응답시간 감소를 위한 분산 OCSP 인증서 검증 모델

Distributed OCSP Certificate Verification Model for decrease in Response Time

공문식, 조용환*
충북대학교*

Kong mun-sik, Cho yong-hwan*
Chungbuk National Univ*

요약

무선 PKI에서 즉시 인증서의 검증이 가능하도록 하는 OCSP기법은 인증서 폐지·효력 정지 상태 파악을 실시간으로 정확하게 할 수 있다는 특성이 있다. 그러나 많은 클라이언트들이 OCSP서버에 인증에 대한 서비스를 요청할 경우 OCSP서버의 부하는 증가하게 되고, 많은 갱신정보들이 집중화될 때도 OCSP서버는 많은 부하를 갖게 된다. 이에 분산 OCSP서버 기법을 무선 PKI에 적용함으로서 빠른 인증서 검증과 OCSP서버로의 트래픽 집중을 막고, 중앙 집중적인 구조의 많은 제약들을 분산된 OCSP 서버로 해결하고자 한다.

Abstract

OCSP has specific characters which can suspend, close, and correct in real time. But, as more clients use the OCSP server verification, more updated information is needed, which can lead to jamming in the OCSP server. To apply this technique of Distributed OCSP server so as to reduce the certificate verification OCSP from jamming. Also, the Distributed OCSP server will solve the problems of the intensive central structure.

I. 서 론

PKI[2] 구축을 위하여 사용되는 기술 중 인증서의 검증 기법은 실제 전자거래에 있어 그 거래의 유효성에 관한 것이므로 가장 신중하게 처리되어야 한다. 이를 위하여 X.509 에서는 효력정지 및 폐지목록(CRL : Certificate Revocation List) 및 CRL 분배점을 사용하는 것을 제시하고 있다[1].

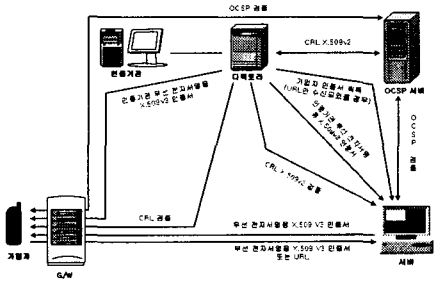
그리고 IETF(Internet Engineering Task Force)는 온라인 상에서 즉시 인증서의 검증이 가능하도록 OCSP와 SCVP를 제안하였다. 이 두 가지 방식 모두 중앙 집중적인 서버를 이용한다. OCSP는 인증서 폐지·효력 정지 상태 파악을 실시간으로 정확하게 할 수 있다는 특성이 있다. 그러나 많은 클라이언트들이 OCSP서버에 인증에 대한 서비스를 요청할 경우 OCSP서버의 부하는 증가하게 되고, 많은 갱신정보들이 집중화될 때도 OCSP서버는 많은 부하를 갖게 된다.

이에 본 논문에서는 무선 PKI에 적합한 인증서 검증 기법에 대해서 고찰하고 분산 OCSP 기법에서의 CRL 정보획득 방법과 OCSP 인증서 검증 요청 및 응답에 대해 알아본다. 그리고 분산된 OCSP서버의 대수에 따라 변하는 서버의 부하율과 인증서 상태 검증 요청에 대한 응답 시간의 변화에 대해 알아본다.

Ⅱ. 무선 PKI에서의 인증서 검증 기법

1. 무선 PKI 구성요소

무선 PKI를 구성하는 요소로는 인증서를 발행하고 효력정지 및 폐지 기능을 수행하는 인증기관, 인증서 등록 및 사용자 신원 확인을 대행하는 등록기관, 인증서 및 인증서 폐지목록을 저장하는 디렉토리, 그리고 인증서를 신청하고 인증서를 사용하는 사용자로 분류될 수 있으며 그림 1은 무선 PKI 구성도를 보여주고 있으며 구성요소들의 각각의 특징은 다음과 같다.



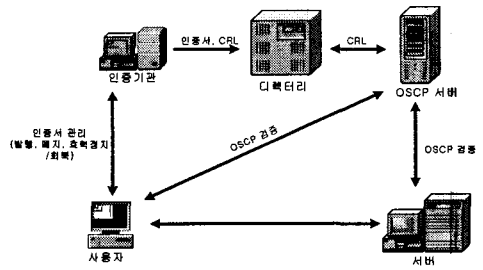
▶▶ 그림 1. 무선 PKI 구성도

- 인증기관(CA : Certification Authority)[2-5]
- 등록기관(RA : Registration Authoryity)
- 디렉토리(Directory)[3,5].
- 사용자(End Entity)
- 인증서(Certificate)
- 인증서 폐지목록(Certificate Revocation List)[6]

2. OCSP를 이용한 인증서 검증 기법

주기적으로 CRL을 체크하는 것을 보완함으로써 인증서의 폐지상태에 관하여 적시의 정보를 얻어내는 요구가 점차 증가하고 있다. 예를 들면, 높은 가치의 자금거래나 금융거래에서는 실시간으로 인증서 폐기상태 정보를 검증해 볼 수 있어야 한다. 따라서 OCSP는 가능한 한 CRL보다 적시의 폐기 정보를 제공할 수 있도록 한다.

기본적인 OCSP 인증 구조는 그림 2와 같이 서버·클라이언트 구조로 구성되며, OCSP 클라이언트는 OCSP 응답자에게 인증서에 대한 상태요구를 한다.



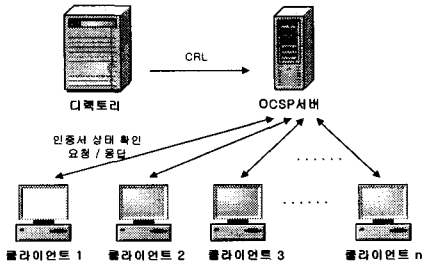
▶▶ 그림 2. OCSP를 이용한 인증서 검증 모델

OCSP(PKIX Online Certificate Status Protocol)는 응용 프로그램이 검증하고자 하는 하나 또는 그 이상의 인증서의 상태를 조회할 수 있도록 한다. CRL보다 인증서의 상태 정보를 보다 실시간으로 얻을 수 있다. IETF의 RFC 2560은 인증서 상태를 체크하는 응용 프로그램과 상태 정보를 제공하는 서버 상에서 오가는 데이터의 구조를 정의하였다[7].

Ⅲ. 분산 OCSP 모델

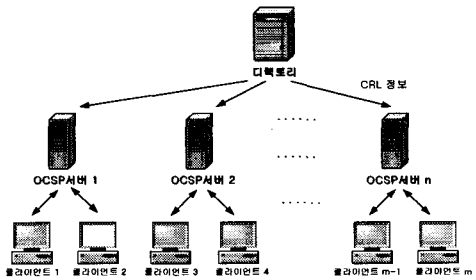
1. 분산 OCSP서버

OCSP서버에 한꺼번에 많은 OCSP클라이언트들이 OCSP서버에 부담을 줄만큼의 많은 량의 인증서 검증을 요청한다면 OCSP서버는 엄청난 트래픽 부하를 가지게 될 것이다. 이는 OCSP서버의 트래픽 증가로 인한 인증서 상태 확인 요청 및 응답시간의 지연을 초래한다.



▶▶ 그림 3. OCSP서버 집중화 현상

이에 하나의 중앙 집중적인 OCSP서버의 부담을 줄이고, 동시에 인증서 상태 확인 요청이 쇄도할 경우 효과적으로 대처하기 위해 분산 OCSP서버 기법을 사용하고자 한다. 이 분산 OCSP서버는 CA에서 관리를 하게 되고, 각 OCSP서버에 전달되어지는 CRL정보는 동일한 디렉토리서버를 이용하여 각각의 OCSP서버에 있는 CRL정보가 하나의 정보를 항상 유지할 수 있도록 해야 한다. 즉 각각의 OCSP서버의 CRL정보는 모두 같아야 한다.



▶▶ 그림 4. 분산 OCSP서버 구성도

그림 4는 분산 OCSP서버에 대해서 설명하고 있다. OCSP서버를 여러 대 설치함으로써 한 대일 때의 OCSP서버의 트래픽 부하를 분산시킨다.

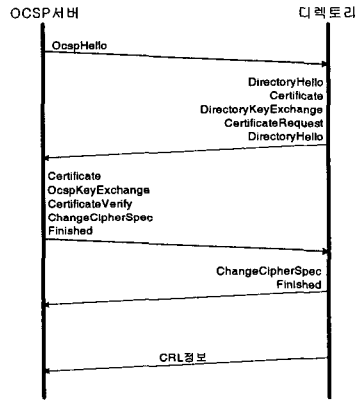
1.1 분산 OCSP 모델 고려사항

분산 OCSP서버를 구축하기 위해서 몇 가지 고려사항이 있다.

- 모든 OCSP서버는 인증서 저장소로부터 사용자의 인증서 검증을 위한 CRL을 일정시간마다 배포 받는다.
- 모든 OCSP서버의 인증서 및 CRL 정보는 같아야 한다.
- 디렉토리에서 각 OCSP서버로 최신 CRL정보를 전달할 때 정보의 보안을 유지해야 한다.
- 디렉토리와 각 OCSP서버 사이에 전달되는 신호는 단순해야 한다.

1.2 분산 OCSP서버의 CRL정보 획득

서버가 공인인증서의 상태를 제공하기 위해서 공인인증서 효력정지 및 폐지정보를 획득·관리하여야 한다. 이를 위해서 OCSP서버는 최신의 공인인증서 효력정지 및 폐지정보를 획득해야 한다. 디렉토리는 각 분산된 OCSP서버들에게 최신의 갱신 정보들을 주기적으로 전송한다. 이때 디렉토리는 OCSP서버에 정보를 전달할 때 정보의 비밀성을 유지하기 위해서 디렉토리와 각 OCSP서버간에 세션키를 이용해서 암호화 한 후에 각 OCSP서버에 전달하게 된다.



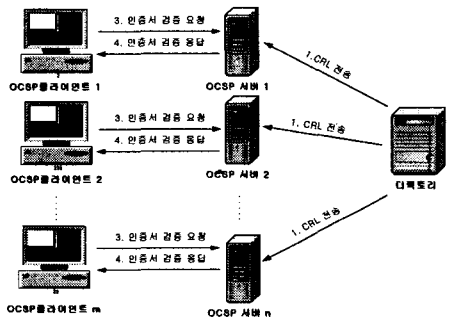
▶▶ 그림 5. Full Handshake

Handshake 과정에서 교환되는 정보는 표 1과 같다.

[표 1] Handshake 과정에서 교환되는 정보

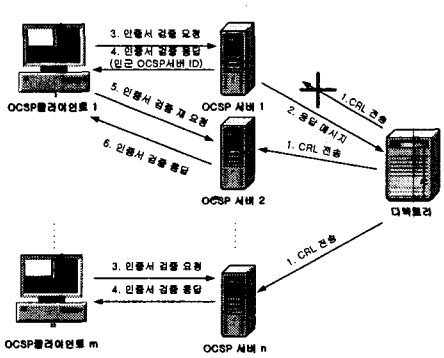
정 보	설 명
Session Identifier	서버가 세션을 식별하는데 사용하는 임의의 수
Protocol Version	프로토콜 버전
Peer Certificate	서버 및 클라이언트 인증서
Compression Method	데이터 암호화에 앞서 사용되는 압축 방법
Cipher Spec	사용되는 관용 암호 알고리즘 및 MAC 알고리즘
Master Secret	클라이언트와 서버에 의해서 공유되는 20바이트의 비밀 정보
Sequence Number Mode	현재 세션에 사용되는 일련번호 사용 방법(off, implicit, explicit)
Key Refresh	보안 서비스 제공에 사용되는 정보(암호키, MAC 정보, IV)등의 교체 주기
Is Resumable	현재 세션이 새로운 세션을 시작하는데 사용될 수 있는지 여부를 나타내는 표시자

디렉토리는 CRL정보를 압축하고 해쉬 및 암호화를 수행하여 전송하고, OCSP서버는 수신한 CRL정보를 복호화 및 검사하는 역할을 한다. 이 때 데이터 압축, 해쉬 계산, 암호화 등에 사용되는 매개변수들은 Handshake 과정에서 결정된다.



▶▶ 그림 6. 분산 OCSP서버 CRL정보 송수신 과정

그림 6은 분산 OCSP서버의 CRL정보 송수신 과정을 나타낸 것이다. 하나의 디렉토리 서버를 이용해서 각각의 OCSP서버는 CRL정보를 수신함으로서 동일한 CRL정보를 유지하게 된다. 일정 시간 간격으로 디렉토리에서 CRL정보를 전송하게 되면 OCSP서버는 CRL정보를 획득하고 관리하게 된다. OCSP서버에서 디렉토리로부터 받은 CRL에 대한 응답 메시지를 보내지 않으므로 OCSP서버의 부담을 약간이나마 줄여줄 수 있다. 즉 디렉토리는 각 OCSP서버가 CRL정보를 잘 받았는지에 대해서는 책임을 지지 않는다.



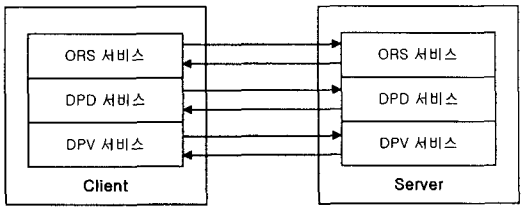
▶▶ 그림 7. 디렉토리로부터 CRL 전송이 없을 때

그림 7과 같이 디렉토리로부터 일정 시간이 지났음에도 CRL 전송이 없을 때에는 OCSP서버가 CRL 요청 메시지를 보낸다. CRL 요청 메시지를 보냈음에도 디렉토리로부터 일정 시간동안 CRL이 전송되지 않을 때는 OCSP서버는 자기 자신을 불능의 상태로 만들고 인근에 있는 다른 분산 OCSP서버의 ID를 OCSP클라이언트에게 보내서 재 인증서 검증을 요청하도록 한다. 이렇게 한 이후에 OCSP서버는 계속하여 디렉토리에 CRL 정보 요청 메시지를 보내서 정상 상태가 되도록 한다.

2. 분산 OCSP 모델의 인증서 검증 서비스

분산 OCSP서버 기법은 IETF PKIXWG에서 2001년 3월 드래프트 형태로 발표한 OCSPv2가 제공하는 서비스를 따르고 있다. OCSPv2는 클라이언트가 온라인 상에서 특정 인증서의 상태를 OCSP서버에게 문의하거나 그에 대한 인증 경로를 획득 가능하게 하고 획득한 인증경로의 유효성에 대해 검증할 수 있는 프로토콜로 제안되었다. OCSPv2가 포함하고 있는 서비스로는 온라인 취소 상태 확인 서비스

(ORS), 대리 인증 경로 검증 서비스(DPV), 대리 인증 경로 발견 서비스(DPD)들이 있다.



▶▶ 그림 8. OCSP 서버·클라이언트 구조

그림 8은 인증서 상태확인 모듈을 OCSP 서버가 대행하는 것을 나타낸다.

Ⅳ. 실험 및 결과분석

본 장에서는 무선 PKI에서의 분산 OCSP 서버 모델에 대해 실험을 통해 본 모델에 대한 실험 결과와 가능성을 알아본다.

1. 실험 환경 및 실험

[표 2] 실험 환경

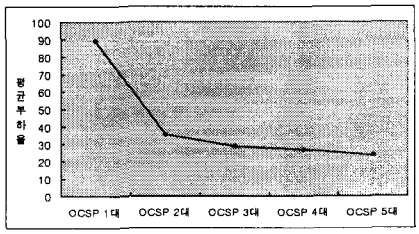
Host (User)	1000대
OCSP 서버	1 ~ 5대
암호화알고리즘	DES
해쉬알고리즘	SHA1
서명알고리즘	ECDSA
무선 대역폭	2Mbps
유선 대역폭	10Mbps
Empty CRL 크기	55kb
인증서 크기	3kb
인증서 갱신 요청시간	30sec
평균서비스 요청시간	10sec

앞서 분산된 OCSP서버들에게 디렉토리의 CRL정보를 안전하게 전달하는 모델을 설명하였다. 분산 OCSP 기법에 대한 실험을 하기 위해 표 2와 같은 실험환경과 조건들을 설정하였다.

네트워크의 기본 환경은 기존의 기본 환경을 그대로 적용하였다[8].

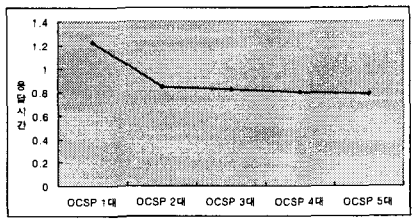
2. 실험 결과 및 분석

그림 9는 OCSP 서버가 클라이언트의 인증서 상태 검증 요청에 대하여 1대일 때와 2대일 때 그 이상일 때 각각의 경우에 OCSP서버 CPU의 평균 부하율을 측정하여 그래프로 나타낸 것이다.



▶▶ 그림 9. OCSP서버 평균 부하율 비교

그림 9는 OCSP 서버의 대수에 따라 인증서 상태 검증 서비스를 요청했을 때 서버의 성능을 나타낸 것이다. OCSP 서버가 한 대일 경우는 많은 부하가 있음을 보여주고 있다. 평균 부하율은 약 89.12%의 높은 부하율을 보이고 있다. 그러나 2대일 경우와 3대일 경우는 각각 35.4%와 28.6%로 나타나고 있다.



▶▶ 그림 10. 인증서 상태 검증 서비스 요청에 대한 응답시간

그림 10은 인증서 상태 검증 서비스 요청에 대한 응답시간을 보여주고 있다. 이 응답시간에 관한 결과 또한 서버를 분산했을 경우에 한 대일 경우보다 빠른

응답시간을 보여준다. 한 대일 때의 응답시간은 평균 1.22초이다. 그러나 2대일 경우와 3대일 경우는 0.845초와 0.824초로 거의 차이를 보이지 않고 있다. 4대일 때와 5대일 때도 비슷한 결과가 나타났다. 1대일 때와 2대일 대를 비교하면 응답시간의 차이가 어느 정도 보여지나 2대 이상에서의 응답시간의 비교는 무의미할 정도로 미미한 차이를 가진다.

V. 결 론

본 논문은 무선 PKI에서 기존의 하나의 OCSP서버에서 인증서 상태 검증 서비스를 할 때 많은 클라이언트들이 OCSP서버에 서비스를 요청할 때의 OCSP서버에 가해지는 부하율의 증가와 응답시간의 지연에 대해서 분석을 하고 이에 대한 해결 방안으로 분산 OCSP서버를 활용하였다. 하나의 OCSP서버가 담당하던 인증서 유효성 검사를 몇 개의 OCSP서버로 분산시키는 방법을 통해서 OCSP서버의 대수가 1대일 때, 2대일 때, 그 이상일 때에 대해서 실험하였다. OCSP서버의 수가 늘어날수록 서버의 부하 감소와 인증서 검증 요청 평균 응답속도의 성능이 향상됨을 증명하였다. 그리고 OCSP서버의 수가 2대일 때 비용효율 면에서 가장 경제적인 것을 알 수 있었다.

▮참고문헌▮

[1] 이석래, "무선보안기술동향", 전자서명인증관리센터, 한국정보보호진흥원, 2002.
[2] "전자상거래를 위한 보안 기술 체계 및 요소기술에 대한 이해", 한국전산원 차세대 서비스부, 1999. 6.
[3] R.L Rivest, A. Shamir and L. Adleman, "A Method for obtaining digital signatures and public-key cryptosystems", ACM, Vol.21. no.2, pp.644-654 Feb. 1978.
[4] ElGamal, T. "A public key Cryptosystem and a signature scheme based on discrete logarithms", IEEE Trands. Infor. Theory, vol. IT-31, pp.469-472, 1985
[5] "Recommendation for a Unique Identifier for X.500 Distinguished Names", 4. March, 1998.
[6] Schneier. B, "Applied Cryptography : Protocols, Algorithms, and Source Code in C", Jone Wiley & Sons, New York, 1996.
[7] 채송화, "CRL 분배 및 온라인 인증서 상태 확인 비교", 전자서명 인증관리 센터, KISA, 1999.