분산 OCSP 서버로의 안전한 정보 전달 설계

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

A Design for Secure Information Transmission to Distributed OCSP Server

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

요 약

공개키 기반 구조는 인증서의 유효성을 검증하기 위해서 인증서 취소 목록 검증을 한다. 그러나 시간이 지남에 따라 크기 증가와 오프라인 방식으로 인해서 목록을 다운 받은 시간의 부담으로 인해서 실시간 처리가 어렵다. 이런 문제점을 해결하기 위해서 온라인 서비스가 가능한 OCSP(Online Certificate Status Protocol) 방법이 제안되었지만, 서비스의 요청이 집중될 경우 문제가 발생될 수 있다. 그래서 분산된 OCSP를 구축했다. 본 논문에서는 인증서 저장소에서 분산된 OCSP에게 안전한 정보 전달하는 방안을 설계 하였다.

1. 서 론

공개키 기반 구조는 인증서의 유효성을 검증하기 위해서 인증서 취소 목록 검증을 한다. 그러나 시간이 지남에 따라 크기 증가와 오프라인 방식으로 인해서 목록을 다운 받은 시간의 부담으로 인해서 실시간 처리가 어렵다. 이런 문제점을 해결하기 위해서 온라인 서비스가 가능한 OCSP(Online Certificate Status Protocol) 방법이 제안되었지만, 서비스의 요청이 집중될 경우 문제가 발생될 수 있다. 그래서 분산된 OCSP를 구축했다. 본 논문에서는 인증서 저장소에서 분산된 OCSP에게 안전한 정보 전달하는 방안을 설계 하였다. 논문 구성은 다음과 같다. 2장은 OCSP 서버의 구성, 3장은 제안한 방법의 모델 설계, 4장은 설계에 따른 분석 및 결과를 설명한다. 마지막으로 5장에서는 결론을 맺는다.

2. OCSP 서버 구성

OCSP(Online Certificate Status Protocol) 방식은 인증기관과 디렉토리와는 별도로 서버를 두고 이 서버에서 사용자의 검증 요구에 대한 검색 결과를 제공해 주는 방식이다[1][2].

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[5]

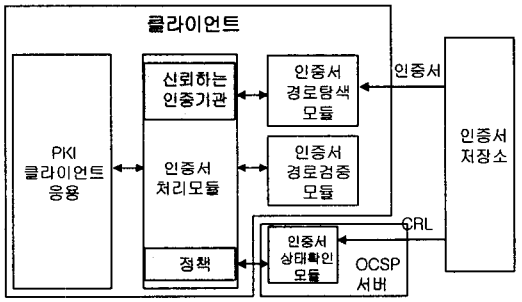

그림 1 : OCSP를 이용한 인증서 검증

3. Secure OCSP 서버 구성

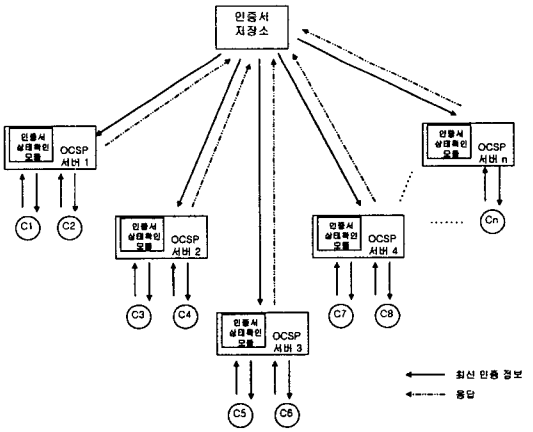

그림 2 : 분산된 OCSP 서버 구성도

본 모델을 구축하기 전에 인증서 저장소와 분산된 OCSP 서버들은 미리 비밀키를 공유해야 한다. 공개키를 이용하는 방안도 있지만, 공개키의 특성인 속도적인 문제점 때문에 실시간 처리를 요하는 본 모델에서는 어울리지 않다.

인증서 저장소는 OCSP 서버에게 비밀키를 이용해서 갱신정보를 암호화해서 전송하게 된다. 이를 수신한 OCSP 서버는 고유한 비밀키를 이용해서 복호화 하게 된다. 중간에 해킹에 의해서 암호화된 정보를 가져가더라도 비밀키를 모르기 때문에 이를 복호화를 한다는 것은 불가능하다.

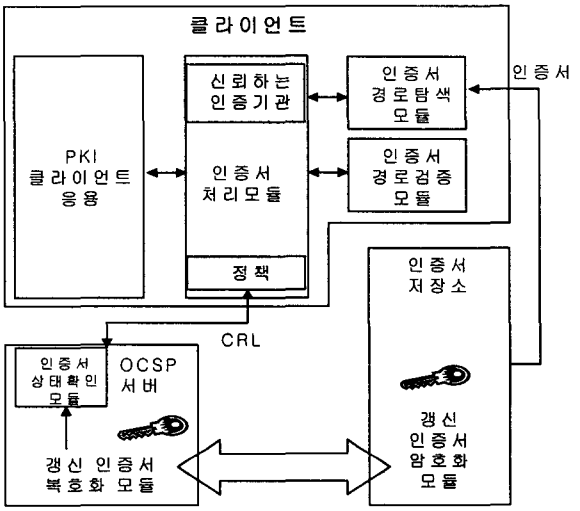

그림 3 : 암호화/복호화 과정

그림 3은 인증서 저장소에서 비밀키를 이용해서 암호화를 한 후 전송하는 과정과 OCSP 서버에서 암호화 된 정보를 수신한 후에 복호화 하는 과정을 보여주고 있다.

4. 설계 및 결과

본 모델을 설계하기 위해서 사용된 메시지들에 대한 정의이다.

[Notation]

- *OCSPServer* : 각 OCSP 서버
- *U_CRL* : 갱신 인증서 취소 목록
- *Resp_id* : 각 OCSP의 응답 메시지
- *Req_id* : 각 OCSP의 요청 메시지
- *Confirm_id* : 성공 메시지
- *Fail_id* : 실패 메시지
- *E(U_CRL)* : CRL 암호화
- *D(U_CRL)* : CRL 복호화

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

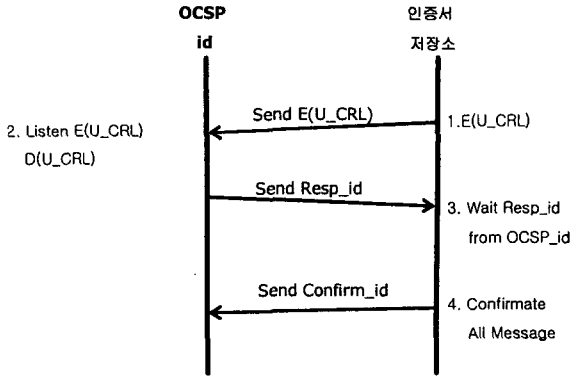

그림 4 : 암복호화 송수신 과정

[1단계] *E(U_CRL)*
send *E(U_CRL)* to OCSPServer
[2단계] *D(U_CRL)*
send *Resp_id* to 인증서저장소
[3단계] wait *Response* from *OCSPServer*
[4단계] send *Confirm* to *OCSPServer*

그림 4는 인증서 저장소에서 암호화 해서 전송하면 OCSP 서버는 이를 복호화 해서 인증서 저장소에 수신 확인 메시지를 보내는 과정이다.

먼저 인증서 저장소가 갱신된 인증서 정보를 암호화 해서 OCSP 서버에 전송한다. OCSP 서버는 이를 수신해서 복호화를 한후에 받았다는 응답 메시지(Resp_id) 메시지를 인증서 저장소에 전송한다. 응답 메시지를 받은 인증서 저장소는 OCSP 서버가 갱신된 인증서 정보를 제대로 수신 한걸로 인식을 하고 확인 메시지(confirm_id)를 보낸다.

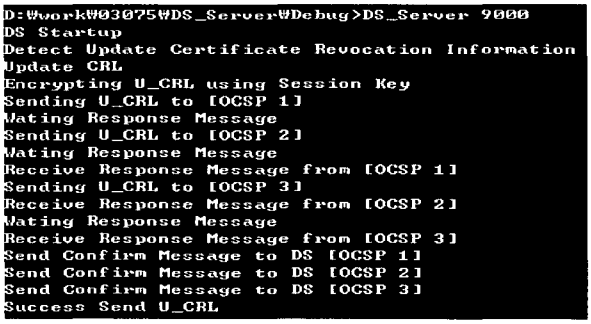

그림 5 인증서 저장소 화면

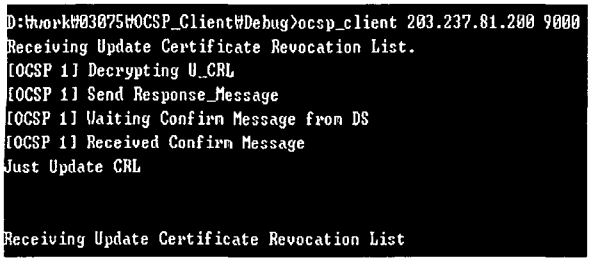

그림 6 OCSP 화면

그림 5는 인증서 저장소에서 특정한 사용자의 CRL 갱신 신호 발견 후, CRL을 갱신 한 다음에 각 *OCSP_id*로 전달되는 과정과, *OCSP_id*로부터 *Resp_id* 수신, 그리고 *Confirm_id* 전송 과정을 보여주고 있다.

그림 6은 *OCSP_id*가 *U_CRL*을 수신한 후에 인증서 저장소로 *Resp_id*를 전송하고, *Confirm_id* 메시지를 수신한 과정을 보여주고 있다.

5. 결론

본 논문에서 제안한 방법은 분산된 OCSP 서버 구조를 기준으로 인증서 저장소에서 OCSP 서버로의 인증서 취소 목록 정보를 안전하게 전송하는 방안을 제안하고 간단한 구현을 해 보았다. 그러나 본 논문에서는 인증서 취소 목록을 하나의 파일로 고려한 상태에서 정보의 안정성에 대해서 중점을 두어 연구를 해 보았다. 물론 정보는 암호화 되어서 전송되었다. 그러나 CRL은 하나가 존재하는 것이 아니라, 인정단위 개수의 인증서에 하나의 CRL을 생성하여 할당시키는 방법을 사용하고 있다. 이것은 KISA의 표준은 없고, 한국전자인증에서는 1000개당 하나의 CRL파일을 할당하고 있다. 결국 1000개 이상이 된다면 하나 이상의 CRL파일이 생성 된다는 의미를 담고 있다. 예를 들어 사용자가 100,000명인 경우 30%가 인증서 취소 요청 및 갱신 요청을 하였을 경우 3000개의 인증서 취소 목록이 발행하고 3개의 CRL파일이 생성된다. 현재 우리나라 인구의 70% 이상이 인터넷을 이용하고 있으면 이중 90%이상이 인터넷을 통해 물품을 구입해본 경험이 있다고 한다. 그리고 이 수치는 계속 증가하고 있다. 수치적으로 3천만명이상이 인터넷을 하고 있으며 2천700백만 이상이 전자상거래를 이용한 경험이 있다. CRL파일이 몇 개가 생길지는 대충 짐작이 가는 대목이다. 10%의 사용자가 인증서 갱신을 요청할 경우 수많은 CRL파일이 생성된다. 결론적으로 암호화 및 네트워크의 보안도 중요하지만 먼저 CRL의 획기적인 구성 방안도 병행해서 연구가 진행되어야 할 듯 하다.

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