보안성을 고려한 분산된 OCSP 서버 구축 제안

고훈°), 김대원, 장의진, 신용태
대진대학교 컴퓨터공학과, (주) 디지캡스, 숭실대학교 컴퓨터학과
skoh21@daejin.ac.kr neon@digicaps.com shin@comp.ssu.ac.kr

A Proposal of Distributed OCSP Server Construction Considering Security

Hoon Ko°), Daewon Kim, Uijin Jang, Yongtae Shin
Department of Computer Science Daejin Univ. Digicaps Inc,
Department of Computer Science Soongsil Univ.

요 약

공개키 기반 구조는 공개키의 무결성을 제공해 주기 위해서 인증서를 발행한다. 그리고 인증서의 유효성을 체크하기 위해서 인증서 취소 목록(Certificate Revocation List : CRL)을 다운받아서 유효성을 검사하지만 사용자가 증가와 CRL의 크기 증가로 인해서 많은 부담이 된다. 그래서 최근에는 온라인상으로 유효성을 검사하는 OCSP(Online Certificate Status Protocol)이 대안방안으로 발표되었지만 이 또한 하나의 인증서 저장소에 집중화됨으로써 문제가 발생된다. 따라서 OCSP 서버를 분산된 위치에 배치하여 집중화 문제를 방지하고자 한다.

1. 서 론

공개키 기반 구조는 공개키의 무결성을 제공해 주기 위해서 인증서를 발행한다. 그리고 인증서의 유효성을 체크하기 위해서 인증서 취소 목록(Certificate Revocation List : CRL)을 다운받아서 유효성을 검사 하지만 사용자가 증가와 CRL의 크기 증가로 인해서 많은 부담이 된다. 그래서 최근에는 온라인상으로 유효성을 검사하는 OCSP(Online Certificate Status Protocol)이 대안방안으로 발표되었지만 이 또한 하나의 인증서 저장소에 집중화됨으로써 문제가 발생된다. 따라서 OCSP 서버를 분산된 위치에 배치하여 집중화 문제를 예방하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 OCSP 서버에 대해서 설명하고 3장에서는 제안하는 분산된 OCSP 서버의 구성도를 설명하고 4장에서는 모델 분석 5장은 결론을 맺는다.

2. OCSP 서버

OCSP(Online Certificate Status Protocol) 방식은 인증기관과 디렉토리와는 별도로 서버를 두고 이 서버에서 사용자의 검증 요구에 대한 검색 결과를 제공해 주는 방식이다[1].

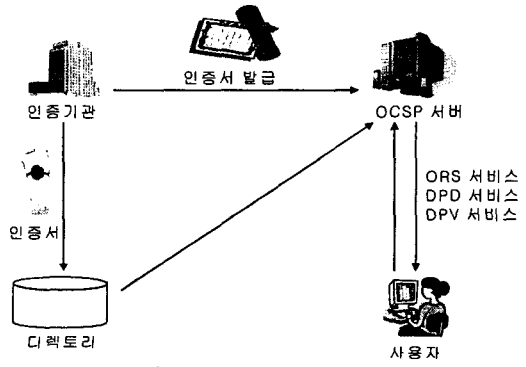

그림 1 : OCSP 구조

OCSP는 클라이언트가 온라인 취소 상태 확인 서비스(ORS), 대리 인증 경로 발견 서비스(DPD), 그리고 대리 인증 경로 검증 서비스(DPV) 등의 3가지의 상태 및 유효성 검증 서비스를 요구하고 서버가 이 요구 메시지에 대한 응답을 하는 프로토콜로서, 현재 IETF에서 제안하고 있는 인터넷 드래프트 OCSPv2에서 구체적인 동작을 정의하고 있지 않다. 단지 서버와 클라이언트 간에 교환되는 메시지의 구성과 형태만을 정의하고 있다[2][3]. 그림 1은 OCSP의 구조를 나타낸 것이다. 인증서는 클라이언트들의 공개키 정보와 이름을 바탕으로 하여 인증기관의 비밀키로 서명을 하게 되고, 이러한 과정을 통해 공개키에 대한 무결성을 제공해 준다. 인증서를 사용하거나 서명문을 검증하고자 하는 클라이언트는 공개키에 대한 인증서의 유효성을 확인한 후 서명문에 대하여 검증을 한다. OCSP는 위임받은 서버에게 인증서 상태확인을 의뢰한다[3][4]. 그림 2에서 보는 것과 같이 클라이언트는 실시간에 가까운 인증서 폐지 상태 정보를 OCSP 서버를 통해서 실시간으로 얻을 수 있다[5]. OCSP의 데이터 구조는 클라이언트가 서버로 보내는 요구 메시지(Request)와 서버에서 클라이언트에게 보내는 응답 메시지(Response)로 구성 된다

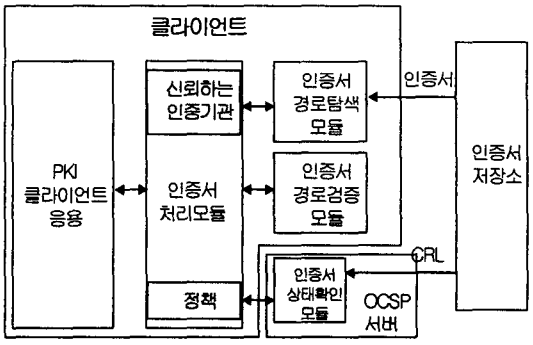

그림 2 : OCSP를 이용한 인증서 검증

1.1. 요구 메시지

요구 메시지(OCSPRequest)는 클라이언트가 서버에게 특정 인증서의 상태 정보를 요구하는 메시지이다. 요구자가 서버에게 이 메시지를 보냈을 경우에는 서버의 응답 메시지(OCSPResponse)를 수신할 때까지 인증서의 유효성에 대한 판단을 보류하여야 한다[1][2].

1.2 응답 메시지

응답 메시지(OCSPResponse)는 클라이언트로부터 요구 메시지를 수신한 OCSP 서버가 요구된 인증서의 상태 검증 결과를 포함한 메시지를 클라이언트에게 전송하는 메시지이다. 응답 메시지도 요구 메시지와 마찬가지로 서명되어 전송되어야 하며 서명문을 생성하기 위해 인증서를 발급한 인증기관의 서명용 키를 이용한다. 클라이언트가 서버로부터 보내온 응답 메시지의 유효성을 검증하기 위해 사용되는 서버의 공개키는 인증서의 형태로 클라이언트에게 전송하게 된다[1][2].

3. 분산 OCSP 구성

그림 3에서 보듯이 모든 클라이언트들이 OCSP 서버 한곳에 서비스를 요청한다면 OCSP 서버는 부담을 가지게 된다.

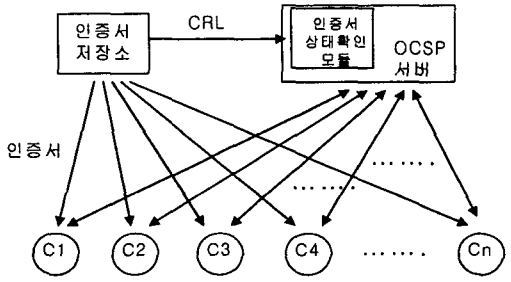

그림 3 : OCSP 서버 집중화 현상

게다가 최근에는 전자상거래를 이용하는 사용자가 급격히 증가하고 있는 상태에서 그림 3과 같은 현상이 발생할 것은 시간문제인 듯싶다. 그래서 아래와 같이 OCSP 서버를 분산시켰다.

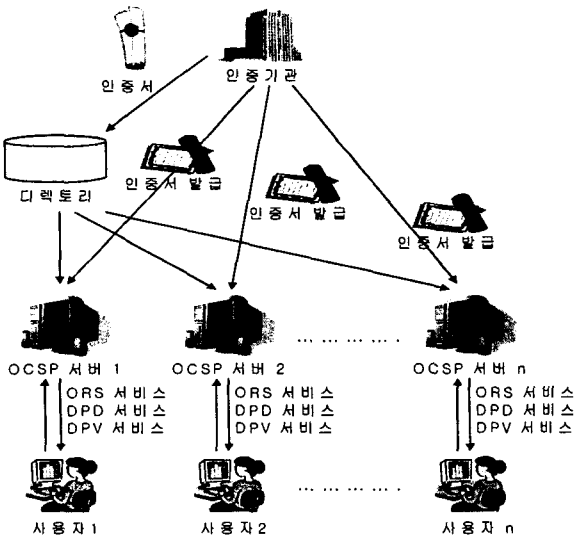

그림 4 : 분산 OCSP 서버모델

제안한 분산된 OCSP 서버는 인증기관에서 관리를 하게 되고, OCSP 서버에 전달되는 CRL 정보는 동일한 저장소를 이용하게 된다. 즉 많은 OCSP 서버가 각 지점에 분산되어 있을지라도 분산되어 있는 OCSP 서버에 CRL 정보를 전달해 주는 인증서 저장소는 같음을 의미한다. OCSP를 분산한 이유는 앞서 설명했듯이 전자상거래를 사용하는 사용자가 계속적으로 증가하고 있기 때문에 사용자 인증 처리는 계속적으로 증가될 것이라고 예측된다. 그러나 이를 위해서 고려되어야 할 사항 두 가지가 있다.

3.1. 분산된 서버 정보의 동시성

분산된 OCSP 서버 모델은 실시간 인증서 상태 검증을 위한 모델이다. 본 모델을 이용할 사용자는 여러 곳에 분산되어 있다. 따라서 각 사용자가 인증서 상태 검증을 요청할 때, 동일한 OCSP 서버에 서비스를 요청하지 않을 것이다. 서로 다른 곳의 OCSP 서버에 같은 인증서의 유효성에 대해서 검증을 요청할 것이다. 이때 서로 다른 OCSP 서버에 서로 다른 정보를 가지고 있으면 문제가 생긴다. 즉, 인증서 저장소에서 많은 OCSP 서버로의 정보 전달시 동시에 정보를 전달하고 수신을 확인해야 한다. 요약하면 서로 다른 OCSP 서버는 서로 같은 인증서 취소 목록을 가지고 있어야 한다.

3.2. 갱신 정보 전달의 안전성

인터넷의 가장 큰 문제점은 정보의 공개 및 프로토콜의 위험성이다. 즉 정보 전달 과정에서 해킹 등의 피해로 인한 정보의 유출이다. 따라서 정보 전달 시에 안전성을 고려해야 한다.

4. 모델 분석

4.1. 분산된 서버 정보의 동시성 해결 방안

분산된 OCSP 서버 구성도에서 정보의 동시성을 해결하기 위한 방안으로 *All or Nothing* 개념을 이용하고자 한다. 즉 OCSP 서버들 중 하나의 서버라도 정보 수신에 에러가 발생되면 다른 OCSP 서버에 전송된 모든 갱신 정보를 취소하는 방안이다. 이렇게 하면 정보의 동시성 문제를 해결할 수 있다.

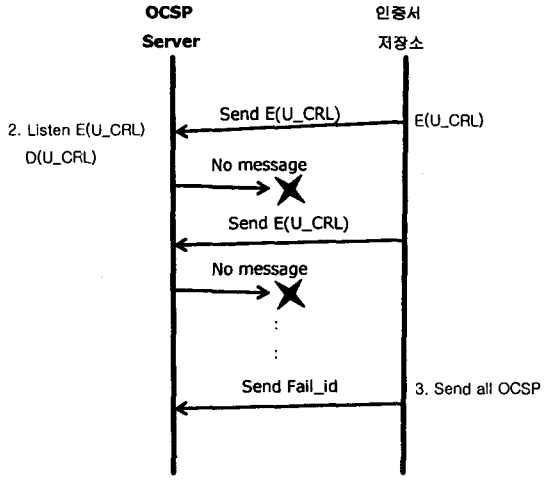

그림 5 : OCSP 서버로부터 응답이 없는 경우

그림 5은 인증서 저장소에서 OCSP 서버r에게 갱신된 인증서 취소 정보를 보냈으나 OCSP 서버의 응답이 없는 경우이다. 인증서 저장소는 일정시간 후에 다시 한번 전송하게 되고, 그래도 응답이 없으면, 인증서 저장소는 모든 OCSP 서버에게 Fail메시지를 보내게 되어 모든 OCSP 서버가 바로 전에 받았던 갱신 정보를 취소하게 된다.

4.2. 갱신정보 전달의 안전성 문제 해결 방안

동시성이 모든 OCSP 서버의 정보에 대한 일치성에 대한 문제라면 안전성 문제는 인증서 저장소에서 OCSP 서버로의 갱신정보 전달 과정에서 유출 및 변경에 위험성 문제이다. 그러나 본 모델을 구축할 때 인증서 저장소와 모든 OCSP 서버들은 각각의 비밀키를 소유하게 된다. 구축하기 전에 한번은 만나야 한다는 단점과 주기적으로 모여서 비밀키를 생신해야 하는 단점은 있지만, 공개키를 이용할 경우 인증서 저장소에서 OCSP 서버의 개수만큼 공개키를 가지고 있어야 하며 느린 암호화 속도 때문에 실시간 서비스를 목표로 하는 OCSP 특성상 맞지 않다.

[단계설명] : 갱신정보 안전한 송수신 과정

[1단계] $E(U\_CRL)$

send $E(U\_CRL)$ to OCSPServer

//인증서 저장소는 갱신된 U_CRL을 암호화 해서 OCSPServer에 전송하게 된다.

[2단계] $D(U\_CRL)$

send *Resp_id* to 인증서저장소

//OCSPServer에서 이를 수신하여 복호화 하게 된다..

[3단계] wait *Response* from *OCSPServer*

//인증서 저장소는 모든 OCSP 서버로부터 수신 응답 메시지가 올 때까지 기다린다.

[4단계] send *Confirm* to *OCSPServer*

//인증서 저장소는 모든 OCSP 서버에게 성공 메시지를 전송한다.

5. 결론

본 논문은 기존의 Root CA에서 처리하던 인증서 검증의 서비스를 분산함으로써 Root CA의 집중화된 처리 부담을 없앴다. 기존의 오프라인 방법의 단점은 시간이 지남에 따라서 크기 증가와 실시간 체크가 어렵다는 것이었다. 이런 단점을 보완하기 위해서 OCSP서버를 두어서 온라인 처리가 제안되었지만, 이 또한 하나의 OCSP 서버로는 증가되는 서비스 요청자의 요구를 처리하기에는 부담이 가중된다. 본 논문은 이러한 부담을 해결하기 위해서 분산된 OCSP 서버를 분산하는 방안을 제안하였다. 차후 본 모델을 활용한 이동 인증 OCSP 서버의 구축 방안도 연구해야 하겠다.

참고문헌

[1] 곽진, 이승우, 조석향, 원동호, "온라인 인증서 상태 검증 프로토콜(OCSP)의 최근 연구 동향에 관한 분석", *한국정보보호학회 학회지*. 제12권, 제2호, pp50-61, 2002

[2] 곽진, 이승우, 조석향, 원동호, "시간 정보를 이용한 인증서 상태 검증 정보 제공에 관한 연구", *한국정보처리학회 춘계학술발표논문집*. 제9권, 제1호, pp833-837, 2002

[3] W.Diffie and M.Hellman, "New Directions In Cryptography", *IEEE Trans on Information Theroy*. vol.IT-22, pp.644-654. Nov, 1976

[4] R.Housley, W.Ford, W.Polk, D. Solo. RFC2459 "Intranet X.509 Public Key Infrastructure Certificate and CRL Profile", Jan.1999

[5] M.Myers, R.Ankney, A.Malpani, S.Galperin, C.Adams, RFC2560 "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP", IETF Standard, June, 1999