전자서명기반의 해킹방지 보안 커널시스템 설계

도경화° 이상훈 이영택 정우식 전문석
숭실대학교 컴퓨터학과 통신연구실
khdo0905@dreamwiz.com°, iam@leesanghun.pe.kr,
lsy3513@hotmail.com, wsjung@haksan.dsc.ac.kr, mjun@comp.ssu.ac.kr

Design of Security Kernel System based on the Digital Signature to Prevent Hacking

Kyounghwa Do° WooSe Jung Sanghun Lee Youngtaek Lee Moonseog Jun
Network Security Lab of Soongsil University

요 약

최근 전자서명방식의 사용이 급증하고 있으나, 인터넷의 해킹과 데이터의 피해는 날로 심각해져가고 있다. 특히, 정보의 특성에 따라 데이터의 접근을 허용하지 않아야 하는 경우는 보안에 대한 중요성이 더욱 강조된다. 따라서, 본 논문은 시스템의 안전성을 위하여 암호화와 공개키기반구조를 이용하고 있으며, 중요 데이터의 안전성을 높이기 위하여 데이터베이스 접근시에도 전자서명 및 암호화를 통한 보안 커널시스템을 제안하고 설계한다. 본 논문은 교육망이라는 특정 목적을 가진 네트웍망을 실험환경으로 하여 전자서명방식을 통한 인증 뿐만아니라, 데이터의 공개 및 위·변조를 막기 위한 방법인 보안 커널시스템을 제공하기 위한 방법을 제안하고 설계한다.

1. 서 론

최근 인터넷의 발전과 디지털을 이용한 정보화로인해 좀 더 편안한 데이터의 전송과 보관이 가능해졌으나, 해킹와 바이러스를 통한 데이터의 공개 및 위·변조가 심각해지고 있다. 특히, 대부분의 중요 데이터는 디지털화되어 각종 서버 및 데이터베이스에 저장되고 있다. 이는 편리성을 제외하면 보안상으로는 매우 위험하다고 볼수 있다. 따라서, 서버 및 데이터베이스의 보안을 위하여 공개키기반구조를 활용한 사용자 접근에 관련한 인증과 데이터의 접근 및 수정을 위한 암호화를 통한 보안이 필요하다.

즉, 서버의 파일(데이터베이스)의 정보를 보호하기 위해서는 무결성(Integrity), 기밀성(Secrecy), 인증(Authentication) 그리고 가용성(Available)을 제공해야 한다. 이는 외부로부터 저장서버로 전송되는 데이터의 위·변조를 막아야 하는 무결성을 제공해야 하며, 다른 제3의 사용자가 데이터의 내용을 알 수 없어야 하는 비밀성과 서버의 파일의 사용자 접근권한에 대한 사용자 인증 그리고, 마지막으로 본 데이터가 실제 역할을 할 수 있는지에 대한 가용성을 모두 제공해야 한다.

본 논문에서는 전자서명을 기반으로 하는 해킹방지 보안 SQL 커널 시스템을 제안한다. 본 논문에서 제안하는 시스템은 전자서명 기반을 사용하여 데이터베이스의 정보를 안전하게 관리하는 방식으로, 전자서명을 통하여 정보요청자의 신분을 확인하고, 전자서명 검증을 통한 신분확인 후 부여된 사용자 프로세스의 접근 권한을 이용하여 특정 파일에 대한 접근제어 수단을 제공한다. 또한, 전송되는 모든 데이터는 암호화를 수행하여 기밀성을 제공하게 된다. 또한, 본 논문에서는 교육정보망이라는 특정환경에 적용하여 시스템을 설계한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 전자서명기반의 인증 및 암호화에 대해 알아보고, 기존교육정보망의 환경과 보안요구사항에 대해 분석하고, 3장에서는 보다 안전한 교육정보망 구축을 위한 해킹방지 보안 SQL커널 시스템을 설계 및 제안한다. 4장에서는 제안한 모델을 평가 및 실험하고 마지막으로 5장에서는 결론을 맺는다.

2. 관련연구

2.1 공개키기반구조를 통한 전자서명 및 암호화

공개키기반구조는 공개키 암호기술이 안전하게 적용될 수 있는 기반구조로 키와 인증서를 안전하게 관리해 주는 서비스를 제공한다. 즉, 공개키 암호를 기반으로 하고 있는 전자서명 어플리케이션에서 무결성, 기밀성, 인증 등의 보안을 효율적이고 안정적으로 제공함을 목적으로 한다.

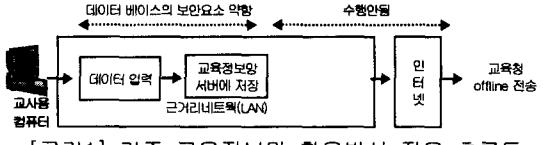
서버의 접근통제와 데이터의 보안을 수행하기 위하여 전자서명과 암호화를 모두 수행한다. 공개키기반구조는 공개키와 개인키의 키쌍을 사용하여 인증과 암호화를 수행하는 방법을 기본으로 한다.

인증은 사용자의 신분을 증명하기위한 것으로서, 미리 오프라인으로 인증받은 사용자가 개인키를 사용하여 전자서명을 생성한후, 이를 전자인증서에 적용시키게 된다.

암호화는 데이터를 전송할 때 인증서를 통하여 인증을 받은 후 공개되어 있는 상대편 서버의 공개키를 사용하여 데이터를 암호화함으로서 제3자로부터 기밀성을 제공할 수 있다.

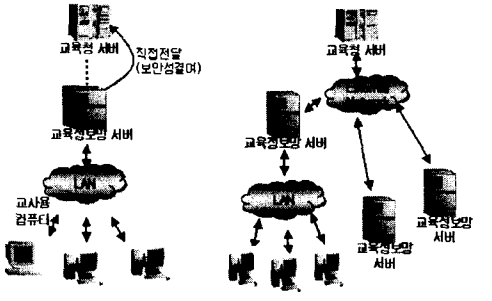
2.2 기존 교육정보망 요구사항 분석

기존의 교육정보망은 각 학교 자체의 근거리네트웍으로 구성되어 있어 외부 인터넷과 연결이 되어 있지 않으며, 내부에서 접속시 간단한 ID와 패스워드 만으로 접속할수 있기때문에, 보안성이 매우 취약하였다. 또한, 외부 네트웍망이 설정되지 않았기 때문에, 각 단말로부터 내부 서버로 취합된 데이터를 CD에 담아 교육청으로 직접 제출해야 하는 번거로움이 있었다[그림1]. 이는 네트웍에 대한 보안이 해결되지 않았기 때문이었다. 그러나, 현재 교육정보망은 각 학교의 서버를 외부 네트웍을 통하여 데이터를 전송하고 외부에서부터 내부의 서버에 접속하여 데이터를 접근 및 수정할 수 있도록 하는 구조의 교육정보망을 구축하고 있다. 따라서, 기존의 보안 취약점이였던, 네트웍 및 서버 접근통제 뿐만 아니라 데이터베이스의 접근통제도 보안하여야 한다.



[그림1] 기존 교육정보망 활용방식 적용 흐름도

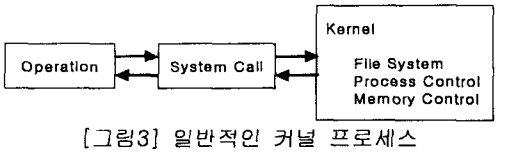
다음 그림과 같이 교육청 서버는 외부 네트웍에 분산되어 있는 교육정보망 서버의 정보를 안전하게 전송받을 수 있어야 하며, 서버내의 데이터베이스의 내용을 접근하고 수정하는데 인증 및 보안을 강화하여야 한다[그림2].



[그림2] 기존교육망과 향후추진교육망 구성 비교

2.3 일반 커널 시스템 분석

일반적인 커널 시스템에서 파일 시스템을 접근하거나, 프로세스를 컨트롤 하거나 메모리를 컨트롤하기 위해서는 명령어가 입력되면 시스템 콜이 수행되고 일단, 커널 레벨로 명령어가 넘어간다[그림3].



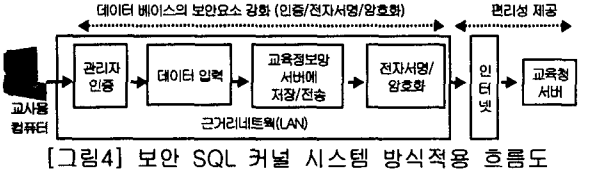
[그림3] 일반적인 커널 프로세스

이때, 파일 시스템의 경우 inode 등의 기본적인 접근 명령을 커널에서 수행하기 때문에, 커널 레벨로 접근하여 파일을 억세스 할 수 있다. 그러나, 커널 레벨을 억세스하기 위한 권한획득에 대한 제한사항을 일반 시스템은 가지고 있지않다. 따라서, 파일시스템의 해킹에 대한 가능성이 높다.

3. 제안하는 전자서명기반의 해킹방지보안 SQL커널 시스템

3.1 제안하는 교육정보망 구성도

향후 교육정보망[그림2]은 교사용컴퓨터에서 관리자 인증을 통하여 억세스에 대한 인증을 받고 입력 및 수정한후, 교육정보망 서버에 전송하고 인터넷을 통하여 교육청 서버로 전송하게 된다. 이때, 전송되는 데이터는 전자서명과 암호화를 수행하여 제3자로부터 해킹 및 수정되는 일이 없도록 한다[그림4]. 또한, 교육청서버에 저장되어 있는 데이터를 수정할 경우도 마찬가지로 관리자 인증서버로부터 인증을 받아 등급을 부여받은 후 접속을 허가하고 사용자의 권한에 따라 작업을 수행한다.



[그림4] 보안 SQL 커널 시스템 방식적용 흐름도

3.2 제안하는 보안 SQL 커널 시스템

3.2.1 보안 SQL 커널 시스템

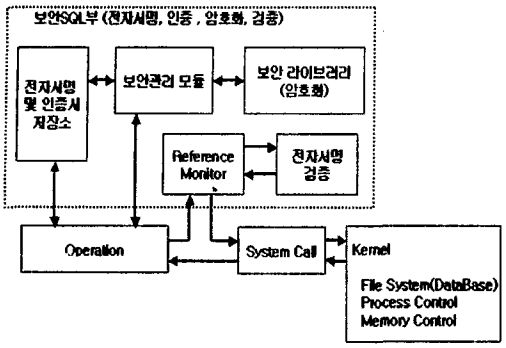
본 논문에서 제안하는 보안 SQL 커널 시스템은 일반 커널 시스템[그림3]에 보안SQL부를 첨부하여 보안커널 시스템을 설계한다. 본 시스템은 전자서명, 인증 및 암호화 등의 보안요소를 가미하고 있어서 운영체제로부터 명령이 들어왔을때, 커널레벨 접속 허용 전에 정해져 있는 보안 요소인 전자서명, 인증 및 암호화 요소들을 확인한 후 파일(데이터베이스)에 접근할 수 있게 한다.

보안SQL부는 인증과 데이터 암호화 부분을 수행한다. 보안관리모듈은 서버의 데이터베이스를 접근하기 위한 인증과 암·복호화에 대한 부분을 명령부를 통하여 관리한다. 이때, 이미 인증서버를 통하여 생성된 개인키로 전자서명을 생성하여 인증서를 만들고 보안SQL부의 전자서명 및 인증서 저장소에 보관한다. 전자서명 및 인증서는 암호화가 되어 있기 때문에, 보안라이브러리로 암·복호화를 수행한다[그림5].

운영체제는 사용자가 접근을 요청했을때, 보안SQL부로부터 미리 인증되고 암호화되어 저장된 전자서명 인증서를 요청하고 그로부터 받은 인증서를 참조 모니터를 통하여 전자서명을 검증한다.

이렇게 해서 인증된 사용자는 접근 권한을 획득하게 되고 시스템콜을 통하여 원하는 파일시스템 즉, 데이터베이스에 접근할 수 있다. 이때, 인증되지 않는 사용자는 파일에 접근이 허가되지 않으며 따라서 파일의 해독도 불가능하게 된다.

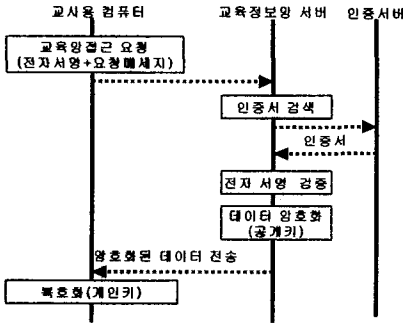
또한, 수정된 파일을 저장할 경우도 사용자의 인증을 받고 암호화하여 데이터베이스에 저장된다.



[그림5] 제안하는 보안 SQL 커널 시스템

3.2.2 보안 SQL 커널의 인증 메시지 흐름도

본 시스템의 접근제어 주체는 개인 사용자와 사용자 그룹이 될 수 있으며, 각각의 사용자는 사용자를 등록하는 SQL 문장에 의해 시스템에 등록된다. 데이터베이스를 사용하는 사용자에 대해 시스템은 사용자 인증으 수행하며, 사용자 인증의 처리는 공개키기반구조를 이용한다. 이 시스템에서 보안 관리자는 사용자의 인증서를 통하여 개개의 사용자에게 각각의 시스템 권한을 부여하여 접근을 통제한다.

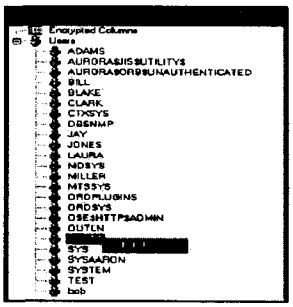


[그림6] 보안 SQL 커널의 인증 메시지 흐름도

인증메시지는 교사용 컴퓨터로부터 교육망 접근을 위한 요청메시지를 전자서명과 함께보내면 교육정보망서버에서 인증서버를 통해 인증서 검색을 요청한다. 인증서 검색요청에 의해 전송된 인증서를 통해 교사용 컴퓨터로부터 온 전자서명을 검증하면 본 사용자는 인증이 되고 권한을 획득하게 된다. 그러면 교육정보망 서버는 데이터베이스의 데이터를 공개키를 통해 암호화하여 전송한다. 이렇게 암호화되어 전송된 데이터는 접근요청을 한 교사용 컴퓨터에서 개인키를 사용하여 복호화된다.

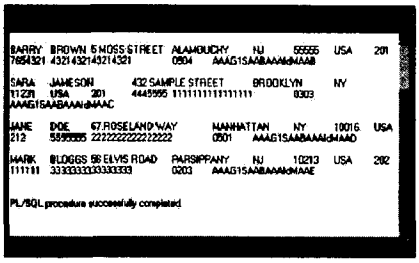
4. 평가 및 실험

파일(데이터베이스)에 접근요청 명령이 요청되면, 시스템은 미리 인증이 되어서 등록되어 있는 보안SQL 시스템 내의 Key Management System의 리스트를 검색하여 접근을 요청한 사용자의 공개키로 인증서의 내용을 확인한 후 접근권한을 부여한다[그림7]. 이때, 사용자의 공개키를 통하여 인증서에 암호화되어 있는 전자서명을 복호화하여 확인한다. 그러나, 리스트에 공개키가 등록되어 있지 않은 사용자는 접근 권한을 주지 않는다.



[그림7] 저장된 사용자 공개키 저장리스트

접근이 허가되어 권한이 부여되면 데이터베이스의 내용을 확인할 수 있으며, 데이터베이스의 내용을 수정하거나 추가하였을 경우는 공개키를 사용하여 데이터베이스의 내용을 암호화하여 저장한다[그림7].



[그림7] 암호화된 데이터베이스 컬럼 내용

5. 결 론

본 논문은 사용자의 인증 및 암호화를 수행함으로서 보안SQL 커널 시스템을 제안함으로서 시스템내의 파일(데이터베이스)의 데이터를 보호하는데 목적을 두었다.

또한, 인증서버에서 인증서를 생성하고 암호화하여 데이터를 저장함으로서 데이터베이스를 접근하기 위하여 커널로 명령이 넘겨지기 전에 보안 요소를 첨가할 수 있었다. 따라서, 보안SQL 커널에서는 인증을 통하여 부여된 권한으로 파일 내용을 확인, 수정 그리고 첨가 함으로서 접근자의 신분을 확인할 수 있었고, 데이터를 암호화하여 저장함으로서 데이터를 안전하게 저장하고 전송할 수 있었다. 따라서, 서버의 인증뿐만 아니라 서버 내 데이터를 접근할때도 이러한 인증과 암호화 등의 보안요소의 적용이 이루어져야 한다고 본다.

참고문헌

[1] Stanley R. Ames, Jr. et al., Security Kernel Design and Implementation: An Introduction, IEEE Cat. No. 830700-001 (July 1983)

[2] 한국 교육망 운영본부, 교육망정책보고서, 2002.

[3] Vijayalakshmi Atluri, Sushil Jajodia, Elisa Bertino, Transaction Processing in Multilevel Secure Databases with Kernelized Architecture, IEEE TRANSCATIONS VOL 9. NO.5, SEPTEMBER/OCTOBER 1997