PKI 기반 보안운영체제의 권한 인증 설계

이윤희*, 정창성*

*티에스온넷㈜

e-mail:yhlee@tsonnet.co.kr

Design of Privilege Authentication for Secure OS based on PKI

Yun-Hee Lee*, Chang-Sung Jung*

*Research Center, TSonNet Co.,Ltd.

요 약

보안운영체제에서는 등급기반 사용자, 프로세스, 파일에 대한 영역분리 및 등급별 보안관리를 하는 다중등급보안(Multi Level Security)을 구현하고 있다. 안전한 운영체제에서는 사용자가 등급 즉, 자신의 보안등급과 보호범주를 설정하기 위해 권한 인증절차를 수행한다. 권한은 보안운영체제에서 강제적 접근 제어(Mandatory Access Control)의 기본이 되므로 그 보안에 중요성이 크다. 따라서, 권한 인증 절차의 보안이 부각되고 있다. 본 논문에서는 PKI 기반 전자서명 인증절차를 이용하여 신원 확인과 권한 인증을 한번에 수행할 수 있는 방법을 제시한다.

1. 서 론

인터넷의 확산과 더불어 정보보호에 관한 일반 대중의 관심이 높아졌고, 인터넷을 이용하여 기업활동을 하거나 상거래를 하고자 하는 수요가 늘어나면서 시스템 보안은 필수적으로 요구되고 있다. 기업들은 시스템 외부에 여러 가지 네트워크 보안장비를 설치하여 시스템을 보호하고 내부에는 서버보안 제품들을 설치하여 보안을 유지하고 있다. 서버보안 제품 중 보안운영체제는 등급기반 접근통제 시스템으로 패스워드 기반 인증을 받은 사용자가 시스템 자원(파일, 디렉터리, 디바이스)등을 사용할 경우 일반적으로 사용하는 permission에 의한 접근 제어가 아니라 등급권한에 의해 접근 제어가 이루어진다. 따라서, 해당 권한을 얻기 위하여 권한 인증 절차를 한번 더 수해하여야 한다. 결국 보안운영체제에서 패스워드 기반 인증을 사용할 경우 다음과 같은 문제점을 갖게 된다.

첫째, 패스워드 관리는 보안의 가장 기본적인 사항으로 유추하기 어려운 패스워드를 사용하고, 주기적으로 패스워드를 변경하는 등 패스워드 관리에 신경을 많이 써야 한다.

둘째, 패스워드 길이에는 한계가 있다. 패스워드 관리를 철저히 하더라도 사전공격과 같은 고성능 크랙 도구를 사용하거나 고성능 컴퓨터를 사용할 경우 패스워드를 알아내는 것은 많은 시간이 걸리지 않는다.

셋째, IP 스니핑(sniffing)이나 스푸핑(spoofing)과 같은 방법으로 패스워드 도청 및 도용이 쉽다는 것이다.

넷째, 권한 인증을 받기 위해 한번 더 인증을 받아야 한다. 이는 취약한 패스워드 기반 인증에 한번 더 노출됨을 의미한다.

이러한 문제점들을 해결하기 위해서는 본 논문에서는 보안운영체제에서 사용자의 신원 확인 인증과 권한 인증을 공개키 기반구조(PKI:Public Key Infrastructure)의 인증서 및 개인키 구조를 사용하여 한번에 수행할 수 있는 방법을 제시한다.

공개키 기반구조(PKI)를 사용하여 사용자에게 권한 인증 정보를 제공하기 위해 가장 쉬운 방법은 X.509 인증서 확장 필드를 이용하는 것이다. 이미 나와있는 보안운영체제에서 권한인증 방식도 이 방식을 사용하고 있다. 이러한 방식은 기존의 공개키 기반 구조 시스템의 큰 변경 없이 그대로 이용할 수 있고, 권한, 인증의 절차가 간단하다는 장점이 있다. 그러나, 모든 사람에게 공개되는 인증서의 속성상 사용자의 권한은 모든 사람에게 공개될 수 있다. 이는 사용자의 권한이 자신만이 알아야 하는 기밀성에 위배된다.

이를 해결하기 위해서 공개키 기반구조를 사용하되 사용자의 권한에 대한 기밀성을 유지하기 위해 권한 속성을 인증서가 아닌 개인키 구조에 저장하는 방법을 제안한다. 공개키 기반구조를 사용하므로 권한 인증을 위한 기반 구조 환경이 필요하지 않으며 비밀키에 사용자의 권한을 저장하므로 권한 속성의 기밀성도 확보할 수 있다.

2. 보안운영체제

운영체제 수준의 등급기반 접근통제시스템인 보안운영체제에서는 보안등급(Clearance)과 보호범주(Category)를 사용하여 사용자, 프로세스, 파일에 대한 영역분리 및 접근제어를 위해 다중등급보안(Multi Level Security)을 수행한다.

다중등급 보안이란 주체(사용자, 프로세스 등)에 보안등급과 보호범주를 부여하고 보안등급과 보호범주가 부여된 객체(파일 및 디렉터리, 디바이스)에 접근하는 것을 통제하는 방식으로서 보안 권한 분리가

요구되는 시스템에서 널리 사용되는 보안 기능이다.

다중등급 보안 정책은 주체의 등급을 설정하고 객체의 등급과 비교하여 접근을 허용하거나 거부한다. 이 과정에서 접근에 대한 모델은 수정된 BLP(Bell & LaPadula) 모델을 사용한다[1,2,3]. 여기에서 등급은 보안운영체제에서 보안등급과 보호범주로 분리된다. 따라서, 보안운영체제에는 시스템에 접근하기 위하여 신원 확인을 위한 인증을 수행한 후에 다시 한번 권한을 부여 받기 위해 권한 인증 과정을 거쳐야 하는 것이다.

3. 공개키 기반 구조

일반적으로 전자서명이란 기존에 사용하던 인감이나 서명을 전자거래에서도 사용할 수 있도록 전자적으로 구현한 것이다. 전자서명을 신뢰할 수 있는 제3자로 하여금 인증하게 함으로써 거래상대방 또는 발신자의 신원을 확인할 수 있게 하는 방법이다. 때문에 송수신 상호간에 전자서명 교환을 보증해 주는 제3자로서의 인증기관이 필요하며, 전자서명의 생성 및 검증이 핵심을 이룬다. 전자서명은 메시지인증기능과 사용자 인증기능을 통하여 데이터 교환의 안전성·신뢰성을 보장해 준다. 메시지인증기능은 전자문서의 위·변조 방지를 위하여 비록 정보가 암호화되어 있다 하더라도 이 내용이 처음에 만들어진 내용과 변경이 없었다는 것을 증명하는 기능이며, 사용자인증기능은 송·수신자의 신원을 식별·확인하는 기능이다. 즉, 서명자만이 서명 문을 생성할 수 있기 때문에 위조가 불가능하며, 서명의 재사용 및 서명 사실 부인이 불가능하다.

전자서명에서는 개인키(Private key)와 공개키(Public key) 두 개의 키를 사용하는데, 여기서 비밀키는 사용자 본인이 데이터를 송신하기 위하여 서명을 생성할 때 사용하며 사용자 본인만 알 수 있는 키를 의미하며, 공개키는 수신자에게 제공되어 데이터의 내용과 서명의 진위를 검증할 때 사용된다. 이처럼 전자서명에 필요한 비밀키와 공개키의 안전한 관리·운영에 좌우되는데, 현재 전자서명제도를 구현하기 위한 기술적 요소로서 공개키 기반구조(PKI: Public Key Infrastructure)가 있다. 공개키 기반구조는 공개된 네트워크인 인터넷상에서 안전한 키관리 시스템으로서 안전한 개인키, 인증서를 제공해 주는 기술기반을 의미한다. 공개키 기반구조는 다음과 같은 구성요소가 필요하다.

- 정책승인기관(PAA:Policy Approving Authority) : 최상위 인증기관으로 정책수립 및 PCA 공개키에 대한 인증서 관리
- 정책인증기관(PCA:Policy Certification Authority) : PAA 하위의 정책인증기관으로 CA가 따라야 할 정책 수립 및 CA 공개키에 대한 인증서 관리
- 인증기관(CA:Certification Authority) : 공개키 기반구조에서 관리되는 인증서, 인증서취소목록, 사용자 정보 등을 저장
- 등록기관(RA:Registration Authority) : CA와 사용자들 사이에서 인증요청을 승인하고 신청자 신분 확인
- 디렉터리 : 공개키 기반구조 관련 정보 저장 및 검색. DAP 또는 LDAP을 이용하여 X.500 디렉터리 서비스 제공

인증서를 이용한 전자서명 절차는 다음과 같다.

① 규정된 절차에 따라 사용자는 인증기관(CA)에 인증서를 신청한다.
② 인증기관은 신청자의 신원을 확인하고 사용자의 인증서를 디렉터리 서버에 등록하고 개인키와 함께 사용자에게 발급한다.
③ 송신자는 메시지를 해쉬함수를 이용하여 해쉬값을 구하여 자신의 개인키로 서명한다.
④ 서명과 메시지원본을 수신자의 공개키로 암호화하여 전송한다. 이는 중간에 다른 사람이 메시지를 볼 수 없도록 하기 위함이다.
⑤ 수신자는 송신자로부터 메시지를 수신한 뒤 인증기관에게 수신자의 인증서를 요청한다.
⑥ 인증기관은 인증서와 인증서 취소 리스트를 송신자에게 전송한다.
⑦ 수신자는 먼저 자신의 개인키로 암호문을 복호화 한다.
⑧ 복호화한 결과 중 수신자가 서명한 메시지를 인증기관에게서 전달받은 송신자의 인증서에서 구한 공개키로 복호화 한다. 이때, 송신자의 공개키로 복호화되는 것은 송신자의 개인키만이 가능하므로 송신자의 신원이 확인된다.
⑨ 복호화한 결과 중 원본 메시지는 해쉬값을 구해 송신자의 공개키로 복호화한 값과 비교하여 동일하면 메시지가 통신 중 위·변조가 발생하지 않았음을 의미한다. [4,5]

4. 권한인증 제안 구조

본 논문에서 제안하는 방법은 일반적인 공개키 기반구조에서 제공하는 개인키 구조에 그림 1과 같이 보안운영체제에서 접근제어의 기준으로 사용하는 사용자 권한인 보안등급과 보호범주를 추가한다. 인증서가 아닌 개인키에 권한을 저장함으로써 모든 사용자에게 공개하지 않고 사용자의 권한을 저장할 수 있다. 그러나, 서버는 사용자가 보내온 보안등급과 보호범주가 실제로 그 사용자에게 설정된 권한인지 아니면 악의적인 목적으로 사용자가 수정한 것인지, 또는 중간에 다른 사용자에 의해 변조되었는지 등을 확인할 필요성이 있다. 이를 위해 인증서 extensions 필드에 개인키에 저장하는 보안등급과 보호범주의 해쉬값을 저장한다. 서버는 사용자의

보안등급과 보호범주의 해쉬값을 인증서에 있는 해쉬값과 비교하여 보안등급과 보호범주의 무결성을 확인하도록 한다.

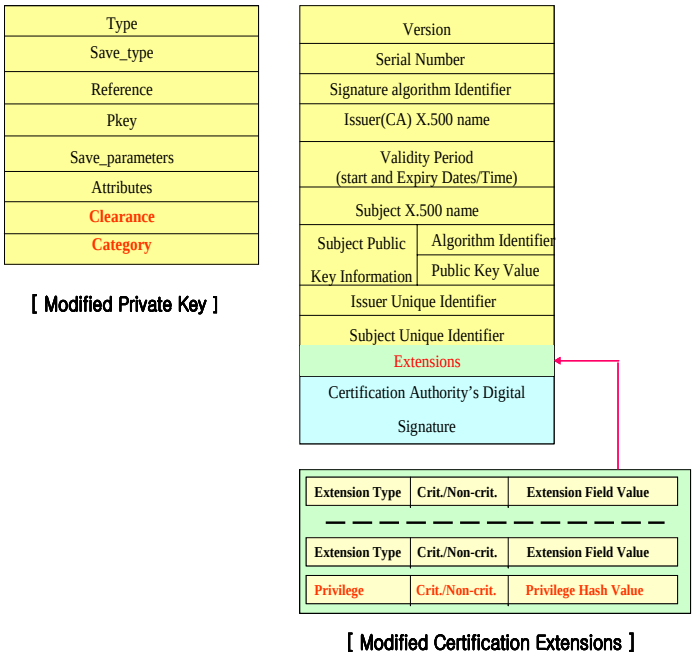

그림 1

그림2는 인증기관이 개인키와 공개키 발급 시 개인키에는 사용자의 보안등급과 보호범주를 저장하고 인증서에는 그에 대한 해쉬값을 저장하는 절차이다.

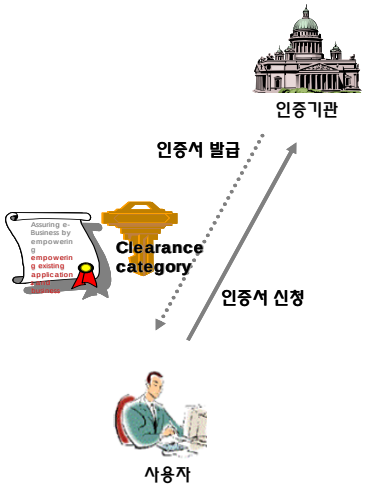

그림 2

인증기관은 사용자가 인증서를 요청하면 개인키와 공개키 쌍을 생성한다. 이때 개인키에는 요청한 사용자의 보안등급과 보호범주를 추가로 저장한다. 그리고, 인증서에 보안등급, 보호범주의 해쉬값을 저장하고 인증기관이 서명하여 인증서를 발행한다. 실제 통신할 경우 개인키에 보관된 보안등급과 보호범주는 사용자 인증시 전달되는 메시지가 된다. 기존 공개키 기반구조에서는 신원 확인을 위해서 **오류! 참조 원본을 찾을 수 없습니다.** 2와 같이 메시지를 주고받는다.

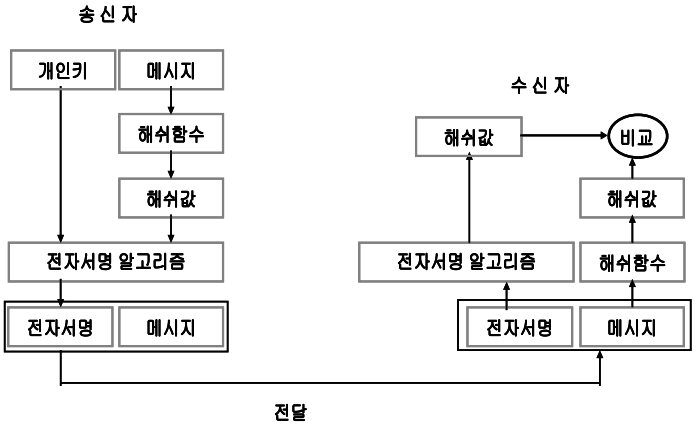

그림 3

본 논문에서 제안하는 방법은 그림 4와 같이 보안등급과 보호범주를 주고받아 인증과 동시에 사용자의 보안등급과 보호범주가 설정되도록 한다.

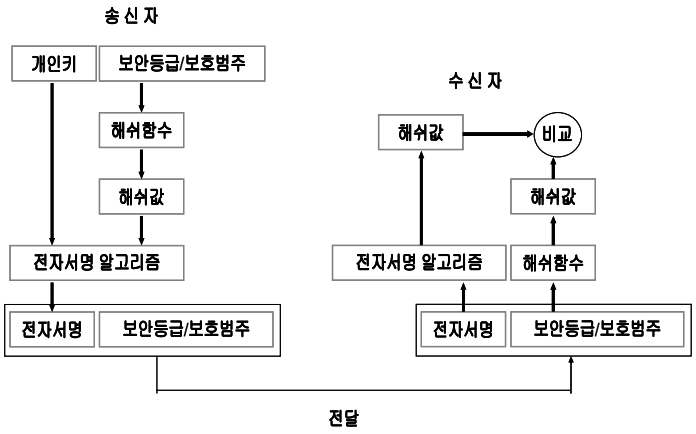

그림 4

개인키에 보안등급과 보호범주를 저장하게 되면 개인키를 소유한 사용자가 자신의 보안등급과 보호범주를 변경할 가능성이 존재한다. 이를 해결하기 위해 그림5와 같이 서버는 사용자의 인증서에서 보안등급과 보호범주의 해쉬값을 얻어 보내온 보안등급, 보호범주의 해쉬값과 일치하는지 확인한다.

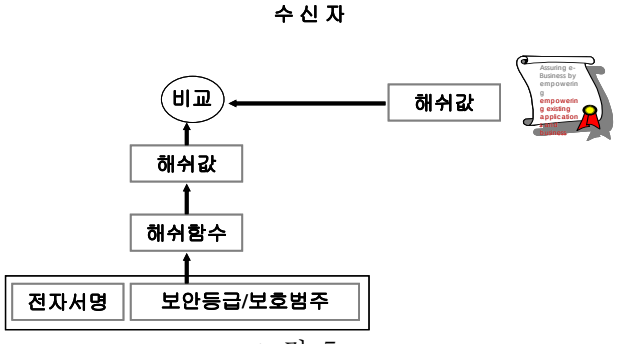

그림 5

5. 권한 인증 과정

본 논문에서는 시스템에 보안운영체제가 설치되었다는 전제로 공개키 기반구조의 전자서명인증 및 권한 설정 절차를 제시한다. 보안운영체제에서 공개키 기반 전자서명 인증을 이용하여 권한 인증을 하기 위해서는 공개키 기반구조에서 제공하는 신뢰할 수 있는 수정된 공개키와 개인키가 필요하다. 사용자는 서버에 인증하는 과정에서 보내는 메시지는 사용자의 보안등급과 보호범주로 대체하여 한번의 인증 과정으로 권한 인증까지 진행한다. 변경된 인증서 및 개인키 발급 및 신원 확인 인증과 권한 인증 절차는 다음과 같다.

① 사용자는 먼저 인증기관에 인증서를 요청한다.
② 인증기관은 신청자의 신원을 확인하고 사용자의 인증서와 개인키를 발행한다. 이때 사용자의 보안등급과 보호범주를 개인키의 정보에 저장하고 보안등급과 보호범주의 해쉬값은 인증서에 저장한 뒤 사용자에게 발급한다.
③ 사용자는 서버에 인증을 요청하기 위해 자신의 개인키에서 보안등급과 보호범주를 얻어 해쉬값을 구하여 자신의 개인키로 서명한다.
④ 자신의 보안등급과 보호범주와 함께 단계 3에서 구한 해쉬값을 서버의 공개키로 암호화하여 전달한다.
⑤ 서버는 사용자의 인증 요청을 받으면 인증기관에게 사용자의 인증서를 요청한다.
⑥ 인증서 요청을 받은 인증기관은 사용자의 인증서와 인증서 취소 리스트를 서버에게 전송한다.
⑦ 서버는 자신의 개인키로 사용자의 암호문을 복호화 한다.
⑧ 서버는 사용자가 보내온 보안등급과 보호범주가 실제 사용자에게 부여된 권한인지 확인하기 위해 사용자의 인증서에서 Privilege extension의 값과 비교한다. 즉, 복호화한 암호문에서 보안등급과 보호범주의 해쉬값을 구하여 인증서에 첨부된 해쉬값과 비교한다. 만약 두 개의 값이 동일하다면 사용자가 보내온 보안등급과 보호범주가 인증기관에게 부여 받은 보안등급과 보호범주임을 확인할 수 있다.
⑨ 사용자가 보내온 보안등급과 보호범주가 동일하다면 사용자의 인증을 위해 복호화한 결과 중 사용자가 서명한 보안등급과 보호범주를 인증기관으로부터 받은 인증서의 공개키로 복호화 한다. 복호화한 결과값과 보안등급, 보호범주의 해쉬값을 구하여 동일하다면 공개키로 복호화되는 것은 쌍을 이룬 개인키 뿐이므로 사용자의 신원을 확인할 수 있다.
⑩ 단계 9에서 비교 값이 동일하다면 보내온 보안등급과 보호범주를 사용자에게 설정한다.

시스템의 신원 확인 인증과 권한 인증을 받은 사용자는 이후 보안등급과 보호범주를 설정하기 위해 별도의 인증과정 없이 설정된 보안등급과 보호범주를 가지고 보안운영체제에서 제어하는 사용자, 프로세스와 파일, 디렉터리간 등급기반 접근제어가 이루어진다. 본 논문에서 제안하는 공개키 기반 인증 및 권한 인증 절차는 사용자에게 편리하고 간편하면서 안전한 신원 인증 및 권한 인증 방법을 제공한다.

6. 결 론

본 논문에서는 사용자 권한설정 절차를 좀더 편리하고 안전하게 할 수 있는 방법을 제시하였다. 공개키 기반구조의 전자서명인증 방법을 이용하여 개인키에 사용자의 권한 즉, 보안등급과 보호범주를 저장하여 사용자의 권한을 설정하는 방법은 보안운영체제에서 단 한번의 인증으로 사용자의 신원 확인과 권한 인증을 할 수 있다. 또한 현재 많이 활성화 되어 있는 공개키 기반구조 환경을 그대로 이용할 수 있어 권한 인증을 위한 또 다른 제반 환경을 구축할 필요가 없다. 단, 보안운영체제에서 제공하는 보안등급과 보호범주에 대한 의미가 인증기관에서도 사용이 되어야 하며 사용자의 보안등급과 보호범주를 인증기관에서 설정할 때 그에 대한 표준이 필요하므로 이에 대한 연구가 좀 더 이루어져야 할 것이다.

참고문헌

[1] Bell. D. and Lapadula, "Secure Computer System : Mathematical Foundations and Model," MITRE Report MTR 2547, 1973.
[2] DoD, "Trusted Computer System Evaluation Criteria", DoD 5200.28.STD, 1985.
[3] 홍승표, "리눅스 커널 기반의 강제적 접근제어 설계 및 구현", 한서대학교, 1- 6page, 2001.
[4] 정지선, "PKI를 활용한 보안 운영체제 구조 설계", 호남대학교, 20-26page, 2001
[5] 저문석외 6명, "PKI", 도서출판 미래컴, 46-56page, 2003