검증 요청자 신원 정보를 이용한 인증서 상태 확인 메커니즘의 설계

김현철*, 이준환*, 한명묵*, 오해석*
*경원대학교 전자계산학과
e-mail: dmzpolice78@korea.com

Design of Certificate Status Checking Mechanism Using Verification Requester Identity Information

Hyun-Chul Kim*, Jun-Hwan Lee*, Myung-Mook Han*,
Hae-Seok Oh*
*Dept of Computer Science, Kyungwon University

요 약

인증서 상태 확인은 해당 거래에 사용되는 인증서에 대해 유효한 인증서임을 판별하기 위한 과정으로 인증서 표준이 제정된 이후로 계속적으로 연구되고 있는 분야이다. 현재 가장 보편적으로 이용되는 인증서 상태 확인 기법은 인증서폐지목록(CRL : Certificate Revocation List)을 이용하는 기법이다. 이 기법은 방법 자체가 가지고 있는 시간격차 문제와 물리적 파일 처리의 과부하로 인하여 사용에 많은 제약이 따른다. 이를 해결하기 위해 온라인 인증서 상태 프로토콜(OCSP : OnLine Certificate Status Protocol) 기법이 제시되었다. 이 기법은 CRL 기법의 비 실시간성 문제를 해결한다. 하지만 서비스 요청 서버의 과부하 문제와 구조적 집중화 문제로 인하여 인증서 상태를 확인 하는데 소요되는 시간이 다소 오래 걸린다는 문제가 있다. 본 논문에서는 검증 요청자의 신원정보에 대한 해쉬값을 이용하여 인증서 상태 확인 요청을 하고 이를 통해 인증서 상태 확인 과정을 진행함으로써 통신 부하를 감소시키고 실시간으로 인증서 상태를 확인 할 수 있는 검증 요청자 신원 정보를 이용한 인증서 상태 확인 메커니즘을 제안한다.

1. 서론

정보화 사회의 급속한 발전으로 인해 과거 오프라인으로 처리되던 많은 일들이 온라인 처리로 빠르게 전환되고 있다. 하지만 온라인통신은 정보노출 및 위변조의 외부 위협요소로부터 항상 노출되어 있다.

이를 위해 거래가 발생 할 때 마다 해당 거래가 유효한 거래인지 아닌지를 판별하는 유효성 검증 과정을 수행하여야 한다. 유효성 검증은 전송되는 메시지에 대해 유효성을 검사하는 전자서명 검증과 인증서의 유효성을 검사하는 인증서 상태 검증으로 구분된다[1].

인증기관으로부터 발급된 인증서는 개인키 분실, 자격상실, 키 변경 등의 여러 가지 이유로 폐지 될 수 있다.

이러한 이유로 해당 거래에 사용되는 인증서에 대해 유효한 인증서임을 판별하기 위한 과정을 거쳐야 하는데 이를 인증서 상태 확인 이라한다. 특히 이 과정은 인증서의 현재 상태와 인증서의 소유자 및 발행자의 신원을 검증하는 과정으로 전자거래에 있어 가장 중요한 부분이다[2].

현재 인증서 상태 확인에 대한 연구는 크게 두 가지로 분류할 수 있다. 첫 째, 인증서 폐지 목록[3]을 이용하는 기법이 있으며, 둘 째, 온라인 인증서 상태 프로토콜[4]을 이용하는 기법이 있다. 하지만, 이 두 가지 인증서 상태 확인 기법 모두 단점을 가지고 있다.

* 본 연구는 경기도의 차세대 성장동력 기술개발 사업에 의한 지원금으로 수행되었음.

우선, 인증서 폐지 목록을 이용하는 기법은 검증자가 해당하는 인증기관에 접속하여 인증서 폐지 목록을 요청하게 되고, 요청한 인증서 폐지 목록을 자신의 단말기에 전송 받아 인증서의 상태를 확인하는 방법이다[5]. 그러나 방법 자체가 가지고 있는 시간 격차(12시간)문제와 물리적 파일 처리의 과부하로 인하여 사용에 많은 제약이 따른다.

온라인 인증서 상태 프로토콜은 OCSP클라이언트와 OCSP서버로 구성되며 클라이언트는 서버에게 특정 인증서의 상태를 요청하거나 그에 대한 인증 경로를 검증하고 획득한 인증 경로의 유효성을 검증하는 기법이다[5-6].

이 기법은 인증서 폐지 목록 기법의 비 실시간성 문제를 해결할 수 있다. 하지만 서비스 요청 서버의 과부하 문제와 구조적 집중화 문제로 인하여 인증서 상태를 검증 하는데 소요되는 시간이 다소 오래 걸린다는 문제가 있다.

국내 공인 인증 시스템 체계에서 사용자는 인증서를 발급받기 위해 신원정보를 인증기관에 제공해야 한다. 또한 대부분의 온라인 서비스는 사용자 가입 과정에서 신원정보를 요구한다.

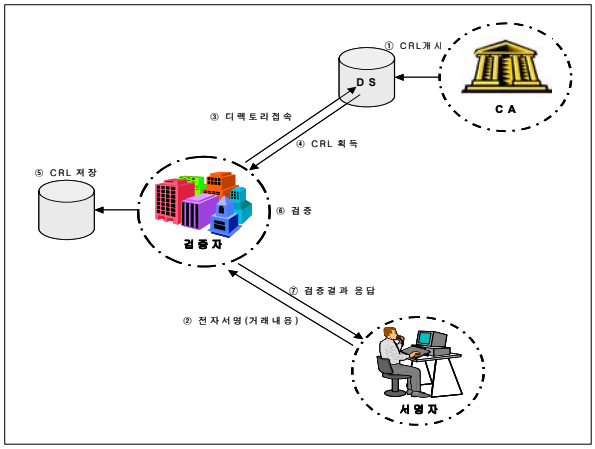
따라서 본 논문에서는 검증 요청자의 신원정보에 대한 해쉬값을 이용하여 인증서 상태 검증을 요청함으로써 통신 부하를 감소시키고 실시간으로 인증서를 검증할 수 있는 검증 요청자 신원 정보를 이용한 인증서 상태 확인 메커니즘을 제안한다.

2. 관련연구

2.1 CRL을 이용한 인증서 상태 검증 기법

CRL은 RFC2459[3]에 정의되어 있다. CRL은 여러 가지 이유로 폐지된 인증서를 모아놓은 목록으로 인증기관이 폐지된 모든 인증서의 일련번호, 폐지시간, 폐지이유를 주기적으로 생성하여 서명한 후 디렉토리에 게시한다. 게시된 CRL을 검증자가 검증시점에 디렉토리로부터 검색하고 다운로드 한 후 인증서 상태 확인시 다운 받은 CRL을 이용하여 인증서 상태 검증을 수행하는 기법이다[5]. 아래 [그림 1]은 CRL을 이용한 인증서 상태 검증 기법의 대한 처리과정을 보여주고 있다.

① CA는 모든 폐지된 인증서의 목록에 전자서명을 하여 디렉토리에 게시한다.
② 서명자는 전자서명된 거래내용을 검증자에게 전송한다.
③ 검증자는 디렉토리에 접속한다.
④ 검증자는 Pull 방식으로 CRL을 획득한다.
⑤ 검증자는 재게시전까지 획득된 CRL을 저장한다.
⑥ 검증자는 해당 인증서가 CRL에 있는지 검증한 후 전자서명에 대해 검증을 한다.
⑦ 검증자는 서명자에게 검증결과를 응답한다.



[그림 1]. CRL을 이용한 인증서 상태 검증 기법

2.2 OCSP를 이용한 인증서 상태 검증 기법

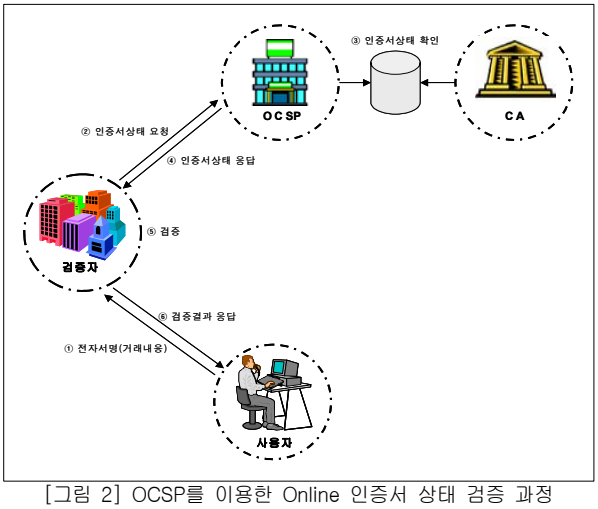
1999년 6월 'X.509 Public Key Infrastructure Online Certificate Status Protocol' OCSP 버전 1.0이 발표되었다. 이 후 2001년 3월 현재 사용되고 있는 OCSPv2가 드래프트 형태로 발표 되었다[7].

OCSP 상태 확인 시스템의 전체 구성은 다수의 클라이언트가 중앙에 위치한 서버를 이용하는 형태로 구성되어 있다. 따라서 서버 부하가 집중되며, 서버 부하가 고도화됨에 따라 처리비용이 지수적으로 증가한다. 또한 각각의 클라이언트에서 검증 요청을 할 때마다 인증서의 모든 정보를 서버로 전송해야 하기 때문에 네트워크 과부하 및 통신 병목현상이 발생할 수 있다. 아래 [그림 2]는 OCSP를 이용한 인증서 상태 확인 기법의 대한 처리과정을 보여주고 있다.

① 서명자는 전자서명된 거래내용을 검증자에게 전송한다.
② 검증자는 OCSP 서버에 인증서상태를 요청한다.
③ OCSP 서버는 CA의 데이터베이스를 검색한다.
④ OCSP 서버는 검증자에게 해당 인증서상태를 응답한다.
⑤ 검증자는 인증서상태 응답을 확인한 후 전자서명

에 대해 검증을 한다.

⑥ 검증자는 서명자에게 검증결과를 응답한다.



[그림 2] OCSP를 이용한 Online 인증서 상태 검증 과정

3. 제안하는 시스템

3.1 제안하는 신원정보 기반의 메커니즘

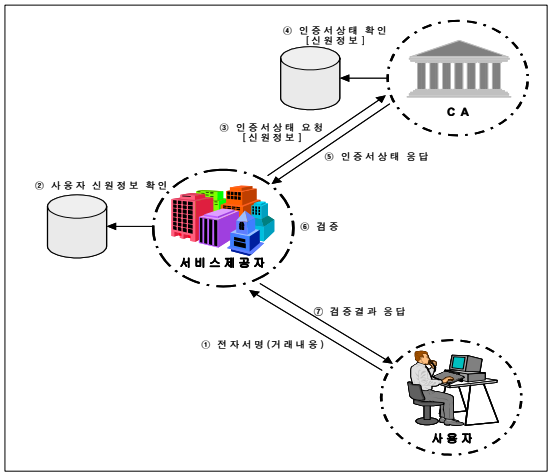
PKI기반에서 사용자는 인증서를 등록하는 할 때 신원정보를 인증기관(CA : Certification Authority)에 전송해야 한다. 국내 공인인증체계에서는 대면 확인을 거쳐 높은 수준의 보안을 유지하고 있다. 각 인증기관은 개인은 주민번호와 법인은 법인번호로써 인증서를 식별하고 있다. 따라서 CA는 사용자에 대한 신원정보와 인증서상태 정보를 보유하고 있다.

인터넷뱅킹, 증권거래시스템, 전자상거래 등의 온라인서비스를 사용하기 위해서 사용자는 가입의 절차를 통해 아이디와 패스워드를 부여받아야 한다. 이러한 가입과정에서 사용자의 신원정보가 서비스제공자에게 제공하도록 되어 있다. 일반적으로 가입과정은 온라인을 통한 확인이 이루어지고 있다. 따라서 서비스제공자 역시 사용자에 대한 신원정보를 보유하고 있다.

온라인서비스 사용자는 특정거래에 대해 전자서명을 수행하여 서비스제공자에게 전송한다. 서비스제공자는 다수의 사용자가 전송한 전자서명을 검증해야 한다. 이때 인증서 상태 확인을 하는 과정에서 CA와 서비스제공자가 보유하고 있는 신원정보를 이용한 방식을 제안한다. 제안하는 방식은 OCSP와 같은 실시간을 보장하고 신원정보의 해쉬값으로 인증서상태 요청을 함으로써 통신부하를 감소시킨다.

3.2 신원정보를 이용한 인증서상태 검증

[그림 3]은 본 논문에서 제안하는 검증 요청자 신원정보를 이용한 인증서상태 검증 과정을 나타낸 것이다. CA는 인증서등록 및 발급 과정에서 신원정보를 보유하고 있다. 또한 서비스제공자 역시 사용자 가입 과정에서 신원정보를 확보하고 있다. 제안하는 인증서 상태 확인 방식은 서비스제공자와 CA가 보유하고 있는 신원정보를 이용하여 인증서 상태 확인을 제공한다.



[그림 3] 검증 요청자 신원정보를 이용한 인증서 상태 검증 과정

① 사용자는 온라인서비스에 접속하여 특정 전자거래에 본인의 개인키로 전자서명을 수행한 후 서비스제공자에게 전송한다.

② 전송된 전자서명의 사용자에 대하여 서비스제공자가 보유한 데이터베이스의 신원을 확인한다.

③ 신원확인을 통해 적법한 사용자 여부를 확인한 후 CA에 신원확인을 전송하여 인증서상태를 요청한다.

④ 서비스제공자가 요청한 신원정보에 대하여 CA가 보유한 데이터베이스에 존재하는지 확인한다.

⑤ CA는 해당 사용자의 인증서상태를 서비스제공자에게 응답한다.

⑥ 서비스제공자는 응답 받은 인증서상태가 유효인지를 확인한 후 전자서명 검증을 수행한다.

⑦ 서비스제공자는 사용자에게 전자서명 검증결과를 응답한다.

4. 성능평과

4.1 실험내용

실험환경은 시스템 하드웨어로 펜티엄 Ⅲ 800MHz, 시스템 메모리 256M SDREM으로, 운영체

제는 WindowXP에서 테스트 하였다. 개발언어는 서버와 클라이언트 모두 MFC로 작성하였다. [그림 4]는 제안하는 검증 요청자 신원정보를 이용한 인증서 상태 확인 시스템의 결과 화면이다.

〔그림 4〕 제안하는 메커니즘 실험 결과

<표 1>은 기존의 인증서상태 검증 프로토콜인 CRL, OCSP와 제안방식을 비교한 실험데이터를 명시하였다. CRL과 OCSP는 국내 공인인증기관의 인증서를 사용하였다. CRL의 실험은 검증자가 최초에 갱신된 CRL을 디렉토리에서 획득하는 과정과 획득한 이후 로컬에서 확인하는 과정으로 나누어서 실험하였다. 실험결과에서는 CRL의 경우 디렉토리에서 획득하고 확인할 때 부담이 있지만 획득한 이후에는 효율적인 것으로 나타내었다. 그러나 실시간이 보장이 되지 않는다. OCSP는 요청자가 OCSP Request에 전자서명을 하였기 때문에 데이터크기가 증가하고 수행시간 역시 부담이 있는 것을 보인다. 제안하는 메커니즘은 OCSP와 동일하게 실시간을 보장하면서 전송량과 수행시간을 감소시키는 결과를 나타내었다.

<표 1> 인증서 상태 검증 실험 결과

분류	전송량	수행시간
CRL DS 참조	3758 byte	491 ms
CRL Local 참조	0 byte	40 ms
OCSP	1948 byte	350 ms
신원확인 응용	350 byte	128 ms

5. 결 론

기존의 CRL 기법은 기법 자체가 가지고 있는 시간격차(12시간)문제와 물리적 파일 처리의 과부하로 인하여 사용에 많은 제약이 따른다. 이를 해결하기 위한 대안으로 OCSP 기반의 인증서 상태 확인 기법이 제시되었다. 그러나 OCSP 기반의 인증서 상태 확인 기법은 구조적인 집중화 문제와 불필요한 정보 전송 등으로 인한 네트워크 과부하 및 병목현상이 발생한다. 그 결과로 인증서 상태 확인 수행시간이 오래 걸린다는 문제점이 있다. 따라서 기존의 OCSP 기반의 인증서 상태 확인 기법은 은행, 증권 등과 같이 주로 실시간 응답시간을 중요시 하는 분야에 사용하는 것은 유효하지 않다. 본 논문에서 제안하는 검증 요청자 신원정보를 이용한 인증서 상태 확인 메커니즘은 검증 요청자의 신원정보에 대한 해쉬값을 이용하여 인증서 상태 확인 요청을 하고 이를 통해 인증서 상태 확인 과정을 진행함으로써 통신 부하를 감소시키고 실시간으로 인증서를 검증할 수 있다. 따라서 시간적 특성이 중요시 되는 증권거래, 전자입찰의 금융거래등과 같은 시스템의 효율적이라 할 수 있다. 향후 본 연구를 토대로 실제 거래환경에 적용할 수 있도록 계속적인 연구를 진행하고자 한다.

참고문헌

[1] 정재동, “CSMP 기반의 실시간 인증서 상태검증의 성능개선”, 숭실대학교 박사학위 논문, pp 30-55, 2003

[2] Ray Hunt, "PKI and Digital Certification Infrastructure" Proceeding of the 9th IEEE International Conference on Networks, 2001

[3] R. Housley, W. Polk, D. Solo, " Internet X.509 Public Key Infrastructure Certificate and CRL Profile," IETF RFC 2459, January, 1999.

[4] M. Myers, "X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol-OCSP," IETF RFC 2560, June, 1999.

[5] RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile,“ 2002.

[6] 고 훈, 장의진, 신용태, “PKI 환경의 OCSP 서버 부하 감소를 위한 OCSP 분산 기법,” 정보보호학회 논문지, 제13권, 6호, pp. 97-106, 2003. 12.

[7] 곽진, 이승우, 조석향, 원동호, “온라인 인증서 상태 검증 프로토콜(OCSP)의 최근 연구 동향에 관한 분석,” 정보보호학회 학회지, pp. 50-61, 2002