제21회 한국정보처리학회 춘계학술발표대회 논문집 제11권 제1호 (2004. 5)

분산 OCSP 에서 효율적인 인증서 상태 검증 기법에 대한 연구

홍성옥, 김경자, 장태무
동국대학교 컴퓨터 공학과
e-mail : suemhong@dgu.edu

A Study on Efficient Certificate Status Validation Scheme in Distributed OCSP

Sung-Ock Hong, Kyoung-Ja Kim , Tae-Mu Chang
Dept. of Computer Engineering, Dongguk Univ.

요 약

PKI(Public key Infrastructure)기반에서 CA(Certificate Authority)는 사용자를 인증하기 위해서 인증서를 생성하고, 인증서의 상태를 검증하기위해서 CRL(Certificate Revocation List)를 발행하여 인증서 취소 상태를 확인하도록 한다. CRL 을 사용할 경우 사용자의 증가로 인하여 CRL 의 크기가 증가 함으로써 많은 부담과 실시간 처리가 어렵다. 이와 같은 단점을 보안하기 위해서 최근에는 실시간 처리가 가능한 OCSP(Online Certificate Status Protocol)방법이 제안되었지만 이 또한 사용자의 급증으로 하나의 OCSP 서버에 집중화 됨으로써 OCSP 서버의 부하가 많이 생긴다.

본 논문에서는 집중 OCSP 서버에서 생기는 부하를 줄이기 위해 여러 개의 OCSP 서버를 두고, 각 OCSP 서버의 응답 처리 시간을 빠르게 하기 위해서 CA 가 실시간으로 인증서 취소 정보를 해당 OCSP 서버에게 분배하여 전달하고 Front Server 를 둠으로써 각 OCSP 의 Load 를 모니터링하여 부하가 적게 걸린 OCSP 에게 인증서 상태 검증을 함으로써 신뢰성과 각 OCSP 서버의 부하를 줄이는 방안을 제시한다.

1. 서 론

현재 정보통신기술의 발전으로 일상생활의 서비스가 온라인으로 전환 되고 있다. 인터넷이 발달됨에 따라 온라인상에 노출되는 정보들에 대한 불법적인 위.변조 및 신분 위장 등 각종 위협이 예상되고 있다. 그러므로 인터넷상에서 사용자와 정보 제공자 간의 정보보호를 위해 상호간의 인증(Authentication)이 중요한 문제가 되었다.

정보 유통 시 안전성과 신뢰성 확보를 위해 각종 분야에 공개키 암호 기술을 적용한 인증서(Certificate)기반의 PKI 가 현재 가장 널리 사용되고 있는 방법이다. PKI 에서는 사용자의 신상정보와 공개키를 확인할 수 있도록 인증기관으로부터 인증서를 발급받는다.

PKI 시스템은 사용자, 인증기관(CA), 등록기관(RA), 디렉토리 서버(Directory Server)로 구성되며[1], CA 가 공개키에 대한 인증서를 서명하여 발급하는데, 이 인증서는 유효기간 동안에만 사용할 수 있다. 그러나 유효기간 만료, 사용자의 허위 사실 기재, 사용자 요청등과 같은 이유로 인증서를 사용할 수 없는 경우가 발생한다. 이런 경우에 인증서 취소가 반드시 필요하다.

CA 는 취소된 인증서를 관리하는 인증서 취소 목록(CRL: Certificate Revocation List)[1]을 일정한 주기로 발생한다. CRL 은 CA 와 디렉토리 서버에서 취소된 인증서를 확인하는 목록이다. 취소된 인증서의 수정과 확장한 인증서 취소 목록들을 CRL 의 인증서 일련번호로서 확인한다.

그러나 사용자의 증가로 인하여 CRL 의 크기 증가와 실시간 처리가 되지 않아서 그에 대한 방안으로 OCSP 를 제시했다. 이 방안은 인증기관과 디렉토리와는 별도로 서버를 두고 이 서버에서 사용자의 검증 요구에 대한 검색 결과를 제공해 주는 방식이다.

하지만 사용자의 증가와 인증서 상태 검증 요청이 집중될 경우 하나의 OCSP 에 생기는 부하가 너무 많아지게 되었다.[6][7] 따라서 본 논문에서는 집중 OCSP 서버에 생기는 부하를 줄이기 위해 여러 개의 OCSP 서버를 두고, 각 OCSP 서버의 응답시간을 빠르게 하기 위해서 CA 가 실시간으로 인증서 취소 정보를 해당 OCSP 서버에게 분배하여 관리함으로써 각 OCSP 서버의 부하를 줄이는 방안을 제시한다 2 장에서는 연구 배경과 OCSP 서버의 구성에 대하여 알아보고, 3 장에서는 제안된 OCSP 구조에 대하여 알아보고 4 장에서는 설계에 따른 분석 및 결과를 설명한다. 5 장에서는 결론을 맺는다.

2. 연구배경

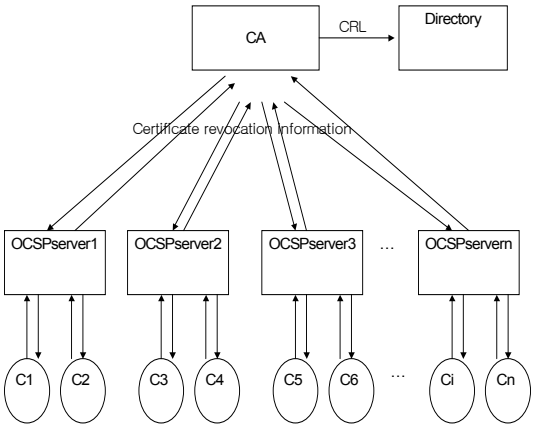
인터넷과 전자상거래의 확산으로 신뢰할 수 있는 네트워크 환경을 제공하기 위해 PKI 의 사용이 널리 활용되고 있다. 특히 거래 당사자간의 신뢰가 더욱 요구되는 인터넷상의 전자 상거래와 금융서비스, 증권 거래등에서는 PKI 가 필수 요소로 인식하고 있다. 이러한 공개키 기반 구조의 기술은 ITU-T 의 X.509 인증서 표준을 근간으로 하며 IETF 에서는 이를 바탕으로 인터넷에 적합한 인증서 표준[1]을 제정하고 있다.

PKI 에서 상대방의 공개키를 사용하기 위해 인증서를 사용하고자 하는 사용자는 인증서를 사용하기 전에 반드시 인증서의 유효성을 확인하는 인증서 상태 검증 과정을 수행하여야 한다.

인증서의 상태 검증 과정이란 인증서와 인증 경로상의 인증서들이 사용하고자 하는 시점에서 그 효력이 정지되었거나 취소되었는지를 검사하는 것을 말하며,[1] 이러한 인증서 상태 검증 과정에서 사용하고자 하는 인증서의 취소 여부의 확인은 매우 중요하다.

인증서의 상태를 검증하기 위한 방법으로는 현재 가장 널리 사용되고 있는 CRL 방식으로 CA 가 일정 주기로 발행한다. 그러나 사용자의 증가로 인증 취소가 많아 질 경우 인증서 취소 목록이 커져서 CRL 를 다운하는 시간이나 인증서 상태 검증 시간이 오래 걸리는 단점이 생기게 되었다. 이와 같은 단점을 극복하기 위해서 부분적인 인증서 취소 목록을 나타내기 위한 방법이 제시되었다. 그 방법으로 CRL 분배점(CRL distribution point)과 델타 CRL 가 제시되었으며, 이들 두 가지 해결책들은 각각 다른 방식으로 이러한 문제점을 해결한다. CRL 을 여러 개의 부분으로 분리하는 데 사용하는 방법이 CRL 분배점이다. 또한 최근에 갱신된 CRL 내용만을 받아 자신이 관리하는 내용에 추가 할 수 있기를 원할 수 있으며, 이 때 사용될 수 있는 방법이 delta CRL 이다.

그러나 이러한 방법들은 실시간으로 인증서의 상태를 검증하지 못 한다는 단점을 가지고 있다. 그러므로 인증서 상태 검증만을 수행하는 독립적인 서버에 관한 연구가 진행되었으며 이러한 연구에는 온라인상에서 실시간으로 인증서의 취소 여부를 확인해 주는 OCSP 가[2][3] 제시되었다. 또한 취소 여부만이 아닌 전체 인증서 검증을 대행해 주는 간단한 SCVP(Simple Certificate Validation Protocol)도[4]나왔으며, 공개키 인증서의 검증과 데이터의 소유 증명 등을 서비스 하여 부인방지 서비스를 제공하는 데이터 검증 및 인증 서버(DVCS : Data Validation and Certification Server)[5]도 제안 되고 있다. 위의 방법 중 OCSP 서버에 많은 사용자가 요청을 할 때 OCSP 서버의 부하가 많아지게 된다. 그러므로 여러 개의 OCSP 서버가 요구되어진다.[6]



[그림 1] 분산 OCSP 구조

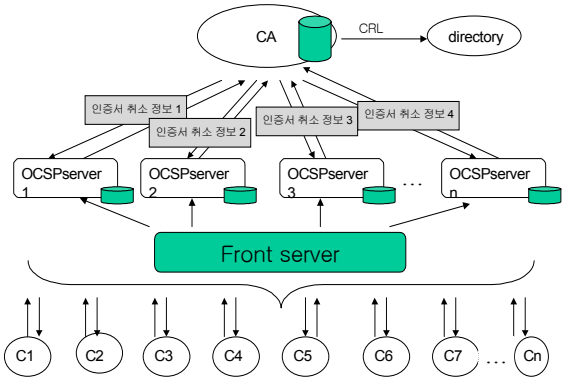
3. 제안된 방법

모든 클라이언트들이 OCSP 서버 한 곳에 서비스를 요청한다면 OCSP 에 대한 부담이 커지게 되며 게다가 최근에는 전자상거래를 이용하는 사용자가 급격히 증가하고 있는 상태에서 OCSP 에게 서비스를 요청하는 일이 많이 발생한다. 그러므로 OCSP 서버를 여러 개 두어 부하를 분산시킬 분산 OCSP 의 필요성이 강조 되었다.[6][7] 그림 1 에서 보여주듯이 분산된 OCSP 서버는 인증기관에서 관리를 하게 되고, CA 는 인증서 취소 정보를 실시간으로 각 OCSP 에 전달하고 또한 CRL 목록을 생성하여 주기적으로 디렉토리에게 전달한다. 그러나 분산 OCSP 에서 각 OCSP 는 동일한 인증서 취소 정보를 CA 에게 받고 있으므로 인증서 취소 정보의 중복성이 존재한다. 이와 같은 모델은 안전성을 유지하는 데는 유리하나 사용자의 급증으로 당연히 CRL 의 크기가 증가되면 각 OCSP 가 인증서 상태를 검증하는 시간이 지연됨과 동시에 CA 에서 인증서 취소 정보를 전달하는 데 네트워크의 지연이 생긴다. 그러므로 OCSP 를 분산시킨 환경에서 각 OCSP 에 인증서 취소 정보를 모두 중복 시키지 않고 분배 시킴으로써 OCSP 와 클라이언트와의 응답시간, 지연시간, Network load 를 줄일 수 있는 효과를 가져올 수 있는 방안을 새롭

게 제안한다.

3.1 제안된 모델 구조

제안된 모델은 분산 OCSP 에서 올 수 있는 문제점을 해결하기 위해 CA 가 가지고 있는 전체 인증서 취소 정보를 각 OCSP 에게 분배하여 전달하면 각 OCSP 의 부하가 줄어든다는 관점에 초점을 맞추었다. 이 환경에서 고려되어야 할 일반적인 사항으로는 여러 개의 OCSP 서버와 많은 사용자의 요구에 서비스를 제공해야 하는 클라이언트들이 여러 개 존재하는 모델이다. 사용자는 인증서를 CA 에게 발급받을 때 사용자 인증서에는 사용자의 인증 취소 목록을 가지고 있는 OCSP 서버의 주소를 알려주는 필드가 추가함으로써 사용자가 클라이언트에게 서비스를 요청할 때 클라이언트는 Front server 에게 사용자 인증서를 넘겨주면 Front server 는 해당 OCSP 에게 인증서 상태 검증을 요청하고 만약 해당 OCSP 가 부하가 많이 걸려서 실시간의 효과가 없다고 판단되면 부하가 적은 다른 OCSP 서버에게 해당 OCSP 서버에게 넘겨준다. 넘겨 받은 OCSP 서버는 자기가 관리하는 데이터베이스에 인증서에 대한 상태가 없기 때문에 CA 에게 요청을 하여 현재의 인증서 상태의 결과를 받는다. 그러므로 각 OCSP 서버에는 CA 와 같은 해당 데이터베이스가 있으며 CA 의 실시간으로 인증서 취소 정보를 받아 데이터베이스를 갱신하여 최신 정보를 가지도록 한다. 그림 2 를 참조한다.



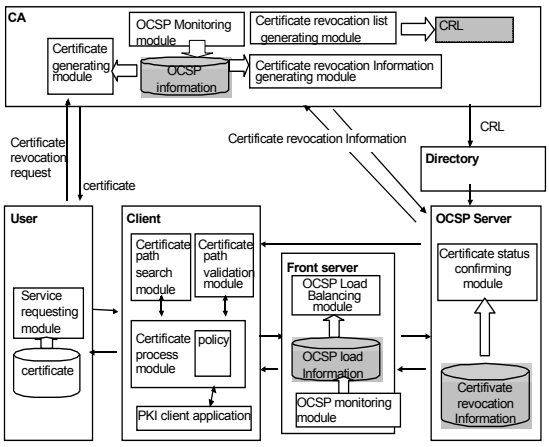
[그림 2] 제안된 모델 구조

3.2 제안된 모델의 처리 방법

분산 OCSP 에서 각 OCSP 의 부하를 줄이고 클라이언트 요청의 응답시간을 단축하기 위해서 제안한 모델의 모듈에는 여러 가지 모듈이 있다. 인증서 상태 메커니즘은 일단 CA 에서는 인증서 생성 모듈과 인증서 취소 목록 생성 모듈이 있다. 사용자의 인증서 생성시 사용자 인증서 항목에 OCSPIPAddress 항목을 추가하며 해당 OCSP 서버의 번호를 나타내는 주소를 적어준 인증서를 발급한다. 사용자는 서비스 요청 모듈을 통하여 클라이언트에게 서비스를 요청하며 자신의 인증서를 클라이언트에게 제출한다. 클라이언트는 사용자의 서비스 요청을 처리하기 위해 일단 사용자의 인증서를 인증서 경로 탐색 모듈, 인증서 경로 검증 모듈을 통하여 검증에 필요한 인증서 및 서명의 유효성 검증, 유효기간 검사, 상위 인증서의 주체 이름과 해당 인증서의 발행자 이름이 일치하는 지와 인증서의 정책 검사와 정책 매핑 검사 및 수행을 하며 인증서 취소 상태를 알기 위하여 OCSP 요청 형식에 맞춰서 요청을 한다. 이에 Front Server 는 OCSPIPAddress 항목을 이용하여 해당하는 OCSP 서버에 이를 보낸다. 이 때 Front Server 는 Load Balancing 모듈을 통하여 각 OCSP 서버들의 상황을 체크하고 해당 OCSP 서버가 부하가 많으면 다른 OCSP 서버들에서 부하가 적은 OCSP 를 찾아 그 OCSP 서버에게 인증서 취소 상태를 요청하며, 이의 요청을 받은 OCSP 서버는 CA 에서 인증서 취소 상태를 요청한다. CA 는 실시간으로 인증서 취소 정보를 각 OCSP 에게 보내주는 모듈이 존재한다. 이와 같은 방법으로 각 OCSP 의 부하를 줄어주며 클라이언트의 요청에 대한 응답시간을 줄일 수 있다.(그림 3 참조)

3.3 제안된 모델에서의 사용자 인증서 형식

제안된 모델에 알맞은 사용자 인증서 형식은 그림 3 와 같다. 일반적인 X.509 인증서 형식에 새로운 항목인 OCSPIpAddress 을 추가하여 클라이언트가 사용자 인증서의 취소 상태를 알고자 할 때 이 항목에 있는 Ip 주소를 이용하여 OCSP 서버에 접속하여 인증서 취소 상태를 알도록 한다. 이때 OCSPIPAddress 는 CA 가 각 OCSP 의 번호를 지정한다.



[그림 3] 제안된 모델의 처리 모듈

4. 제안된 모델에 대한 분석과 비교

이 논문에서 제안된 모델은 하나의 디렉토리에 여러 개의 OCSP 서버를 두는 모델이다. 이와 같은 모델에서 OCSP 서버를 여러 개 두는 것은 사용자의 급증으로 인증서가 증가되며 더불어 사용자의 인증서 취소 요구가 많아 지므로 CRL 크기가 커지게 된다. 분산 OCSP 에서 인증서 취소 정보를 중복시키는 모델은 안전성이 보장되지만 클라이언트가 인증서 상태 검증을 요청했을 때 OCSP 의 부하가 커지므로 클라이언트에 대한 응답시간이 오래 걸리게 된다. 이와 같은 문제점을 해결하기 위해 인증서 취소 정보 트랜잭션을 여러 개로 분배하여 OCSP 서버가 관리해야 하는 정보를 축소 시킴으로써 클라이언트의 인증서 상태 검증 요청에 대한 응답을 빠르게 할 수 있다. 제안된 모델을 중앙 OCSP 즉, 하나의 OCSP 를 두는 경우와 분산 OCSP 로 여러 개의 OCSP 를 두는 경우로 전체 인증서 취소 정보를 모든 OCSP 서버에 중복을 시키는 경우와 비교하여 본다. 각 분석 기준은 OCSP 서버와 클라이언트의 응답시간, 네트워크 부하와 지연시간으로 살펴본다. 그 비교에 대한 결과는 [표 1]와 같다.

[표 1] 제안된 모델의 비교

	Response time	Network load	Delay time
중앙 OCSP	느리다	아주 많다	길다.
분산 OCSP	느리다	적다	짧다
제안 모델	빠르다	적다	짧다

응답시간을 비교하면 중앙 OCSP 가 가장 느리고 분산 OCSP 의 인증서 취소 정보분배가 가장 빠르다. 또한 네트워크 부하는 중앙 OCSP 가 가장 많고 분산 OCSP 의 중복된 인증서 취소 정보와 분산 OCSP 의 인증서 취소 정보분배의 부하는 적다. 분산 OCSP 의 중복된 인증서 취소 정보에서의 지연시간은 전체 인증서 취소 정보를 읽어야 할 만큼의 시간이 걸리며, 분산 OCSP 의 인증서 취소 정보 분배의 지연시간은 분배된 인증서 취소 정보를 읽을 만큼의 시간이 걸리므로 분산 OCSP 의 인증서 취소 정보분배가 지연시간이 적게 걸린다는 것을 알 수가 있다.

또한 Front Server 를 둠으로써 각 OCSP 의 부하 분산으로 응답 처리 시간과 네트워크 트래픽을 감소 시킬 수 있다. 하지만 제안된 모델에서의 단점으로는 CA 의 부하 부담과 Front Server 의 비용 증가와 병목 현상이 있을 수 있다.

5. 결론

인증서 취소 목록을 통하여 검증을 할 경우 사용자의 증가와 CRL 의 크기 증가로 인하여 많은 부담으로 실시간 처리가 어려웠다. OCSP 을 분산시킨 환경에서 각 OCSP 에 인증서 취소 정보를 모두 중복시키지 않고 분배 시킴으로써 CA 의 네트워크 트래픽 감소와 OCSP 와 클라이언트사이의 응답 처리 시간, 지연시간, Network load 를 줄일 수 있는 효과를 가져온다. 또한 Front Server 로 부하 분산을 하여 효율성을 높이는 방안을 새롭게 제안했다. 향후 연구과제는 이 모델에서 각 OCSP 에 인증서 취소 정보를 중복시킨 모델과 각 OCSP 의 응답 처리 시간과 네트워크 부하와 지연 시간에 대한 분석에 대해 좀 더 연구가 필요하다.

참고문헌

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

[2] M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, “ X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”, IETF RFC 2560, June, 1999.

[3] M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, “ X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”, IETF draft-ietf-pkix-rfc2560bis-01.txt, February, 2002.

[4] Ambarish Malpani, Russ Housley and Trevor Freeman, “Simple Certificate Validation Protocol(SCVP)”, IETF draft-ietf-pkix-scvp-07.txt, February, 2002.

[5] C. Adams, P.Sylvester, M. Zolotarev and R. Zuccherato, “ Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols”, IETF RFC 3029, February, 2001.

[6]고훈, 장의진, 신용태, “ 분산 OCSP 서버로의 안전한 정보 전달 설계 “, 한국 정보과학회 2003 추계학술논문지

[7] Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum, “A Certificate Revocation Scheme for a Large-Scale Highly Replicated Distributed System”, IEEE, 2003.