情報保護學會論文誌
第14券 第4號, 2004. 8

Observer를 이용한 인증서 검증의 적시성 증대에 관한 연구

권 오 인[a)†], 김 진 철[b)‡], 오 영 환[a)]
광운대학교[a)], 한국전력 KDN[b)]

A Study on Timeliness Advance Increment of Certificate Verification Using an Observer

OhIn Kwon[a)†], JinChul Kim[b)‡], YongHwan Oh[a)]
KwangWoon University[a)], Korea Electric Power Data Network[b)]

요 약

인증서는 유효 기간 동안 사용할 수 있지만, 사용자의 허위 사실 기재, 사용자요청, 개인키 손상 등의 이유로 인증서를 사용할 수 없는 경우 인증기관은 인증서를 취소해야 한다. 인증기관(Certificate Authority)은 인증서 취소목록(CRL : Certificate Revocation List)을 주기적으로 서명하여 디렉토리 서버에 갱신 하지만 인증기관이 디렉토리 서버에 CRL을 갱신하는 시간 내에 취소된 인증서를 사용할 수 있다는 문제점을 가지고 있다.

본 논문에서는 인증서 상태 확인 및 검증을 위하여 사용되는 인증서 취소 목록 기법 및 OCSP등의 다양한 기법에 대한 구조 및 특징을 분석하고, 서버와 사용자간 핸드셰이크 과정 시 옵저버 정보를 추가하는 새로운 인증서 상태 확인 및 검증 기법을 제안한다. 제안한 방식은 인증서가 유효기간 내에 취소되었으나 디렉토리서버에 인증서 취소 정보가 갱신되지 않은 경우 옵저버를 이용하여 실시간으로 인증서의 상태 확인 및 검증을 할 수 있으므로 적시성을 증대하였을 뿐만 아니라 OCSP의 문제점을 보완할 수 있다.

ABSTRACT

A certificate is expected to use for its entire validity period. However, a false information record of user and compromise of private key may cause a certificate to become invalid prior to the expiration of the validity period. The CA needs to revoke the certificate. The CA periodically updates a signed data structure called a certificate revocation list(CRL) at directory server. but as CA updates a new CRL at directory server. the user can use a revoked certificate.

Not only does this paper analyzes a structure of CRL and a characteristic of certificate status conviction, OCSP method but also it proposes a new certificate status verification method adding an observer information in handshake process between user and server.

접수일 : 2004년 2월 19일 ; 채택일 : 2004년 8월 9일
† 주저자 : kw1226@hanmail.net
‡ 교신저자 : kjc@kdn.com

The Proposed method with observer makes it more efficient for relying parties to verify both the current status of X.509 certificate and the short-lived server certificate. Even when a revoked certificate information is not updated at directory server yet, the status of the certificate can be verified using the observer, and the proposed method can improve timeliness and compensate a weakness of OCSP.

Keywords : *OCSP, CRL, Observer, verify both the current status of X.509 certificate and the short-lived server certificate.*

Ⅰ. 서 론

공개키 기반구조(Public Key Infrastructure)는 공개키 암호 방식을 사용하는 암호시스템에서 사용자의 공개키를 안전하고 신뢰성 있게 공표 하는 수단을 제공한다. 인증서(Certificate)는 공개키를 안전하게 분배하기 위해 사용하는 서명된 문서이며, 인증서를 발급하고 관리하기 위한 기반 구조가 공개키 기반 구조(Public Key Infrastructure)이다.[1]

PKI구조는 사용자, 인증기관(CA : Certification Authority), 등록기관(RA : Registration Authority),디렉토리서버(Directory Server)로 구성된다.[2] 인증서는 웹상에서 비즈니스 또는 기타의 거래를 수행할 때, 인증기관이 가입자의 신분과 공개키 정보를 보증하기 위해 발급하는 전자 문서이다. 인증서[3]는 인증기관으로부터 발급되며, 수령인이 그 인증서의 진위여부를 확인할 수 있도록 소유자의 이름, 일련번호, 유효기간, 인증서 소유자의 공개키 사본 (메시지나 전자서명의 암호화 및 복원에 사용됨), 인증서 발급기관의 전자서명 등이 포함된다. 네트워크에 가입된 모든 사용자는 상대방의 인증서를 CA에게 요청할 수 있으며, CA의 공개키를 이용하여 상대방의 인증서를 확인할 수 있다.

인증서 취소에 관한 정보를 송, 수신 할 때 오랜 지연 시간과 인증서를 취소하는데 필요한 비용은 인증서 취소 기법을 선택하는데 매우 중요하다. 적시성은 인증서 취소 정보를 갱신한 후에 임의의 시간 동안 인증서 취소 정보를 사용할 수 있는가 하는 문제이다. 실제 인증서를 취소하는 시점에서 사용자가 인증서 취소 정보를 확인하는데 걸리는 시간의 차이는 적을수록 적시성은 좋다.

인증서의 유효성을 검증 하는 방법으로는 오프라인 인증서 검증 방법과 온라인 인증서 검증으로 구분할 수 있다. 첫째, 오프라인 인증서 검증 방법은 사용자(User)가 CRL의 유효기간 동안 저장 디렉토리에 CRL을 보관한 상태에서 인증서 유효성에 관한 요청이 들어오면 저장 디렉토리에 있는 CRL목록 중 해당 인증서를 검색하여 인증서의 유효성에 관한 응답을 하는 구조로 되어있다. 오프라인 인증서 검증 방법[4,5]에는 CRL, Over-Issued CRL, Delta CRL방법이 있다. CRL을 사용하여 인증서의 유효성을 검증 하는 오프라인 검증방법은 CRL을 CA의 디렉토리 서버로부터 주기적으로 갱신해야하며, CRL이 증가하면 사용자의 저장 디렉토리의 부하가 커지므로 실시간적인 서비스가 어려울 뿐 아니라, 해당 인증서의 검색이 손쉽게 이루어지지 않으며, CRL을 갱신하지 못한 경우에는 인증서 유효성을 판단할 수 없다는 단점을 가지고 있다.

둘째, 오프라인 인증서 검증 방법의 문제점을 개선하기 위한 방법으로 온라인 인증서 검증 방법이 있다. 온라인 인증서 검증 방법은 사용자가 저장 디렉토리에 CRL을 보관 하는 것이 아니라, 특정 인증서의 유효성 판단 여부를 묻는 요청이 들어오면 온라인으로 CA의 디렉토리 서버에 해당 인증서에 관한 유효성 판단여부를 요청하여 CRL목록을 검색한 후 질의에 관한 응답을 하는 구조로 되어 있다.

온라인 인증서 검증 방법[6-10]에는 CRS(Certificate Revocation System), CRT(Certificate Revocation Tree)방법과 IETF의 PKIX Working Group에 의해 제안된 OCSP (Online Certificate Status Protocol)[11,12] SCVP(Simple Certificate Validation Protocol)[13]방법이 있다. CRS와 CRT는 오프라인 방법보다는 적시에 인증서를 검증할 수 있으나, CA와 디렉토리 서버 사이의 통신량 증가와 CRT 업데이트를 위한 추가적인 연산이 필요한 단점과 전체 CRT의 재계산이 필요하다는 단점이 있으며, OCSP는 실시간으로 인증서의 유효성을 판단할 수 있다는 장점이 있으나, 서비스 불능(denial of service) 공격에 노출될 수 있으며, 응답시간이 중요한 요소이므로 과도한 요청이 들어올 시 오류 응답 발생 확률이 높다. 미리 응답을 생성하여 사용하는 경우, 재연 공격(reply attack)이 가능하다. 인증서 유효기간이 끝나기 전 인증서가 취소되고 미리 응답이 만들어질 경우 이루어질 수 있으며, 요청에

응답을 원하는 응답자(OCSP 서버) 정보가 들어있지 않다. 따라서 공격자, OCSP 응답자 등 아무에게나 요청을 다시 보낼 수 있다는 문제점이 있다. 제안한 방법은 사용자가 취소된 인증서를 사용할 경우 CA의 전자서명이 된 옵져버(인증서의 실시간 검증과 취소된 인증서를 이용해 악의적인 행동을 방지 하는 장치) 자신의 서명 및 추가 정보를 서버의 공개키로 암호화하여 전송하면 서버는 자신의 개인키로 헤더부분에 전자 서명된 정보를 복호화하여 검증함으로써 CRL기법의 단점인 서버의 부하감소와 취소된 인증서의 사용을 실시간으로 검증하고 적시성을 증대할 수 있는 기법을 제시하고자 한다.

본 논문은 다음과 같은 구성을 가진다. 2장에서는 인증서 취소 목록을 이용한 오프라인 인증서 검증 방법의 특징을 분석하고, 3장에서는 오프라인 인증서 검증의 단점을 해결하기 위한 방법으로 등장한 온라인 인증서 검증 방법의 특징 및 문제점을 분석한다. 4장에서는 취소된 인증서의 사용을 실시간으로 검증할 수 있으며 또한 적시성을 증대할 수 있는 기법을 제안하고 5장에서는 제안한 기법과 실시간 검증 방법인 OCSP 프로토콜과 장단점을 서로 비교 및 모의실험을 통한 성능평가를 하였으며, 마지막으로 6장에서는 결론을 맺는다.

Ⅱ. 오프라인 인증서 검증 방법

인증서의 폐지 여부를 확인할 수 있는 방법은 일반적으로 인증기관이 CRL을 공개하는 오프라인 인증서 검증 방법을 사용하고 있다. 사용자는 인증서 검증 시 CRL을 수신하여 해당 인증서가 인증서 취소목록에 포함되는지 여부를 판단한다. 이 경우 CRL의 인증서가 늘어나게 되면 부하가 커지므로 갱신을 주기적으로 하게 되어 실시간적인 서비스가 어려우며, CRL이 갱신되지 않았을 경우 인증서의 유효성을 적시에 검증할 수 없으므로 적시성이 떨어지며, 인증서의 검색이 손쉽게 이루어지지 않는다. 이런 CRL을 이용하여 인증서의 유효성을 검증하는 방법으로는 기본 CRL, Over-Issued CRL, Delta CRL 방법이 있다.

2.1 기본 CRL

David. A. Cooper는 CRL을 제공하는 시스템에서 사용자의 평균 요구 비율보다 최대 요구 비율이 더 중요하다고 한다. 사용자가 인증서 검증을 시도하는 시간은 서로 독립적이기 때문에, 지수 확률 분포를 사용하여 CRL 시스템에 대한 사용자 인증서 검증 시도 확률을 평가했으며, 인증서 검증을 시도할 확률 P(t)는 식(1)과 같다.

$$P(t) = ve^{-vt}dt \quad (1)$$

(t : 시간간격이 [t, t+dt], dt→0, v : 검증 비율)

사용자의 인원수가 증가 할 경우에는 증가하는 인원 수 만큼만 식(1)의 값에 곱해 주면 된다. 사용자 N명이 t시간에 CRL을 요구하는 비율은 $R(t) = Nve^{-vt}$가 된다. CRL을 발표한 후 시간이 경과할수록 사용자의 요구비율이 줄어드는 것을 알 수 있다.

2.2 Over-Issued CRL

기본 CRL에서 인증서의 취소날짜가 모두 동일함으로써 발생하는 문제점을 David. A. Cooper는 CRL의 취소 날짜보다 이전에 CRL을 발행하여 기본 CRL방식에서의 문제점인 사용자 요구량을 감소시키기 위해 검증 시간을 겹치게 함으로써 사용자의 요구 비율을 줄일 수 있는 Over-Issued CRL을 제안했다. CRL을 임의의 시간으로 겹치게 발행함으로써 사용자의 검증 요구 비율을 줄일 수 있다. Over-Issued CRL 검증 시간 동안의 N명 사용자 요구 비율은 식(2)과 같다.

$$Ro(t) = \frac{Nve^{-vt}}{(O-1)(1-e^{vl/o})+1} \quad (2)$$

(O : 현재 검증되는 CRL의 수 l : CRL의 검증 시간, N : 사용자의 수 v : 인증서 검증 비율)

Over-Issued CRL방식은 기존의 방식에 비해 CRL검증 시간을 단축하여 사용자의 최대 요구 비율을 줄일 수 있으며, 트래픽 지연 문제를 해결하는 것이 가능하다.

2.3 Delta CRL

델타 CRL은 기본 CRL을 발급한 후에 발생된 내용들을 전자 서명한 목록이다. 기본 CRL에서는 전체CRL을 가져 와서 인증서 상태를 검증 하지만

델타 CRL은 변경된 최근 CRL만을 가져와서 인증서를 검증하기 때문에 인증서 취소에 관한 정보 중 변경된 사항만을 추가하므로 인증서 취소에 관한 정보를 저장하는데 걸리는 시간이 크게 줄어든다는 장점을 가지고 있다. 델타 CRL을 사용하는 PKI 시스템에서 기본CRL을 요구하는 비율은 기본 CRL 사용자 요구비율과 같다.

$$R(t) = Nve^{-vt} \quad (3)$$

(t : 마지막으로 기본 CRL을 발급한 후에 경과한 시간)

델타 CRL의 사용자 요구 비율은 다음 식(4)과 같다.

$$R_{\Delta}(t) = Nve^{-vt} \quad (4)$$

(t : 델타 CRL을 발급한 후에 경과한 시간)

델타 CRL을 사용하면 기존CRL방식에 비해 CRL검증 시간 단축 및 사용자의 최대 요구 비율을 줄일 수 있고, 트래픽 지연문제를 해결하여 적시성에 효율적인 장점을 가지고 있다.

표 1. 오프라인 인증서 검증기법들의 비교

CRL	사용자 최대요구비율 높음	낮음
	CRL 보다 향상	CRL보다 향상 가능
	사용자 최대요구 비율 높음	CRL 보다 향상

Ⅲ. 온라인 인증서 검증 기법

2장에서 살펴본 오프라인 인증서 검증 방법의 문제점을 해결하기 위해 온라인 인증서 검증 방법이 제안 되었으며, 온라인 인증서 검증 방법은 CRS (Certificate Revocation System), CRT(Certificate Revocation Tree)방법과 IETF의 PKIX Working Group에 의해 제안된 OCSP(Online Certificate Status Protocol)방법이 있다. CRS와 CRT는 오프라인 방법보다는 적시에 인증서를 검증할 수 있으나, CA와 디렉토리 서버 사이의 통신량 증가와 CRT 업데이트를 위한 추가적인 연산이 필요한 단점과 전체 CRT의 재계산이 필요하다는 단점이 있다. OCSP는 실시간으로 인증서의 유효성을 판단할 수 있다는 장점이 있으나, 서비스 불능(denial of service) 공격에 노출될 수 있으며, 미리 응답을 생성하여 사용하는 경우 재연 공격(reply attack)이 가능하다는 문제점이 있다.

3.1 CRS(Certificate Revocation System)

CRS는 CRL의 통신량을 개선하기 위해서 Micali에 의해 제안된 기법이다. CRS기법에서의 중요한 핵심은 인증기관이 인증서의 취소 상태정보를 제공하기 위해서 메시지에 임의의 의사난수를 발생해서 서명하는 것이다. CRS는 다음과 같은 정보를 포함하는 사용자 공개키에 대한 인증서를 전자 서명하여 전송한다.

- 기본 정보 : 사용자 공개키, 사용자 이름, 인증서 일련번호, 발행자 서명알고리즘 종류, 인증날짜, 만료날짜
- 추가되는 정보 : 100bit의 Y값, 100bit의 N값 (두 개 의 랜덤 넘버는 인증기관에서 발생시킴)

CA(인증기관)에서는 의사난수 N_0 ,Y_0를 발생한 후 (일방향 함수 f를 사용하여) $Y_{365}=f^{365}(Y_0)$ and $N=f(N_0)$를 계산하고 인증서 에 추가하여 디렉토리 서버에 전송한다. 디렉토리 서버에 갱신되는 C의 값은 다음과 같다.

- 취소되지 않은 인증서를 표현하는 방법 CA는 100bit값 $C=Y_{365-i}=f^{365-i}(Y_0)$ 를 전송(i : 발행일부터 매일 1씩 증가해야 한다.)
- 취소된 인증서를 표현하는 방법 CA는 100bit값 $C=N_0$

사용자가 디렉토리 서버에 인증서 취소 상태에 관해서 증명을 요청하면 디렉토리 서버는 최근에 갱신된 100bit값을 사용자에게 전송하며 사용자는 $f^i(V)=Y$이면 인증서 취소가 되지 않은 상태인 것을 확인할 수 있고 반대로 $f(V)=N$이면 인증서 취소된 상태인 것을 알 수 있다.(V는 업데이트 된 값)

CRS는 인증서 질의 통신에 관한 비용절감뿐 아니라 의사난수를 사용한 인증서를 사용자가 확인함으로써 보다 충분한 확인을 할 수 있다는 장점은 가지고 있지만 CA와 디렉토리 서버사이에서의 통신량이

증가한다는 단점을 가지고 있으므로 CA와 디렉토리 서버사이의 통신량을 고려해야한다

3.2 CRT(Certificate Revocation Tree)

Paul.Kocher는 인증서 취소 상태 정보를 증명하기 위해서 CRT(Certificate Revocation Tree) 알고리즘을 제안했다. CRT는 인증기관에 의해서 발행된 인증서 일련번호 X에 관한 상태 집합들에 일치하는 단말 노드를 가진 해쉬 트리(hash tree)이다. 인증서 일련번호 X는 인증서의 취소 상태집합에 관한 정보와 취소 상태를 알 수 없는 인증기관의 범위에 있다는 정보를 제공해준다. 예를 들어 CA에서 -∞에서 21번 인증서를 가지고 있으며, 21,36,54의 취소된 일련번호를 가지고 있을 경우 21번을 제외하고 나머지 인증서는 유효하지만 21번은 취소된 인증서라는 것을 알 수 있다.

표 2. 상태 집합의 예

인증서 범위	취소된 인증서	인증서 상태
-∞~21	21,36,54	취소된 인증서21을 제외한 나머지 인증서는 유효
22~36	21,36,54	취소된 인증서36을 제외한 나머지 인증서는 유효
37~54	21,36,54	취소된 인증서 54를 제외한 나머지 인증서는 유효
55~∞	21,36,54	취소된 인증서가 없으므로 나머지 인증서는 유효

CRT 사용의 중요한 장점은 특정 인증서나 특정 사용자증명 뿐 아니라, 인증서 유효성을 간결하게 검증 할 수 있다는 것이지만 , CRT 업데이트를 위한 추가적인 연산이 필요한 단점과 취소된 인증서 집합의 변경은 전체 CRT의 재계산을 요구한다.

3.3 OCSP(Online Certificate Status Protocol)

인증서 상태 프로토콜은 [그림 1]과 같이 OCSP (Online Certificate Status Protocol) 서버와 OCSP 클라이언트간에 수행된다. OCSP 클라이언트는 특정 인증서의 유효성과 취소 상태를 서버로 문의하고, 서버는 인증서 유효성과 취소 상태를 전달한다. 클라이언트는 서버로부터 인증서가 유효하고 취소되지 않았다는 정보를 수신한 후에 문의한 인증서를 사용해야 한다. OCSP는 CRL방법보다 인증서의 상태 정보를 보다 적시에 실시간으로 얻을 수 있으며, 사용자가 OCSP 서버에게 인증서 상태를 요구하면 서버는 인증서의 상태를 응답하는 구조로 되어 있다. IETF의 RFC 2560은 인증서 상태를 체크하는 응용 프로그램과 상태 정보를 제공하는 서버상에서 오가는 데이터의 구조를 정의하였다.

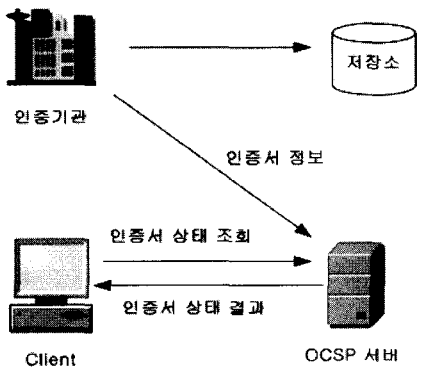


그림 1. OCSP 프로토콜

◉ 요구(Request) : OCSP 메시지는 다음의 요소들을 포함한다.
- 프로토콜 버전
- 서비스 요구
- 대상 인증서의 구별자
- OCSP 서버가 처리할 수 있는 확장 정보(선택)

➜ 요구에 따라 OCSP 다음사항을 확인하여 만족하지 못할 경우 에러 메시지를 전송한다.
- 메시지가 정상적으로 구성되었는지 여부
- 서버가 요구된 서비스를 제공할 수 있도록 설정되어 있는지 여부
- 서버가 서비스를 제공하기에 필요한 부가적 정보들이 요구서에 들어있는지 여부

◉ 응답(Response) : 모든 응답 메시지의 최종 타입은 반드시 전자 서명된 형식이여야 한다. 서명에 이용되는 전자 서명 생성키는 다음 중 하나이다.
- 응답메시지 구문의 버전
- 응답 서버의 이름
- 요구에 따른 응답들
- 선택적인 확장 필드들
- 전자서명 알고리즘의 OID
- 응답 메시지의 해쉬를 이용한 전자서명

➔ 요구에 따른 응답들은 다음으로 구성된다.
- 대상 인증서의 구별자
- 인증서 상태 정보
- 응답에 대한 유효기간
- 선택적인 확장 필드

➔ 인증서의 상태는 다음 세 가지로 구분 된다.
- 양호(good)
- 폐지(Revoked)
- 알 수 없음(Unknown)

◎ OCSP서버 구현 시 고려할 사항은 다음과 같다.
① OCSP서버는 항상 이용할 수 있어야 한다.
② 동시에 대량 인증서 상태 확인 요청이 있는 경 우 서비스의 장애가 발생할 수 있다.
③ 미리 계산된 응답 사용 시 응답 유효 기간 동안 인증서가 폐지되어도 그 응답을 재사용할 문제가 발생할 수 있다.
④ 상태 확인 요청에 응답 OCSP 서버의 정보가 포함되어 있지 않기 때문에 하나의 요청이 많은 OCSP서버에 재사용될 수 있다.

OCSP 서버를 이용하여 인증서 상태 정보를 획득하는 경우 CRL을 통하는 것보다 더 적시에 취소 정보 획득이 가능하고 고액 자금 이체 혹은 대형 주식 거래 시에 유용하며 또한 OCSP 서버를 통하여 부가 정보 획득이 가능한 장점이 있고, 실시간으로 인증서를 검증할 수 있다는 장점이 있는 반면 다음과 같은 문제점이 있다.

첫째, 서비스 불능(denial of service) 공격에 노출된다. OCSP는 응답시간이 중요한 요소이므로 과도한 요청이 들어올 시 오류 응답 발생 확률이 높다. 둘째, 미리 응답을 생성하여 사용하는 경우, 재연 공격(reply attack)이 가능하다. 인증서 유효기간이 끝나기 전 인증서가 취소되고 미리 응답이 만들어질 경우 이루어질 수 있다. 요청에 응답을 원하는 응답자(OCSP 서버) 정보가 들어있지 않다. 따라서 공격자, OCSP 응답자 등 아무에게나 요청을 다시 보낼 수 있다는 문제점이 있다.

3.4 SCVP(Simple Certificate Validation Protocol)

SCVP는 [그림 2]와 같이 SCVP 클라이언트, SCVP 서버, CA서버로 구성되며, SCVP 클라이언트는 경로 검증이나 폐지 상태 등을 확인하고자 하는 정보를 포함한 요청을 SCVP 서버로 전송하고, SCVP 서버는 요청된 내용의 결과를 SCVP 서버의 전자서명 생성키로 전자 서명한 응답을 SCVP 클라이언트에 전송한다. SCVP는 인증서 상태를 문의하거나 인증경로를 발견하고, 경로에 대한 유효성을 문의하기 위한 프로토콜이다. 이는 SCVP 서버와 클라이언트 간에 수행되며, 서버는 클라이언트로 인증서의 유효성과 취소 상태, 서명문 검증을 위한 인증서 체인의 유효성과 설정된 인증서 체인을 결과로 전달한다. SCVP는 응용이 PKI를 채용함에 따라 추가적으로 요구되는 절차와 부담을 간단히 할 수 있는 방법을 제공한다.

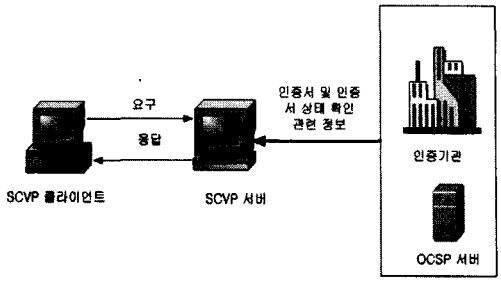


그림 2. SCVP 프로토콜

SCVP는 두 가지 목적으로 사용될 수 있다. 첫째는 스스로 대부분의 PKI 기능을 수행 하고, 단순히 정보 수집에는 유용하지만 신뢰하지 않는 서버를 필요로 하는 클라이언트에 의해 사용된다. 둘째는 인증서 검증에 대한 부담을 덜고 한 기업 내에서 일치된 형태의 정책이 반영된 충분히 신뢰성 있는 서버를 필요로 하는 클라이언트에 의해 사용될 수 있다.

SCVP 서버는 사용자에게 경로 검증을 위한 인증서 연결 정보를 제공하고 CRL 및 OCSP 응답과 같이 사용자의 경로 검증에서 사용할 수 있는 폐지 정보를 제공한다. SCVP 서버는 클라이언트를 위하여 충분한 인증서 검증을 수행한다. 클라이언트가 이 서비스를 사용하는 경우 SCVP 서버를 자신이 소유한 경로 검증의 동일한 수준으로 신뢰해야 한다.

표 3. 온라인 인증서 검증기법들의 비교

	사용자 최대요구비율 증가	낮음
	CRL 보다 향상 가능	낮음
	기존기법 보다 향상	기존기법 보다 향상

Ⅳ. 옵저버를 이용한 인증서 검증의 적시성 증대 기법

2장 3장에서 설명한 오프라인 인증서 검증 기법과 온라인 인증서 검증 기법에서의 문제점을 해결하기 위해 본 논문에서는 새로운 인증서 상태 및 불법적인 사용 방지 확인 기법을 제안한다. 제안한 방식은 사용자 단말기에 CA의 전자 서명된 옵저버를 이용하여 CA가 디렉토리 서버에 CRL을 주기적으로 갱신하는 동안(24시간 주기로 CRL을 갱신) 취소된 인증서 사용을 방지할 수 있으며 적시성도 개선하였다.

4.1 옵저버를 이용한 인증서 검증의 적시성 증대 기법을 위한 공개키 기반구조(PKI) 모델

사용자가 인증서 취소를 등록기관(RA)에 요청하여 인증서를 취소할 경우 [그림 3]과 같은 알고리즘 단계로 수행되며, 알고리즘을 수행할 조건의 가정은 다음과 같다.

1. SSL환경에서 동작하고 핸드셰이크 프로토콜 과정 중 서버와 사용자간 옵저버 정보를 교환하여 인증서의 유효성을 검증하며, 핸드셰이크 과정은 [그림 4]와 같이 동작한다.
2. 공인 인증기관은 일정 주기로 CRL을 배포한다. 공인 인증기관은 새로운 CRL을 갱신 중에 있고, 서버는 갱신될 새로운 CRL을 디렉토리 서버로부터 아직 다운로드 받지 못한 상태에서 사용자가 취소된 인증서를 사용했다고 가정한다.

○ 옵저버를 이용하여 인증서를 실시간으로 검증하기 위하여 다음과 같은 알고리즘을 제안하였고 아래와 같은 단계를 통하여 인증서 검증을 수행 한다.

[단계1] 사용자가 인증서 취소를 RA(등록기관)에 요청한다.

[단계2] RA는 CA에 사용자의 인증서 취소를 통보한다.

[단계3] CA는 RA에게 자신의 전자서명된 옵저버를 전송한다.

[단계4] RA는 인증서 취소 요청을 한 사실, 옵저버ID 및 CA에 인증서 취소 통보 날짜 시간을 기록한 TIMESTAMP를 CA의 전자 서명한 옵저버를 사용자에게 전송한다.

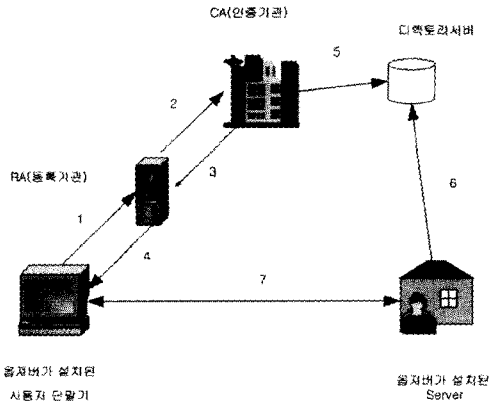


그림 3. 옵저버를 이용한 인증서 검증의 적시성 증대 기법

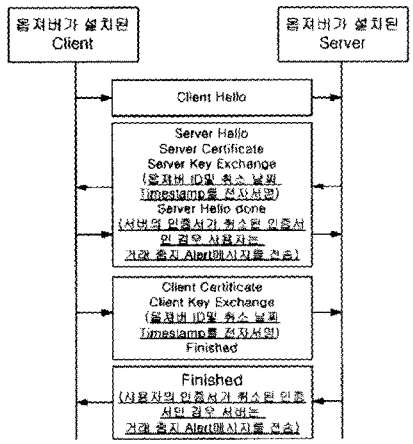


그림 4. 핸드셰이크 절차 흐름도

[단계5] CA는 디렉토리 서버에 사용자가 취소 요청한 인증서를 CRL에 갱신한다.

[단계6] 옵저버가 설치된 서버는 디렉토리 서버에서 사용자의 취소된 인증서가 갱신되지 않은 CRL을 자신의 서버로 다운로드 한다.

[단계7] 갱신되지 않고 취소된 인증서를 사용하여 사용자와 서버가 거래를 할 경우 서버와 사용자간에는 옵저버 정보가 추가된 다음과 같은 SSL(Secure Socket Layer)의 핸드셰이크 프로토콜(Handshake Protocol) 절차를 적용한다.

[핸드셰이크(Handshake) 절차]

현재 SSL 프로토콜에서는 인증서의 유효성 여부

를 검증하지 않지만, 제안한 알고리즘에서는 실시간적으로 인증서의 유효성을 검증하고, OCSP 보안적인 측면의 문제점을 해결하고자 옵져버 정보를 핸드셰이크 프로토콜 과정에 추가하였다.

〔7-1〕 과정

○ 사용자는 Client_hello메시지를 전송한다.

〔7-2〕 과정

○ 서버는 Server_hello 메시지를 사용자에게 전송한다.

〔7-3〕 과정

○ 서버는 메시지 키 분배용 인증서가 포함된 Server_Certi ficate메시지를 사용자에게 전송한다.

〔7-4〕 과정

○ 서버는 자신의 인증서 메시지 및 Server_key _exchange 메시지를 전송하며, 인증서 증명 메시지를 전송하기 전에 옵져버는 서버의 개인키를 사용하여, 등록기관으로부터 부여받은 옵져버 ID와 인증서 취소 통보 날짜 및 시간을 기록한 Timestamp를 전자서명 하여 메시지 header부분에 삽입한다. 이런 메시지를 수신한 사용자는 header부분에 서버의 개인키로 전자 서명된 데이터를 서버의 공개키로 검증하여 추가된 옵져버의 정보를 확인함으로써 사용자의 인증서가 취소된 인증서임을 확인할 수 있다.

〔7-5〕 과정

○ 서버는 Server_Hello_Done 메시지를 전송한다. 만일 서버의 인증서가 취소된 인증서인 경우 이를 검증한 사용자는 인증서의 유효성 여부와 거래중지를 알리는 Alert 메시지를 전송한다.

〔7-6〕 과정

○ 사용자는 인증서 정보, 공개키 등의 데이터가 포함된 Client_Certificate메시지를 전송한다.

〔7-7〕 과정

○ 사용자는 서버로부터 수신한 옵저버 정보를 서버의 공개키로 암호화한 데이터가 포함된 Client_Key_Exchange 메시지를 전송한다. 만일, 사용자의 인증서가 취소된 인증서인 경우 옵저버 정보는 등록기관으로 부터 부여받은 옵져버 ID인증서 취소 통보날짜 및 시간을 기록한 Timestamp가 메시지 header부분에 삽입된다. 이런 메시지를 수신한 서버는 header부분에 서버의 개인키로 복호화하여 추가된 옵져버의 정보를 확인함으로써 사용자의 인증서가 취소된 인증서임을 검증할 수 있다.

〔7-8〕 과정

○ 사용자는 Finished 메시지를 서버에게 전송한다.

〔7-9〕 과정

○ 서버는 Finished 메시지를 사용자에게 전송한다. 만일 사용자의 인증서가 취소되었으나 디렉토리 서버에 갱신되지 않았을 때 이를 검증한 서버는 인증서의 유효성 여부와 거래중지를 알리는 Alert 메시지를 전송한다.

4.2. 핸드셰이크 프로토콜과정에 추가된 옵져버 정보 (＊ : 추가된 정보)

CRL방법의 단점인 실시간 검증과 OCSP에서의 보안적인 문제점을 보완하고자 핸드셰이크 프로토콜 과정에 추가되는 옵져버에 정보는 다음과 같다.(제안한 방법은 인증서 유효성 검증을 위해 SSL 핸드셰이크 과정 중 header부분에 취소된 인증서 사용을 방지할 수 있는 정보를 추가하였다.)

＊senderObserver ObserverID -- 등록기관에서 부여한 옵져버 ID를 기록
＊ObserverSignature Observer 서명
＊SignatureAlg -- Observer 서명 알고리즘
＊TIMESTAMP -- RA가 CA에 인증서 취소 요청을 통보한 날짜 및 시간을 기록
＊notify&reject(Alert 메시지에 포함 -- 취소된 인증서라는 것을 통보한다.)

V. 모의실험 및 고찰

본 장에서는 각각 다른 인증서 상태 확인 기법들의 비교 및 실시간 검증 방법인 OCSP와 제안한 기법인 옵져버를 이용한 인증서 검증의 적시성 증대 기법의 장단점을 비교 분석하였으며, 실시간 검증 방법인 OCSP프로토콜과 제안한 방법인 옵져버를 이용한 인증서 검증의 적시성 증대 기법에 대한 성능을 분석하여 검증 시간이 개선됨을 보이고자 한다. 또한 제안한 Observer를 이용한 인증서 검증 방법은 실시간 검증 방법이므로 오프라인 인증서 검증 방법인

CRL과, Over-issued CRL 검증 방법보다 적시성이 우수함을 직관적으로 알 수 있으므로 모델 분석이나 시뮬레이션은 수행하지 않았다. 인증서를 검증 하고자 할 때 검증 시간을 평가하기 위하여 Jose L. Munoz가 보고한 성능 평가 환경 및 모의실험 모델, 파라메터, 결과 값을 근거로 COMNET3툴을 이용하여 모의실험을 하였다.

○ 모의실험을 위한 가정은 다음과 같다.

1) 전체 취소 시스템 안에서 발생하는 검증 과정(검증 시간)에 중점을 두었다.
2) 제안한 기법은 인증서의 유효성 검사를 실시간적으로 적시에 검증할 수 있고, OCSP의 보안적인 문제점을 해결하기 위해 제안 하였으므로, 오프라인 인증서 검증 방법이 아닌 온라인 인증서 검증방법 중 OCSP와의 성능평가만 하였다. 또한 현재의 네트워크의 데이터 처리 속도 및 하드웨어의 성능 등을 고려하여 옵져버 추가에 따른 부하는 고려하지 않았다.
3) 모의실험을 위한 모델로는 [그림 5]와 같은 Repository model을 사용하였으며, 동일한 시간에 하나 이상의 요청(인증서 검증 요청)은 처리하지 않는다(N : 검증자의 수, vi : 평균 요청비율).

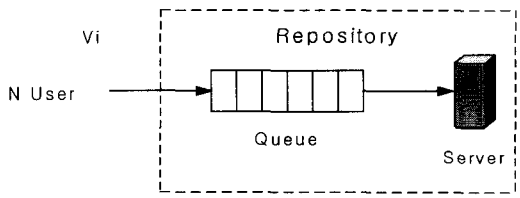


그림 5. Repository model

N이 상당히 크고 다른 사용자에 의해 들어온 응답이 각각 독립적이라고 한다면 요청과 다음 요청 사이의 경과시간은 지수 확률 밀도 함수의 표현할 수 있다. 지수 확률 밀도 함수는 e^{-vt}와 같은 식으로 표현된다.(여기서 v는Repository로 향하는 평균 요구비율이다.)

서비스 시간 Ts는 요청 들어온 인증서를 검증하는데 필요한 시간 Tp와 전송하는데 필요한 시간을 더한 값 식(5)과 같이 표현된다.

$$Ts = Tp + Tx \tag{5}$$

Tp : 요청 들어온 인증서 검증 시간
Tx : 요청에 대한 응답 시간

*VD(Validation Data)*는 헤더 H에 하나의 인증서 안에 포함된 정보 I를 더한 것이다.

$$VD = H + I \tag{6}$$

서버의 부하량 ρ는 식(7)과 같이 표현하며 여기서 $\upsilon = Nvi$이다.(vi 평균 요구비율을 나타낸다.)

$$\rho = \upsilon Ts \tag{7}$$

M/D/1 큐잉 시스템을 통해서 대역폭B와 검증시간 Tv식을 얻을 수 있다. 식 (5), (6), (7)에 의해 얻어진 대역폭의 식은 다음과 같다.

$$B = \frac{H+I}{\frac{\rho}{\upsilon} - Tp} \tag{8}$$

M/D/1 큐잉 시스템으로부터 얻어진 Tv은 다음과 같다.

$$Tv = \frac{Ts(2-\upsilon Ts)}{2(1-\upsilon Ts)} = \frac{(\frac{H+cI}{B} + t_p)[2-\upsilon(\frac{H+cI}{B} + t_p)]}{2[1-\upsilon(\frac{H+cI}{B} + t_p)]} \tag{9}$$

5.1 인증서 검증 과정

OCSP와 제안한 알고리즘에서의 인증 과정은 [그림 6]과 같다.

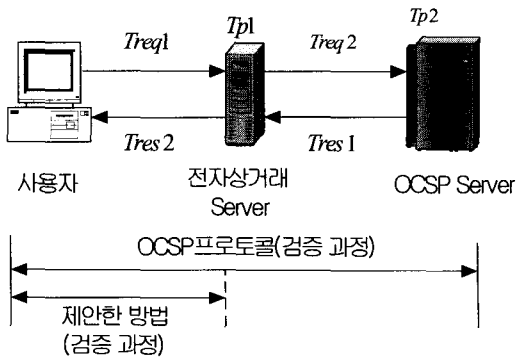


그림 6. 인증서 검증 과정

5.2 OCSP에서의 응용

OCSP에서의 서비스 시간 Ts는 요청 들어온 인증서를 검증하는데 필요한 시간Tp와 전송하는데 필요한 시간을 더한 값 식(10)과 같이 표현된다.

$$Ts(ocsp) = Treq1 + Tp1 + Treq2 + Tp2 + Tres1 + Tres2 \quad (10)$$

사용된 용어는 다음과 같다.

Treq1 : 사용자가 전자상거래 서버에 인증서 검증을 요청하는 시간
Tp_1 : OCSP 서버를 라우팅 하는데 걸리는 시간.
Treq2 : 전자상거래 서버가 OCSP 서버에 전송하는 시간.
Tp2 : 요청 들어온 인증서를 검증하는 시간.
Tres1 : OCSP 서버에서 전자상거래 서버에 인증서 검증에 대한 응답시간
Tres2 : 전자상거래 서버에서 사용자에게 인증서 검증에 대한 응답시간

*VD(Validation Data)*는 헤더 *H*에 하나의 인증서 안에 포함된 정보 *I*를 더한 것이다.

$$VD_{(OCSP)} = H + I \quad (11)$$

서버의 부하량 ρ는 식(12)과 같이 표현하며 여기서 $\upsilon = Nvi$이다.(*vi* 평균 요구비율을 나타낸다.)

$$\rho_{(OCSP)} = \upsilon Ts \quad (12)$$

식 (10), (11), (12), 에 의해 얻어진 대역폭의 식은 다음과 같다.

$$B_{(ocsp)} = \frac{H + I}{\frac{\rho}{\upsilon} - (Tp1 + Tp2)} \quad (13)$$

M/D/1 큐잉 시스템으로부터 얻어진 Tv은 다음과 같다.

$$Tv_{(OCSP)} = \frac{Ts(2 - \upsilon Ts)}{2(1 - \upsilon Ts)} \quad (14)$$

5.3 제안한 알고리즘에서의 응용

제안한 알고리즘에서의 서비스 시간 Ts는 식(15)과 같다.

$$Ts_{(제안한알고리즘)} = Treq1 + Tp1 + Tres2 \quad (15)$$

*VD(Validation Data)*는 헤더 *H*에 하나의 인증서 안에 포함된 정보 *I*를 더한 것이다.

$$VD_{(제안한알고리즘)} = H + I \quad (16)$$

서버의 부하량 ρ는 식(17)과 같다.

$$\rho_{(제안한알고리즘)} = \upsilon Ts \quad (17)$$

대역폭B의 식(18)과 같이 표현된다.

$$B_{(제안한알고리즘)} = \frac{H + I}{\frac{\rho}{\upsilon} - Tp1} \quad (18)$$

인증서 검증 시간 Tv는 식(19)과 같이 표현된다.

$$Tv_{(제안한알고리즘)} = \frac{Ts(2 - \upsilon Ts)}{2(1 - \upsilon Ts)} \quad (19)$$

모의실험을 실행하기 위한 파라메터들은 [표 3]과 같으며, 사용된 파라메터 값은 M. Myers, Jose L. Munoz가 보고한 결과 값을 근거로 하였다.

표 4. 모의실험에 이용된 파라메

파라메터	입력값
N(사용자수)	30,000명
H(헤더)	130Byte
I (인증서에 관련된 정보)	28Byte
Tp (인증서 검증시간)	0.0001[ms]
ρ(서버 부하량)	0.7초

5.4 모의실험 결과

본 절에서는 OCSP 프로토콜과 제안한 옵져버를 이용한 인증서검증의 적시성 증대기법의 모의 실험결과를 분석하였다.

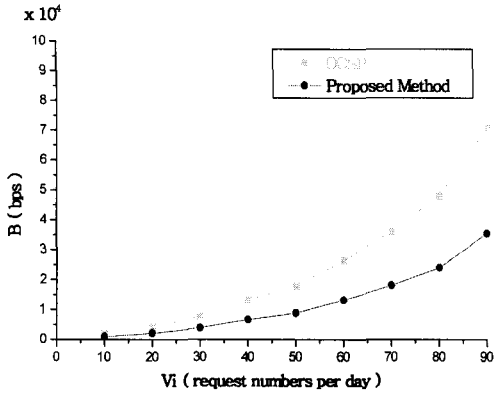


그림 7. 평균 요구비율에 따른 대역폭 비교

〔그림 7〕은 평균 검증 요구비율에 따라 대역폭의 변화를 그래프로 나타내었다. 〔그림 7〕은 OCSP 프로토콜과 제안한 알고리즘과의 대역폭을 서로 비교 분석한 그래프이다. OCSP 프로토콜은 제안한 알고리즘 보다 평균 검증 요구 비율이 증가함에 따라 더 높은 대역폭이 요구 되며, 또한 많은 수의 인증서 검증 요청이 들어오면, 제안한 방법은 대역폭이 OCSP보다 덜 요구되기 때문에 OCSP보다 더 많은 인증서 검증 요청에 대한 인증서를 검증할 수 있으므로, 제안한 방법이 OCSP보다 적시성이 향상되었다.

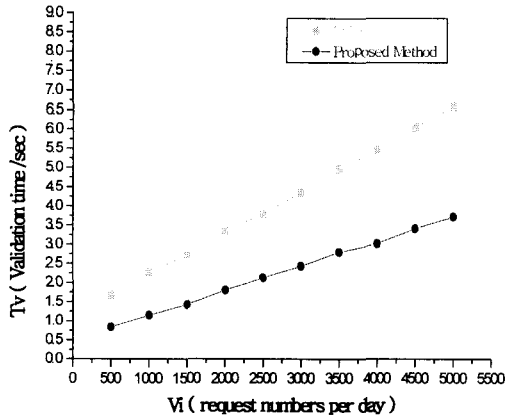


그림 8. 평균 요구 비율에 따른 검증 시간 비교

〔그림 8〕은 OCSP 프로토콜과 제안한 방법과의 검증시간을 서로 비교 분석한 그래프이다. 〔그림 6〕 인증서 검증 과정 에서도 볼 수 있듯이 OCSP 프로토콜 같은 경우에는 사용자가 인증서 검증을 전자상거래 서버에 요청할 경우 전자상거래 서버는 CRL 목록을 가지고 있지 않기 때문에 CA의 OCSP 서버에 검증을 요청해야한다. OCSP 서버에서 인증서 검증에 관한 정보를 전자상거래 서버에 전송하면 전자 상거래 서버는 사용자에게 요청에 대한 응답을 하기 때문에 실시간으로 인증서 검증을 할 수 있지만 검증시간이 오래 걸린다. 하지만 제안한 방법은 사용자와 전자상거래 서버사이에서 모든 검증이 이루어지기 때문에 OCSP 프로토콜보다 검증시간이 줄어들고 적시성이 향상될 수 있음을 알 수 있다.

오프라인 인증서 검증 방법에는 CRL, Over-Issued CRL, Delta CRL방법이 있다. CRL을 사용하여 인증서의 유효성을 검증 하는 오프라인 검증방법은 CRL을 CA의 디렉토리 서버로부터 주기적으로 갱신해야하며, CRL이 증가하면 사용자의 저장 디렉토리의 부하가 커지므로 실시간적인 서비스가 어려울 뿐 아니라, 해당 인증서의 검색이 손쉽게 이루어지지 않으며, CRL을 갱신하지 못한 경우에는 인증서 유효성을 판단할 수 없다는 단점을 가지고 있다. 온라인 인증서 검증 방법에는 CRS(Certificate Revocation System), CRT(Certificate Revocation Tree)방법과 IETF의 PKIX Working Group에 의해 제안된 OCSP (Online Certificate Status Protocol)방법이 있다. CRS와 CRT는 오프라인 방법보다는 적시에 인증서를 검증할 수 있으나, CA와 디렉토리 서버 사이의 통신량 증가와 CRT 업데이트를 위한 추가적인 연산이 필요한 단점과 전체 CRT의 재계산이 필요하다는 단점이 있으며, OCSP는 실시간으로 인증서의 유효성을 판단할 수 있다는 장점이 있으나, 서비스 불능(denial of service) 공격에 노출될 수 있으며, 응답시간이 중요한 요소이므로 과도한 요청이 들어올 시 오류 응답 발생 확률이 높다. 미리 응답을 생성하여 사용하는 경우, 재연 공격(reply attack)이 가능하다. 인증서 유효기간이 끝나기 전 인증서가 취소되고 미리 응답이 만들어질 경우 이루어질 수 있으며, 요청에 응답을 원하는 응답자(OCSP 서버) 정보가 들어있지 않다. 따라서 공격자, OCSP 응답자 등 아무에게나 요청을 다시 보낼 수 있다는 문제점이 있다.

〔표 4〕는 OCSP와 제안한 방법을 비교 하였다. 제안한 기법은 옵져버를 사용함으로써 인증서에 대한 실시간 검증이 가능하다. 취소된 인증서가 디렉토리 서버에 갱신되지 않았을 때, 사용자가 취소된 인증서를 사용할 경우 옵져버가 동작하여 PKI 메시지 헤더 부분에 옵져버 추가 정보가 기록되어 전송되면 서버는 옵져버의 추가 정보를 확인함으로써, 적시에 취

소된 인증서를 검증할 수 있다.

표 4. OCSP와 제안한 방법과의 비교

구분	OCSP	제안한 방법
실시간 인증서 [illegible] 여부	가능	가능
[illegible]	좋음	OCSP보다 향상
[illegible]	많음	적음
[illegible] 요소	서비스 불능 및 재연공격 가능	OCSP 보안 문제 해결

또한 인증서 검증 시 매번 인증기관의 OCSP서버에 인증서 검증을 요구하고 응답 받음으로써 발생되는 전송시간을 줄일 수 있을 뿐 아니라 OCSP서버로의 트래픽 집중 및 보안 문제점을 보완할 수 있다.

Ⅳ. 결 론

본 논문에서는 오프라인 인증서 검증 방법과 온라인 인증서 검증 방법의 특징과 장단점을 분석하여, 인증서 상태의 실시간 검증 및 적시성 향상을 위해 옵져버를 이용한 인증서 검증의 적시성 증대 기법을 제시하였다. 첫째, 오프라인 검증방법은 CRL을 CA의 디렉토리 서버로부터 주기적으로 갱신해야하며, CRL이 증가하면 사용자의 저장 디렉토리의 부하가 커지므로 실시간적인 서비스가 어려울 뿐 아니라, 해당 인증서의 검색이 손쉽게 이루어지지 않으며, CRL을 갱신하지 못한 경우에는 인증서 유효성을 판단할 수 없다는 단점을 가지고 있다.

둘째, 온라인 인증서 검증 방법인 CRS와 CRT는 오프라인 방법보다는 적시에 인증서를 검증할 수 있으나, CA와 디렉토리 서버 사이의 통신량 증가와 CRT 업데이트를 위한 추가적인 연산이 필요한 단점과 전체 CRT의 재 계산이 필요하다는 단점이 있으며, OCSP는 실시간으로 인증서의 유효성을 판단할 수 있다는 장점이 있으나, 서비스 불능(denial of service) 공격에 노출될 수 있으며, 응답시간이 중요한 요소이므로 과도한 요청이 들어올 시 오류 응답 발생 확률이 높다. 미리 응답을 생성하여 사용하는 경우, 재연 공격(reply attack)이 가능하다. 인증서 유효기간이 끝나기 전 인증서가 취소되고 미리 응답이 만들어질 경우 이루어질 수 있으며, 요청에 응답을 원하는 응답자(OCSP 서버) 정보가 들어있지 않다. 따라서 공격자, OCSP 응답자 등 아무에게나 요청을 다시 보낼 수 있다는 문제점이 있다.

제안한 기법에서는 이런 문제점을 해결하기 위해 옵져버를 사용하여 디렉토리 서버에 갱신되지 않은 취소된 인증서 사용여부 검증, 인증서 검증의 적시성 증대를 위한 모델을 제안하여, 취소된 인증서를 사용하였을 경우 실시간으로 검증 및 적시성을 향상하였으며, 제안한 기법은 옵져버가 설치되어 CA와 디렉토리 서버 사이에서의 트래픽과 CA와 사용자 사이에서의 트래픽이 발생하지 않기 때문에 CA와 디렉토리 서버, CA와 사용자 사이에서의 통신량 증가의 문제점을 해결 할 수 있음을 알 수 있었다.

참고 문헌

[1] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영,"전자 상거래 보안 기술" 생능 출판사, 1999.

[2] R. Housley, W. Ford, T. Polk, D.solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, pp.1-64, 1999.

[3] William. Stallings," Cryptography and Network Security" Principles and Practice, Prentice Hall. pp.444-460

[4] D. A. Cooper, "A Model of Certificate Revocation,"Proceedings of the 15th Annual Computer Security Applications Conference, pp.1-6, 1999.

[5] D. A. Cooper, "A More Efficient Use of Delta-CRLs, In Proceedings of the 2000 IEEE Symposium on ecurity and Privacy, pp.1-10, 2000.

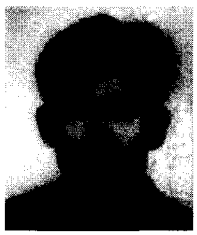
[6] A. Arnes, S. J. Knapskog, " Selecting Revocation Solutions for PKI," NORSEC 2000, pp.1-7, 2000.

[7] S. Berkovits, J. C. Herzog, "A Comparison of Certificate Validation Methods for Use In a Web Environment," MITRE Technical Report,

[8] Naor, K. Nissim, "Certificate Revocation and Certificate Update," Proceedings of the 7th USENIX Security Symposium, pp.1-3, 1998. November,

pp.12-21 1998. 2002.
[9] P. McDaniel, S. Jamin, "Windowed Certificate Revocation," IEEE INFOCOM, pp.1-4, 2000.
[10] 김명희. 전문석, "공개키 기반구조의 인증서 상태확인 기법" SK Telecom Telecommunications Review, 제 12권 1호, pp.1-8, 2002.
[11] Jose. L. Munoz Jordi Forne Juan C. Castro. "Evaluation of Certificate Revocation Policies : OCSP Vs Over-issued-CRL." IEEE, pp.1-5, 2002.
[12] M. Myers, R. Ankney, and C. Adams. "Online Certificate Status Protocol - Version 2."pp.1-6. 2000. IETF Internet Draft Draft-ietf-pkixocspv2 -00.txt
[13] 이만영, 원동호, 이민섭, 송주석, 임종인, 박춘식,"현대 암호학 및 응용" 생능 출판사, pp. 368-36.

〈著者紹介〉



권 오 인 (Oh-In, Kwon)
2001년 2월 : 서울산업대학교 전자공학과 졸업
2004년 2월 : 광운대학교 전자통신공학과 석사
2004년 3월~현재 : 전자부품연구원(KETI) 신뢰성 평가센터 위촉 연구원
〈관심분야〉 정보보호, 컴퓨터/네트워크 보안, 공개키 기반 구조(PKI)

김 진 철 (Jin-Chul, Kim)
1995년 2월 : 광운대학교 전자공학과 졸업
1997년 2월 : 광운대학교 전자공학과 석사
2000년 3월~현재 : 광운대학교 전자공학과 박사과정
〈관심분야〉 PKI, WPKI, Mobile Ad-hoc Network

오 영 환 (Yong-Hwan, Oh)
1980년 3월~현재 : 광운대학교 전자통신공학과 교수
〈관심분야〉 정보보호, 전자공학, 통신공학