내부 프로시저를 이용한 인증서 상태 검증 시스템의 관한 연구

김현철*, 이종호*, 이옥경*, 오해석*
*숭실대학교 컴퓨터학과
e-mail : dmzpolice78@korea.com

A Study on Certificate Status Validation System using Internal Procedure

Hyun-Chul Kim*, Chong-Ho Lee*, Ok-Kyoung Lee*, Hae-Seok Oh*
*Dept of Computer Science. SoongSil University

요 약

2002년 기준 우리나라 전체 인구의 약 67%인 3000만명 정도가 인터넷을 사용하고 있으며, 인터넷 사용량 증가 속도 또한 매년 기하급수적으로 늘어나고 있다. 하지만 개방형 네트워크인 인터넷은 개인정보누출, 개인정보 위변조 등과 같은 문제를 내포하고 있으며 이러한 개인 신상정보와 관련한 문제를 해결하기 위하여 PKI기반의 인증서 검증 시스템 즉 공개키 기반의 인증서 검증 시스템이 제안 되었다. 본 논문에서는 PKI 기반의 인증서 검증 시스템에서의 인증서 상태 검증 방식 기법인 CRL기반의 인증서 상태 검증 방식과, Delta-CRL 기반의 인증서 상태 검증 방식, OCSP 기반의 인증서 상태 검증 방식에 대해 기술하고 현재 사용되고 있는 인증서 상태 검증 방식의 문제점인 실시간 처리와 네트워크 과부하 문제를 해결하기 위한 방안으로 내부 프로시저와 데이터베이스를 이용한 클라이언트-서버 기반의 인증서 상태 검증 시스템을 제안하고자 한다.

1. 서 론

PKI(Public Key Infrastructure)기반의 인증서 검증 시스템은 인터넷을 통해 전송되는 중요 정보의 불법 노출을 방지하기 위한 기밀성(Confidentiality), 정보의 위조 및 변조 여부를 판단하는 무결성(Integrity), 정보의 송 · 수신자가 송 · 수신 사실을 부인하지 못하도록 하는 부인방지(Non-Repudiation), 전송된 정보의 송수신자와 수신자를 확실하게 증명해주는 인증(Authentication)을 제공해 주고 있다.[2][3]

위와 같이 PKI 기반의 인증서 검증 방식에서 제공되는 기술은 기존 오프라인으로 처리 되어지던 업무들이 온라인 처리로 변해가고 있는 시점에서의 가장 큰 문제점인 개인정보 누출, 개인정보 위조 및 변조에 관한 문제점을
해결해 줄 수 있다.

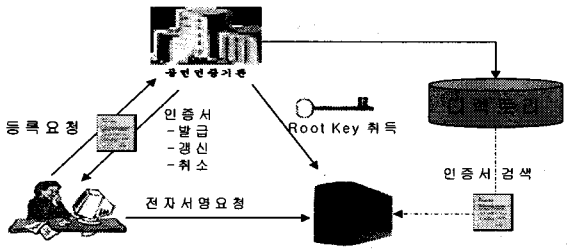
하지만 기존의 PKI기반의 인증서 검증 시스템에서의 인증서 상태검증 방식인 CRL방식, Delta-CRL방식, OCSP방식 모두 중대한 문제점을 가지고 있다.

본 논문에서는 기존 PKI기반의 인증서 검증 시스템에서의 인증서 상태 검증 방식인 CRL방식, Delta-CRL방식, OCSP방식에 대해 2장에서 기술하고, 3장에서 기존 인증서 상태 검증 방식의 문제점을 기술한다. 4장에서는 본 논문에서 제안하는 시스템인 데이터베이스와 내부 프로시저를 이용한 인증서 상태 검증 시스템에 대하여 5장에서는 제안하는 시스템의 기대효과에 대해 기술하고 6장에서 결론을 맺는다.

2. 관련 연구

PKI 기반의 인증서 검증 시스템은 공개키 인증서를 통해 전자상거래에서의 기밀성, 무결성, 부인방지, 인증을 제공하는 정보 보호 시스템이다.

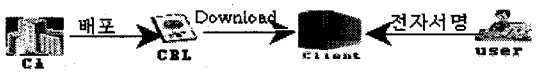
국내에서는 1999년 7월 전자서명법이 발표되면서 PKI를 이용한 정보 보호 시스템의 법적인 토대가 마련되었으며, 2000년 국가공인 PKI 운용 기관인 공인인증기관이 지정되었고 현재 PKI기반의 인증서 시스템은 금융권에서 개인의 정보보호를 위해 주로 적용되어지고 있으며 PKI기반의 인증서 시스템의 구조는 아래 [그림1]과 같다.[3]



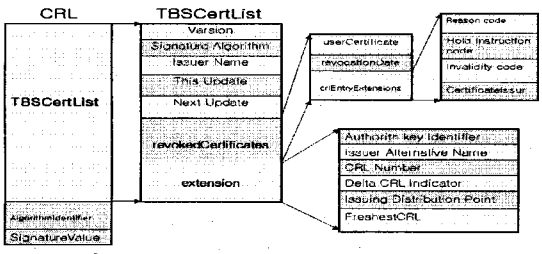
[그림 1] 공개키 기반구조

2-1CRL(Certification Revocation List)

일반적으로 인증서의 유효기간은 인증서 발급일로부터 1년이다. 하지만 인증서 유효기간 이전에 사용자의 개인키가 노출되거나, 사용자가 인증서 취소를 요청했을 때, 사용자가 인증서를 발행했던 기관으로부터 퇴직 했을 때와 같이 몇 가지 이유로 인해 인증서 유효기간 내에 폐지 될 수 있는데 이러한 폐지된 인증서의 불법적인 사용과 도용을 막기 위해 폐지된 인증서를 하나의 리스트로 모아 놓은 것이 인증서 폐지목록 즉 CRL이다.[1] 현재 사용되고 인증서는 CCITT에서 제정한 X.509V3이며 X.509 CRL방법은 1993년 X.509 version2에서 CRL version1이 제정되었고, 1997년 X.509 version3에서 CRLversion2가 제정되었다. 현재 RFC2459에서 CRL 프로파일을 규정하고 있다. CRL포맷은 [그림3]과 같으며, CRL기반의 인증서 검증 방식의 수행과정은[그림2]과 같다.



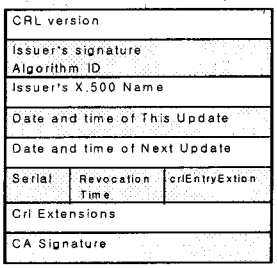
[그림 2] CRL기반의 인증서 검증 방식 수행과정



[그림 3] X.509v3 CRL 포맷

2-2 Delta-CRL

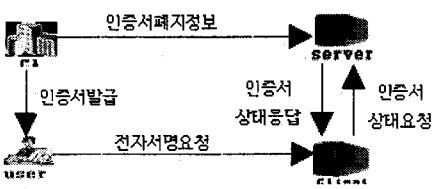
CRL의 주기적인 갱신기간(24시간) 동안 현재성 문제를 보완하기 위해서 제안된 방식으로 Delta-CRL은 가장 최근 폐지된 인증서만을 포함하는 인증서 폐지목록이다. 즉 CRL이 생성된 때부터 다음 CRL생성까지의 포함된 폐지 인증서와의 차이만큼을 포함하는 인증서 폐지목록이다. 따라서 사용자는 전체 CRL을 다운 받을 필요 없이 가장 최근에 발급된 CRL과 그 이전에 발급된 CRL과의 차이만큼을 다운 받아서 사용하기 때문에 CRL을 저장하기 위한 공간을 줄일 수 있으며, CRL 갱신 이전에 폐지목록을 제공하기 때문에 CRL에 현재성 문제를 해결할 수 있다는 장점이 있다. [그림4]는 Delta-CRL포맷이다.



[그림 4] Delta-CRL 포맷

2-3OCSP(Online Certificate Status Protocol)

OCSP기반의 인증서 상태 검증 방식은 CRL기반의 인증서 상태 검증 방식의 문제점인 인증서 상태의 대한 실시간 반영 문제를 해결하기 위해 제안되었다.[4] OCSP의 데이터 구조는 OCSP클라이언트가 OCSP서버로 인증서 상태 정보를 요구하는 Request 메시지와 요청에 대한 결과로 OCSP서버에서 OCSP클라이언트로 보내는 Respon
se 메시지로 구성되며 OCSP 인증서 상태 검증 방식은 사용자가 CA로부터 인증서를 발급 받은 후 사용자가 정해진 포맷으로 OCSP 클라이언트에게 전자서명을 요청하면 OCSP 클라이언트는 정해진 포맷 즉 Request 메시지 포맷으로 OCSP서버에게 인증서 상태를 요청하고, OCSP서버는 요청받은 인증서에 대한 상태 정보를 검색하여 결과의 대한 응답으로 정해진 포맷 즉 Response 메시지 포맷으로 OCSP클라이언트로 넘겨줌으로써 실시간으로 인증서의 대한 상태 검증을 수행하는 방식이다. OCSP 기반의 인증서 검증 방식의 수행 과정은 [그림5]와 같다.[4][5]



[그림 5] OCSP기반의 인증서 검증 방식 수행과정

3. 문제점

3-1 CRL

CRL 기반의 인증서 상태 검증 방식은 인증서의 발급이 증가할수록 폐지되는 인증서의 양도 비례적으로 증가하기 때문에 CRL을 저장하기 위한 공간이 증가한다는 점과 하루에 한번씩 인증서 폐지목록을 다운받아야 하기 때문에 인증서 상태에 대한 실시간 반영이 어렵다는 문제가 있다.[1]

3-2 Delta-CRL

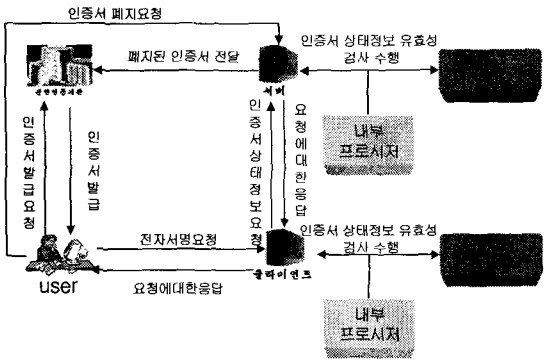
Delta-CRL은 CRL 갱신 시간 이전에 폐지된 인증서에 대해서만 실시간 검증을 제공하는 단점과, 최초 CRL과 이후 생성된 Delta-CRL의 정보는 다음 CRL의 정보와 동일하기 때문에 검증 속도의 성능은 개선되지 않는다는 문제가 있다.

3-3OCSP

OCSP기반의 인증서 상태 검증 시스템의 최대 장점은 기존의 CRL, Delta-CRL기반의 인증서 상태 검증 방식의 최대 단점인 인증서 상태에 대한 실시간 반영이 가능하다는 점이다. 하지만 실시간으로 인증서에 대한 상태검증을 수행해야 하기 때문에 많은 통신량 발생으로 인한 네트워크 과부하 문제이며, 그에 따른 결과로 네트워크 상태에 따라 인증서 상태 검증 수행 시간이 달라진다는 단점이 있다.[4][5]

4. 제안하는 시스템

본 논문에서는 인증서 상태 검증 시스템에서의 인증서상태 검증 수행 시간을 향상시키기 위한 방법으로 내부 프로시저를 이용한 데이터베이스 기반의 클라이언트-서버 모델을 제안하고자 한다. 제안하는 시스템의 구성도는 [그림6]과 같다.



[그림 6] 제안하는 시스템 구성도

4-1 내부 프로시저

데이터베이스를 이용하기 때문에 인증서 상태 검증을 위해서 여러 번 반복적으로 SQL문을 사용하게 된다. 이러한 SQL문에 빈번한 사용은 프로그램 실행속도를 저하 시킬 뿐 아니라 전송되는 SQL문으로 인한 네트워크 과부하가 발생 할 수 있다.

내부 프로시저는 여러 번 반복적으로 실행되는 SQL문을 하나로 모아 미리 컴파일 하고 실행결과를 캐시에 저장해 놓고 사용하기 때문에 네트워크 과부하 문제를 해결 할 수 있으며, 시스템 내에 캐쉬를 이용하기 때문에 인증서 상태 검증 속도 또한 향상 시킬 수 있다.[6]

4-2클라이언트

본 논문에서 제안하는 클라이언트 시스템은 자체적으로

사용자에 의한 전자서명 요청을 수행하고, 전자서명을 요청한 인증서에 대한 인증서 상태 정보 검증 기능을 수행 할 수 있는 시스템이며 제안하는 클라이언트 시스템의 기능은 다음과 같다.

▶ 사용자의 전자 서명 요청을 받아들이고 수행 한다.

▶ 전자서명을 요청한 사용자의 인증서 상태 정보를 검증

▶ 전자 서명을 요청한 인증서 상태 정보가 클라이언트 데이터베이스에 있을 경우 검증의 결과를 사용자에게 전송

▶ 전자 서명을 요청한 인증서 상태 정보가 클라이언트 데이터베이스에 없을 경우 서버로 인증서 상태 정보를 요청한다.

▶ 서버로부터 요청에 대한 응답의 결과로 인증서 상태 정보를 받아들이고, 전자서명 요청한 인증서 정보를 클라이언트 데이터베이스에 저장함으로써 인증서 상 태 검증에 대한 실시간 문제를 해결 할 수 있다.

4-2 서버

본 논문에서 제안 하는 서버 시스템은 사용자로부터 인증서 폐지 신청을 직접 받아들이고 변경된 인증서 폐지정보를 클라이언트로 보낸다.

또한 클라이언트로부터의 인증서 상태 정보 요청에 대한 처리를 수행하고 처리 결과를 클라이언트로 보내는 기능을 수행하는 시스템이다. 제안하는 서버 시스템의 기능은 다음과 같다.

▶ 사용자로부터 직접 인증서 폐지 신청을 받아들일 수 있다.

▶ 클라이언트로부터의 인증서 상태 정보 요청에 대

한 처리를 수행 하고, 처리 결과를 클라이언트로 보낼 수 있다.

5. 기대 효과

본 논문에서 제안하는 내부 프로시저를 이용한 인증서 상태 정보 검증 시스템은 클라이언트-서버 모델을 이용함으써 인증서 상태 정보 검증 과정에 있어서 실시간 문제를 해결 할 수 있으며, 내부 처리 과정에서 내부 프로시저를 이용함으로써 다음과 같은 기대 효과를 가진다.

▶ 프로그램수행 과정에서 내부 프로시저는 처음 실행시 한번만 컴파일하고 컴파일 결과를 시스템내의 캐쉬 메모리에 저장해 놓기 때문에 인증서 상태 검증에 걸리는 시간을 줄 일 수 있다.

▶ 네트워크에서 오고 가는 긴 SQL문으로 인한 네트워크 과부하를 줄일 수 있다.

▶ 내부 프로시저는 공개가 되지 않으므로 기본 소스가 노출되더라도 내부 처리과정이 들어나지 않으므로 보안상의 안정성을 가질 수 있다.

▶ 원격 프로시저를 이용하여 원격 서버의 데이터를 처리 할 수 있다.

6. 결론

본 논문에서는 기존 PKI기반의 인증서 시스템에서의 인증서 상태 검증 방식에 대해 기술하였고 또한 각 방식에 대한 문제점을 제시 하였다.

본 논문에서는 기존 방식의 문제점을 해결하면서 인증서 상태 검증 과정에 있어서 인증서 검증 시간 향상을 위한 내부 프로시저를 이용한 인증서 상태 검증 시스템을 제안하였다. 향후 제시한 시스템을 실제 PKI기반 인증서 검증 시스템에 적용할 수 있도록 연구를 계속 진행해 나갈 것이다.

참 고 문 헌

[1] J. Willemson "Certificate Revocation Paradigms" Technical Report, Cybernetica. 1998

[2] Russ Housley & Tim Polke "Planning for PKI" WILEY. 2001

[3] 권태경, 강명호, 김승주, 서정욱, 진승헌 "정보 보호 표준 개론" 한국정보통신기술협회. 2002

[4] M.Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. "Internet X.509 Public key Infrastructure On-line Certificate Status Protocol-OCSP",RFC2560, 1999

[5] M.Myers, R. Ankney, C. Adams, S. Farrell and C. Covey "Online Certificate Status Protocol, Version2" draft-ietf-pkix-ocspv2-02, March 2001.

[6] 정원혁 "Microsoft SQL Server200 전문가로 가는 지름길" 대림. 2001