PKI를 이용한 원격 통합 서버 관리 시스템

김지호*, 박세현*, 송오영*

*중앙대학교, 전자전기공학부

Remote Integrated Server Management System Based on PKI

Ji Ho Kim*, Se Hyun Park*, Oh Young Song*

*Chung-Ang Univ., School of Electrical & Electronic Engineering

요 약

본 논문에서는 기존 서버 원격관리 시스템이 안고있던 보안상의 문제점을 최근에 보안 인프라로써 각광을 받고 있는 PKI(Public Key Infrastructure)를 사용한 원격 통합 서버관리 시스템을 제안하고자 한다. 통합 인증서버는 관리자의 인증을 SCVP를 사용해서 검증하며, SSL(Secure Socket Layer)을 통해서 데이터의 기밀성을 보장한다. 또한 제안된 시스템은 관리자가 다양한 종류의 플랫폼과 운영체제를 한번의 인증과정으로 원격에서 통합 관리가 가능한 SSO(Single-Sign On) 시스템이다.

I. 서론

최근 들어 급속한 인터넷의 확산과 더불어 다양한 목적으로 기업, 연구소, 학교에서는 수대에서 수십대의 UNIX 기반의 서버를 사용한다. 이런 상황에서 서버 관리자는 다수의 서버를 효율적으로 관리할 수 있는 확장성, 보안성이 있는 관리 시스템의 필요성이 점점 증가하고 있다. 서버 관리란 시스템의 유지, 보수, 장애 예방, 장애 시 긴급 복구를 의미한다. 서버 모니터링을 통해서 장애를 사전에 방지해야 하며, 서버에 이상 시 긴급 대처하여 손실을 최소화해야 한다. 현재까지 서버 관리는 관리자가 여러대의 서버를 직접 콘솔에서 관리를 하거나 원격으로 서버를 관리하는 방법이 있다. 직접 콘솔 관리 시에는 관리자가 관리하는 서버가 많아질수록 서버관리가 비효율적이 되며 관리자가 퇴근을 했거나 외부에 있을 때 서버에 이상이 생기면 서버의 긴급 대처가 어려워진다. 관리자가 원격으로 서버를 관리 시에는 서버 이상에 대한 긴급 대처가 가능하지만 다음과 같은 보안상, 관리상의 문제점이 존재하게 된다.[7]

- 관리자 아이디, 패스워드 암기 부담
- 관리자 아이디, 패스워드 누출의 위험
- 중요한 데이터의 기밀성을 제공 못함
- 다수의 관리자가 다수의 서버 관리 시 다수의 아이디, 패스워드 관리 및 기록에 대한 보안 위험 존재
- 터미널 로그인을 통한 관리 시 서버의 네트워크에 문제가 있을 경우 접속 자체가 안됨

위와 같은 보안상의 문제점을 해결하기 위하여, 본 논문에서는 기존 서버 원격관리 시스템이 안고있던 보안상의 문제점을 최근에 보안 인프라로써 각광을 받고 있는 PKI(Public Key Infrastructure) [1][2][3][4]를 사용한 원격 통합 서버관리 시스템을 제안하고자 한다. PKI를 사용한 제안된 관리 시스템은 다음과 같은 보안상, 관리상의 장점이 존재한다.

- 공인 인증서를 사용한 인증(아이디, 패스워드 인증의 단점 해결)
- SSL을 통한 데이터 기밀성 제공[6]
- SCVP[5]를 통해서 검증을 수행하므로 인증서버의 부담 감소
- SCVP를 사용함으로써 인증서의 신뢰성 있는 검증
- 가정에서 인터넷을 통한 안전한 서버 관리 가능
- 관리자의 로그인 부인방지 기능제공
- 한번의 인증과정으로 다수의 서버를 동시에 관리가 가능한 SSO(Single-Sign On) 시스템

본 논문에서 제안된 시스템은 서버관리자가 공인 인증기관(한국정보인증, 한국전자인증, 금융결재원)에서 발급한 공인 인증서를 사용하므로 별도의 사설 CA, RA를 구축할 필요가 없다. 또한 제안된 시스템은 PKC(Public Key Certificate)를

사용하므로 PKI에서 제공하는 인증, 무결성, 기밀성, 부인방지 등의 보안 서비스를 받을 수 있다. 2장에서는 제안된 시스템의 구조 설명한다. 3장에서는 관리자 인증절차 및 검증 절차에 대해서 설명한다. 4장에서는 구현된 시스템에 대해서 설명한다. 그리고 5장 결론에서는 제안된 시스템을 적용한 결과와 결론에 대해서 설명한다.

II. 원격 통합 서버 관리 시스템 구조

통합 서버 관리시스템은 그림 1에서와 같이 크게 4부분으로 구성되어 있다. 각 부분에 대한 설명은 아래와 같다.

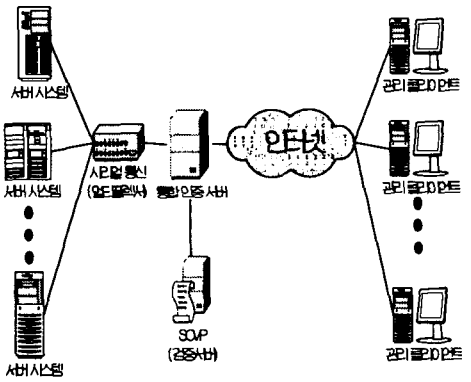

그림 1 원격 통합 서버 관리 시스템 구조

- 원격 관리 클라이언트: 원격 서버를 관리하기 위한 전용 프로그램으로 구성

- 통합 인증서버: 관리자가 서버 시스템에 접속하기 위한 인증과정을 수행(인증서가 등록 되어 있는지 확인, 인증서 검증을 SCVP에 요청, 인증메시지 검사)

- SCVP 서버: 통합 인증서버로부터 관리자의 인증서를 검증(인증서 경로 검증 수행)

- 서버 시스템들: 관리 대상이 되는 UNIX 기반의 서버. 통합 인증서버를 통해서 관리 클라이언트와 연결됨

관리 클라이언트는 TCP/IP 기반의 인터넷 망 또는 LAN을 통해 통합 인증서버와 연결이 가능하다. 관리 클라이언트는 전용의 관리 프로그램으로 구성되며 통합 인증서버는 멀티 스레드로 동작하는 다중 접속 서버이다. 관리자는 집이나 외부 인터넷이 가능한 곳이면 어디든지 관리프로그램 설치와 더불어 공인 인증서와 개인키만 가지고 있으면 원격으로 서버 관리가 가능해진다. 통합 인증서버는 관리자 인증서의 검증을 SCVP를 사용하여 검증한다. SCVP를 사용했을 때의 장점은 인증서버의 부담을 줄일 수 있는 점과 인증서 경로검증을 수행하는 SCVP를 사용함으로써 인증서의 보다 신뢰성 있는 검증이 가능한 장점이 있다. 통합 인증서버와 서버시스템들은 직렬통신으로 직접 연결되어 있다. 직렬통신은 외부에 노출이 안되어서 보안상 안전하며 네트워크의 이상과는 관계가 없는 비교적 장애가 거의 없는 통신 방법이다.

III. 관리자 인증 및 인증서 검증 절차

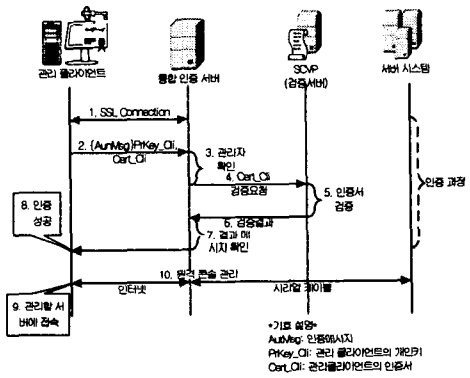

그림 2 관리 시스템간 메시지 흐름도

그림 2는 인증을 수행하기 위한 관리 시스템간 메시지 흐름도를 보여준다. 먼저 관리 클라이언트와 통합 인증서버 사이에 데이터의 기밀성을 위한 server side SSL 연결을 맺고 관리자의 개인키로 인증메시지를 전자서명해서 인증서와 같이 통합 인증서버에 보낸다. 통합 인증서버는 클라이언트로부터 받은 인증서가 등록된 관리자의 인증서인지 확인한 다음 SCVP에 인증서 검증요청을 한다. SCVP로의 인증서 경로 검증 결과 인증서의 상태가 유효(Valid)한 상태이면 통합 인증서버는 인증메시지를 사인검증을 한 다음 인증메시지가 올바를 경우 관리자는 인증에 성공하게 된다. 그림 3은 이와 같은 인증, 검증 절차의 순서도를 보여준다. 본 인증 시스템에서는 관리자가 사전에 관리자의 인증서를 통합 인증서버에 등록하는 절차가 필요하다. 만약 관리자의 인증 및 인증서 검증 도중에 인증서가 통합 인증서버에 등록이 되어있지 않거나 인증서 검증 결과 유효한 인증서가 아닐 때, 또는 인증 메시지 사인 검증에 실패했을 경우 관리자는 인증에 실패하게 되어 통합 인증서버와 접속을 종료하게 된다.

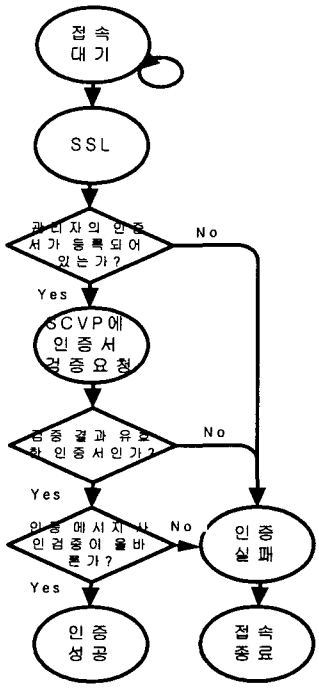

그림 3 인증서버에서 인증 및 검증 절차 순서도

관리자가 인증과정을 통과하게 되면 통합 인증서버와 시리얼 통신으로 연결되어 있는 서버들 중에서 관리하고자 하는 서버에 접속이 가능하다. 서버에 접속 시 다시 로그인 할 필요가 없이 바로 슈퍼유저 권한으로 콘솔환경에서 접속이 가능하다. 이 방법은 터미널을 통한 원격 접속의 한계인 네트워크 데몬(demon)에 이상이 생겼을 때 접속이 안되는 문제점을 해결한다. 또한 원격에서 한 번의 인증과정으로 다수의 서버를 동시에 접속/관리가 가능하다. 이것은 관리 편의성을 좋게 해서 관리비용과 수고를 줄일 수 있는 장점이 있다. 최근에 기업 인트라넷과 웹서비스에서 많이 확산되고있는 SSO(Single Sign On) 시스템이므로 접근제어의 통합 관리가 가능해진다. 그리고 차후에 PMI와의 연동 시 권리자에 따라 권한을 부여 할 수 있어 RBAC(Role Based Access Control)가 가능해진다.[8] 관리자가 수행하는 모든 작업은 통합 인증서버까지 SSL을 통해 암호화되어 전송되고 통합 인증 서버에서 서버 시스템까지는 직렬통신으로 데이터가 전송되기 때문에. 관리자의 모든 작업은 네트워크상에서 기밀성을 보장한다. 통합 콘솔 서버에서는 관리자의 접속 로그, 작업 로그를 저장하여 보관한다. 이것은 관리자 접속과 작업 내용에 대한 부인방지 기능을 제공한다. 이것은 유사시 접속 현황과 작업현황 분석에 사용될 수 있다. 또한 이런 로그 정보가 훼손되는 것을 방지하기 위해서 통합 인증서버의 개인 키로 전자서명해서 로그정보를 저장한다.

IV. Testbed 시스템 구축

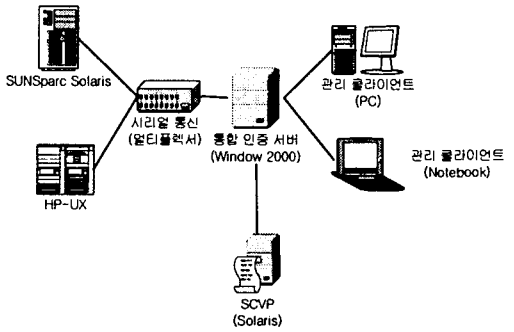

그림 4 테스트 시스템 구축

본 논문에서 제안된 통합 서버 관리 시스템의 Testbed 시스템을 구축하였고 그림 4는 그 구조를 보여 준다. 테스트 시스템은 윈도우 운영체제의 관리 클라이언트와 통합 인증서버, 유닉스 운영체제의 SCVP 서버와 관리 대상 서버들로 구성된다.

제안된 시스템 테스트는 공인 인증기관(한국정보인증, 한국전자인증, 금융결재원)에서 발급 받은 공인 인증서와 자체 개발한 사설 CA로 발급 받은 사설 인증서를 사용하여 테스트하였다. 그림 5는 관리 클라이언트에서 테스트 과정을 보여준다. 관리자가 접속할 통합 인증서버를 선택하면 개인키의 암호 입력 후 개인키로 인증메시지를 전자서명해서 인증서와 같이 통합 인증서버에 보낸다. 관리자는 인증에 성공하게 되면 서버들 중에서 관리하고자 하는 서버에 접속한다. 서버에 연결되면 콘솔 윈도우에서 관리작업을 수행한다.

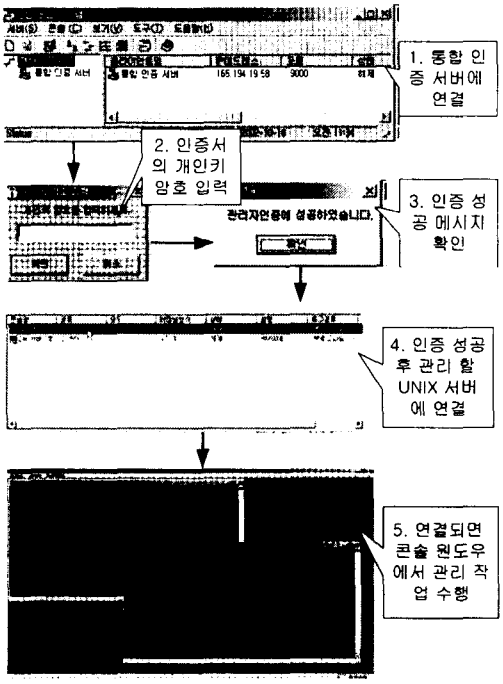

그림 5 관리 클라이언트

V. 결론

본 논문에서는 기존 서버 원격관리 시스템이 안고있던 보안상의 문제점을 최근에 보안 인프라로써 각광을 받고 있는 PKI(Public Key Infrastructure)를 사용한 원격 통합 서버관리 시스템을 제안하였고 Testbed 시스템을 구축해 테스트를 수행하였다. Testbed 시스템으로 제안한 시스템을 검증 한 결과 원격에서 공인 인증서 및 사실 인증서를 사용한 서버관리 시스템이 사용자 인증, 검증, 데이터 기밀성 등의 측면에서 기존의 서버 관리 시스템 보다 보안상 안전함을 확인하였다. 제안된 원격 서버 관리 시스템은 통합 관리가 가능한 유연한 확장성과 보안성을 갖추고 있다. 이 시스템은 차후에 회사, 학교, 연구소의 서버관리에 사용할 경우 관리 수고 및 비용을 줄일 수 있고 보안성을 향상시킬 수 있다.

참고문헌

[1] R. Housley, W. Ford, W.: Polk, and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, 1999

[2] ITUT public-key and attribute certifica te frameworks, X509, 2000

[3] Russ Housley and Tim Polk, Planning for PKI, Wiley Computing Publishing, 2001

[4] Andrew Hash and William Duane and Celia Joseph and Derek Brink, PKI:Implementating and Managing E-Security, McGraw-Hill, 2001

[5] A. Malpani, R. Housley, T. Freeman, Simple Certificate Validation Protocol, 2002

[6] Stephen A. Thomas, SSL and TLS Essestials: Securing the Web, Wileyl, 2000

[7] Stuart McClure and Joel Scambra and George Kurtz, Hacking Exposed, McGraw-Hill, 2001.

[8] S. Farrell and R. Housely, An Internet Attribute Certificate Profile for Authentication, RFC 3281, 2002.