서명자 정보를 이용한 인증서 상태 검증 기법

*김현철° **이용준 **백주호 *오해석
*경원대학교 전자계산학과
**숭실대학교 컴퓨터공학과
dmzpolice78@korea.com° yjlee@koscom.co.kr backjuho@psmkorea.co.kr oh@kyungwon.ac.kr

Certificate Status Validation Method using Signer Information

*Hyun-Chul Kim° **Yong-Jun Lee **Ju-ho Back *Hae-Seok Oh
*Dept. of Computer Science, Kyungwon University
**Dept. of Computer Science, Soongsil University

요 약

인증서 상태 검증이란 해당 거래에서 사용되는 인증서에 대한 유효성을 결정하는 과정으로 인증서를 이용하는 거래에 90%이상이 실시간적이고 신속 정확한 처리를 필요로 하는 인터넷뱅킹과 증권 트레이닝에 사용된다. 하지만 기존의 CRL을 이용한 인증서 상태 검증 기법은 인증서 상태의 대한 실시간성을 반영할 수 없다는 문제점이 있다. 이와 같은 CRL 기반의 인증서 상태 검증 기법의 문제점을 해결하고자 OCSP를 이용한 인증서 상태 검증 기법이 제기되었다. 이 기법은 인증서 상태에 대한 실시간성 문제는 해결 할 수 있었지만 OCSP 서버에 대한 중앙 집중화 처리구조로 인해 네트워크 과부하라는 또 다른 문제가 발생한다. 따라서 본 논문에서는 서명자가 인증서 발급을 요청하고 이에 따른 결과로 인증서가 인증기관으로부터 발급되었을 때 서명자정보와 인증서 일련번호가 인증기관 데이터베이스에 매칭되어 저장된다는 점에 기인하여 위애 문제점들을 해결할 수 있는 서명자의 정보를 이용한 인증서 상태 검증 기법을 제안한다.

1. 서 론

현재 공인PKI 사용율의 90%이상이 실시간 처리를 필요로 하는 인터넷뱅킹과 증권 트레이닝에 사용되어 진다. 이러한 만큼 인증서의 대한 신뢰성 보장이 반드시 선행되어야하며 이를 위해 해당 인증서가 유효한 인증서인지 아닌지를 판별하는 유효성 검사 즉 인증서 상태 검증을 거쳐야 한다.

현재 인증서 상태 검증을 위해 가장 많이 사용하는 방법은 인증서 폐지목록(CRL : Certificate Revocation List)을 이용하는 것이다. 이 방법은 일정시간 간격으로 CRL을 다운 받아 인증서 상태 검증이 필요할 때마다 CRL과 비교하여 인증서의 유효 여부를 판단한다.[1]

하지만 이 방법은 일정시간 간격으로 CRL을 다운 받기 때문에 인증서 상태에 대한 현재성을 반영할 수 없으며 발급된 인증서 수가 증가 할수록 폐지되는 되는 인증서 수 또한 비례적으로 증가한다는 문제가 있다.

이러한 CRL에 문제점을 해결하기 위해 제기된 방법으로 OCSP(Online Certificate Status Protocal)가 있다. 이 방법은 실시간으로 인증서 상태를 온라인에서 확인 할 수 있다. 하지만 실시간으로 인증서의 대한 유효성 검증을 수행해야 하기 때문에 서버 집중적이며 그로인해 지역분산이 어렵고 인증서 상태 검증에 소요되는 시간이 오래 걸린다는 문제가 있다.

본 논문에서는 서명자가 인증서 발급을 요청하고 이에 따른 결과로 인증서가 인증기관으로부터 발급되었을 때 서명자정보와 인증서 일련번호가 인증기곤 데이터베이스에 매칭되어 저장된다는 점에 기인하여 전자서명을 요청하는 서명자의 정보만을 이용한 인증서 상태 검증 시스템을 제안하고자 한다.

본 논문의 구성은 아래와 같다. 2절에서 관련연구에 대하여 기술하고 3장에서 본 논문에서 제안하는 서명자 정보를 이용한 인증서 상태 검증 시스템을 제안 한다. 4장에서 결론을 맺는다.

2. 관련연구

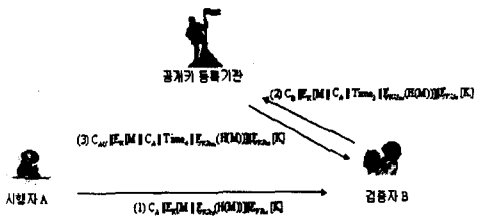
2.1 공개키 기반구조(Public Key Infrastructure)

PKI는 공개키 알고리즘을 통한 전자상거래, 금융거래등과 같은 여러 가지 응용분야에서 인증서의 사용을 용이하도록 정책, 수단, 도구등을 수립하고 제공하는 보안 시스템으로서 인증서의 대상이 되는 사용자나 사용자 시스템을 의미하는 End-Entity, 인증서를 생성 발급 운영 폐지를 담당하는 인증기관(CA:Certification Authority), 인증기관 대신 사용자들이 인증서 신청시 그들의 신분과 소속을 확인하는 기능을 수행하는 등록기관(RA: Registration Authority), 인증서와 사용자 관련 정보 상호 인증서 쌍 및 인증서 취소 목록 등을 저장 및 검색할 수 있는 장소에 역할을 하는 디렉토리(Directory)로 구성된다.

또한 합법적인 서명자만이 전자서명을 생성할 수 있는 위조불가(Unforgeable), 전자서명의 서명자를 불특정 다수가 검증할 수 있는 서명자인증(User Authentication), 서명자가 서명한 사실을 부인할 수 없는 부인방지(Non-Repudiation), 서명한 전자 문서의 내용을 변경할 수 없는 변경불가(Unalterable), 전자문서의 서명을 다른 전자문서의 서명으로 사용할 없는 재사용불가(Not Reusable)등의 기능을 제공한다.[2]

2.2 인증서 상태 검증

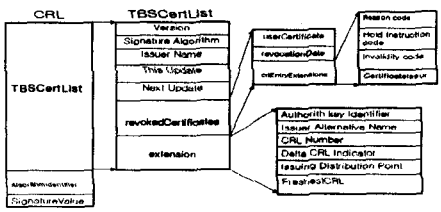
인증서 상태 검증은 인증서의 소유자 및 발행자의 신원과 인증서의 현재 상태를 확인하는 부분으로서 PKI 처리의 소요되는 시간 중 90% 이상이 인증서 상태 검증 작업에 해당 될 정도로 전자상거래시 가장 중요한 부분이다. [그림 1]은 인증서 상태 검증 진행과정을 보여주고 있다.



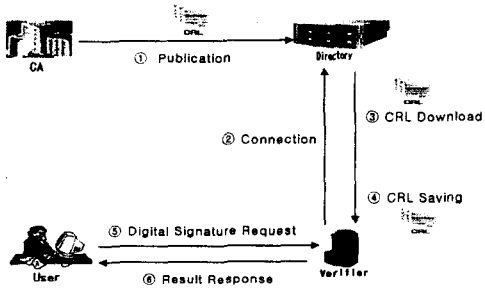
[그림 1] 인증서 상태 검증 진행과정

2.3 인증서 폐지 목록(CRL : Certificate Revocation List)

CRL은 폐지된 인증서를 모아놓은 목록으로 인증기관이 폐지된 모든 인증서의 일련번호, 폐지시간, 폐지이유를 주기적으로 생성하여 서명한 후 디렉토리에 게시한 후 게시된 CRL을 검증자가 검증시점에 디렉토리로부터 검색하고 다운로드 한 후 상태 검증시 다운 받은 CRL을 이용하는 방법이다. CRL에 대한 프로파일은 표준문서 RFC 2459에 정의 되어 있으며 [그림 2]에서와 같이 V509. V2 프로파일을 이용하며 CRL을 이용한 인증서 상태 검증 방법은 [그림 3]과 같다.[1]



[그림 2] X.509v2 CRL



[그림 3] CRL을 이용한 인증서 상태 검증 방법

2.4 OCSP(Online Certificate Status Protocol)

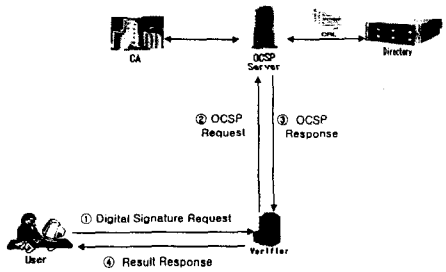
OCSP는 기본적으로 OCSP 서버와 OCSP 클라이언트로 구성되며 OCSP클라이언트 OCSP서버에게 OCSP를 이용하여 인증서에 대한 상태를 요구하며 서버는 요청에 대한 응답을 주는 형태로 이루어지는 방식이다.[3]

OCSP Response Value <표-1>과 같이 3가지이다.

<표-1> OCSP Response Value

유효(Good)	: 인증서가 유효함을 의미
폐지(Revoked)	: 인증서가 폐지된 상태임을 의미
알수없음(Unknown)	: 응답 서버가 해당 인증서의 상태를 알 수 없음

하지만 이 방식은 서명자가 인증서 상태 검증을 요청할 때마다 중앙 집중적인 서버를 이용함으로 서버에 부하가 집중되며, 지역적인 분산 및 부과적인 시스템에 도입이 필요하다는 문제점이 있다. 서버로 부하 집중이 고도화 됨에 따라 처리비용은 지수적으로 증가하게 되며 인증기관 마다 각각 다른 정책을 적용함으로 상호연동에 어렵다는 점도 문제점이다.[3] [그림 4]는 OCSP를 이용한 인증서 상태 검증 방법을 보여주고 있다.



[그림 4] CRL을 이용한 인증서 상태 검증 방법

2.5 SCVP(Simple Certificate Validation Protocol)

SCVP는 OCSP와 동일한 구조를 가지고 있으며 클라이언트의 요청으로부터 서버는 OCSP의 기능외에도 추가적인 인증서 경로 등에 대한 정보를 제공하는 방법이다.[4][5]

3. 제안하는 시스템

기존의 인증서 검증 시스템에서 서명자는 자신이 서명한 전자서명과 전자문서 그리고 인증서를 가지고 유효성 검증을 요청한다. 이때 전자서명과 전자문서는 전자서명 검증을 위해 사용되며 인증서는 실제 거래에 대한 유효성을 파악하기 위한 인증서 상태 검증에 사용된다. 이때 전송하는 정보의 총 크기는 전자문서 크기에 따라 차이는 있지만 대략 1500Byte정도이며 그 중에서 인증서 상태 검증을 위해 사용되는 인증서의 크기는 1300Byte이다.

더욱이 서명자는 해당 거래가 발생 할 때마다 매번 유효성 검증을 위한 전자서명과 전자문서, 인증서를 전송해야 하며 검증자 측에는 요청에 있을 때마다 유효성 검증을 수행해야 한다. 그로인해 네트워크 과부하 및 서버 과부하 문제가 발생한

다. 또한 부하 집중이 고도화됨에 따라 처리비용이 지수적으로 증가하는 2차적인 문제가 발생한다.

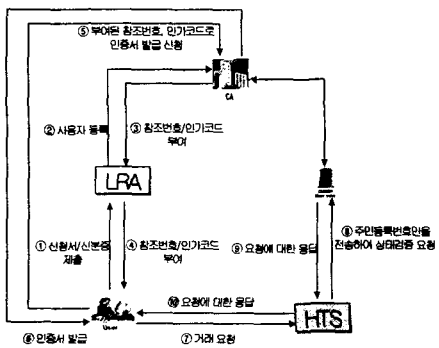
본 논문에서 제안하는 기법은 User, HTS, LRA, CA로 구성되며 구성요소에 대한 설명은 아래와 같다.

① User or End-Entity
CA로부터 발급받은 인증서를 소유하는 개인 또는 법인으로 인증서의 대한 유효성 검증을 요청하는 객체.

② HTS(Home Training System)
End-Entity가 사용하는 응용 프로그램.

③ LRA
가입자 등록 정보를 입력받고 입력 받은 정보를 CA로 전송함으로써 가입자 등록 업무를 수행하는 기관 또는 프로그램. LRA Client(LRAC)와 LRA Server(LRAS)로 구분할 수 있으며 LRAC는 가입자 등록 정보를 입력 받고 LRA Server로 전송하며, 등록 결과를 LRA Server로부터 받는 응용 프로그램이며 LRAS는 LRA Client의 등록 정보를 받아서 CA 서버로 전송하고, 등록 결과를 CA로부터 받아서 LRA Client로 전달하는 프로그램.

④ CA(Certification Authority)
인증서의 대한 발급, 변경, 폐지를 담당하는 기관



[그림 5] 제안하는 시스템

본 논문에서 제안하는 기법의 처리절차는 아래와 같다.

1. 사용자는 LRA에게 인증서 발급 신청서를 제출한다.
2. LRA는 사용자로부터 접수 받은 인증서 신청서를 기반으로 사용자를 인증기관에 등록한다.
3. CA는 접수된 신청서에 대해 적법성 여부를 판단하고 참조번호와 인가코드를 사용자에게 부여한다.
4. 사용자는 인증기관으로부터 부여받은 참조번호와 인가코드를 이용하여 인증서 발급을 신청한다.
5. CA는 인증서를 발급한다.
6. 사용자는 HTS를 통해 거래를 요청하고 거래가 성립되면 주민등록번호만을 이용하여 인증서 상태 검증을 요청한다.
7. CA는 요청받은 사용자의 주민등록번호와 매칭되는 인증서 일련번호를 자신에 데이터베이스에서 찾아 해당 인증서 상태의 대해 유효성 여부를 검사한다.
8. 인증서 상태 유효성 여부를 사용자에게 전송한다.

본 논문에서는 서명자가 인증서 발급을 요청하고 이에 따른 결과로 인증서가 CA로부터 발급되었을 때 서명자정보 즉 주민등록번호와 인증서 일련번호가 인증기관 데이터베이스에 매칭되어 저장된다는 점에 기인하여 전자서명을 요청하는 서명자의 정보만을 이용하여 인증서의 대한 상태 검증을 수행함으로써 인증서 상태 검증속도를 향상 시킬 수 있는 방안을 제안한다. 제안하는 시스템은 [그림 5]에서 보여주고 있다.

4. 결 론

본 논문에서 제안하는 시스템인 서명자 정보를 이용한 인증서 상태 검증 시스템은 인증서 상태 검증을 요청하고 요청한 작업을 처리하는데 있어 해당 인증서에 대한 모든 정보를 보내야만 하는 기존의 상태 검증 시스템과 달리 서명자에 주민등록번호만을 이용하여 인증서 상태 검증을 요청함으로써 네트워크에 부하를 감소시킬 수 있다. 또한 인증서 상태 검증 과정에서 서명자의 최소한의 정보만을 이용하여 검증을 수행하기 때문에 인증서 상태 검증 시간을 향상시킬 수 있다.

본 논문에서는 기존 인증서 상태 검증 시스템의 문제점인 네트워크 과부하 문제 및 인증서 상태 검증 시간의 향상을 위해 인증서 상태 검증을 요청하는 서명자 정보만을 이용한 인증서 상태 검증 시스템을 제안하였다. 향후 본 연구 결과를 토대로 실제 응용이 가능하도록 계속적인 연구를 진행해 나갈 것이다.

참 고 문 헌

[1] R. Housley, W. Ford, W. Polk, and D. Solo, RFC2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.

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

[3] 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

[4] A. Malpani, R. Housley, T. Freeman "Simple Certificate Validation Protocol" draft-ietf-pkix-scvp-10.txt, Nov 2002.

[5] 장기식 "보안을 위한 효율적인 방법 PKI" 인포북. 2003