 있는지 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 오류 메시지와 함께 login 프로그램이 종료된다.

III. 안전성 분석

본 논문에서 제안한 인증 방법은 보안 커널을 기반으로 하고 있기 때문에 사용자와 시스템간의 상호인증을 제공할 수 있는 메커니즘을 제공하고, 사용자가 중요정보를 전달하는 인증처리 스로세스를 다른 프로세스들과 분리할 수 있는 신뢰경로를 제공한다. 기존에 연구된 비밀번호 인증 방식의 신뢰성을 강화하기 위한 방법들은 주로 비밀번호 자체의 보호를 통하여 유추공격은 방지할 수 있으나요즈음의 공격추세인 시스템 호출 수준의 가로채기 공격(트로이 목마 유형의 공격)에는 방지책을 가지고 있지 않다. 표1에서 지금까지 연구되어 온 방법들과 제안된 연구방법의 안전성을 비교분석하였다.

본 논문에서제안한 방법에서는 사용자에게 시스템을 인증 시키기 위한 수단으로 스마트카드를 사요

하고 있다. 반드시 스마트카드 리더기를 사용할 필요는 없으며 다른 장치로 쉽게 변경이 가능하다. 또한, 스마트카드를 이용하여 제안된 방법에 암호화 기법을 추가할 수 있는데 이렇게 하면 유추공격에 대한 방어도 가능하게 된다. 암호화 기법의 추가는 본 논문에서 다루고 있지 않으나 기존의 방법을 쉽게 적용 가능하다.

표1: 인증 기법의 특성 비교

X: 불가능, O: 가능

인증 기법 / 성능	비밀번호 인증	질의-응답 인증	암호화 인증	스마트카드 인증	생체정보 인증	제안한 신뢰인증
유추 공격 방지 여부	X	O	O	O	O	X
위조 인증 공격 방지 여부 (상호인증 기능)	X	X	O	O	X	O
System call 가로채기 공격 방지 여부	X	X	X	X	X	O
비밀번호 파일 접근 공격 방지 여부	X	O	O	O	X	O
경제성 (처리부하)	상 (적음)	중 (많음)	하 (많음)	중 (많음)	하 (많음)	중 (많음)
효율성 (처리속도)	상 (빠름)	중 (느림)	하 (느림)	중 (느림)	중 (느림)	상 (빠름)

개발된 인증 시스템을 실제 사용되고 있는 위조인증 프로그램과 시스템호출 hooking공격 프로그램을 사용하여 실험한 결과 가로채기 공격을 방어할 수 있고 사용자의 중요 정보를 안전하게 보호할 수 있음을 확인하였다.

IV. 결론

개발된 시스템은 기존 시스템이 시스템 관리자 권한을 집중하여 발생했던 문제를 해결하기 위해서 시스템 관리자의 권한을 분리하여 보안에 관련된 처리는 보안 관리자라는 역할을 가진 사용자만이 수행할 수 있도록 하였다. 사용자는 인증 절차를 통해서만 역할을 부여받을 수 있고 등록 시 허가받은 범주 내에서만 시스템에 접근이 가능하다. 시스템의 보안 홀을 이용하여 공격하는 경우 인증을 거치지 않고 슈퍼유저의 권한을 획득할 수 있는데 이 경우 획득한 프로세스에는 아무 역할도 할당되어 있지 않아 역할이 설정되어 있는 중요 정보나 자원의 접근을 할 수 없도록 하는 방법도 제공된다.

제안된 신뢰성이 강화된 인증 방법에서는 커널의 수정이 필수적이다. 커널 수준의 RBAC 접근제어를 기반으로 하기 때문인데 접근제어를 통한 시스템 보호는 그 효과 측면에서 매우 유용한 것이기는 하나 그 운용에 있어서 전체적인 보안 관리 개념이 있어야 시스템의 보안이 유지 될 수 있다. 인증 시스템의 신뢰성을 위해서 커널의 변경과 인증 인터페이스를 변경하는 것은 다소 그 부하가 크다고 볼 수 있으나 커널의 내부 동작에는 영향을 주지 않도록 설계하였다.

근래에 인증서를 사용하는PKI기반의 인증방법이 범용화 되고 있는 추세이다. 본 연구에서는 인증서를 활용하는 인증 방법에 대한 내용은 다루지 못하였다. 또한, 사용자와 시스템간의 상호인증 만을 다루었고, 시스템과 프로그램 그리고 시스템과 시스템간의 인증에 대한 내용도 접근하지 못하고 있다. 이러한 연구들은 모두 향후 연구 과제로 남기고 심도 있는 연구를 계속 진행할 계획이다.

참고문헌

[1] R.Morris and K.Thompson. "Password security: a case history." *Communications of the ACM*, Vol.22, No.11, 1979.

[2] D.Klein. "Foiling the cracker: a survey of, and improvements to, password security." *Proceedings of USENIX Security Workshop*, 1990.

[3] T.Wu. "A real-world analysis of Kerberos password security." *Proceedings of Symposium on the Network and Distributed System Security*, 1999.

[4] M.Bishop. "Password management." *Proceedings of the International Computer Conference*, 1991.

[5] R.E.Smith. *Authentication from passwords to public keys.* Addison-Wesley. 2002.

[6] C.P.Pfleeger and S.L.Pfleeger. *Security in Computing*. Prentice hall. 2002.

[7] D.FFerraiolo, R.Sandu and S.Gavrilla. "A Proposed standard for RBAC." *on the internet* http://wcsrc.nist.gov/rbac

[8] N.Itoi and P.Honeyman. "Practical Security Systems with Smartcards." *Proceedings of the IEEE workshop on Hop Topics in Operating Systems*. 1999.