분산된 OCSP 그룹으로 안전한 인증서 취소 목록 전달 방법에 관한 연구

A Proposal for Transmission Method of Safety CRL to Distributed OCSP Group

고 훈* 장 의 진** 신 용 태***
Hoon Ko Uijin Jang Yongtae Shin

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 검사 한다. 그러나 사용자의 증가와 CRL의 크기 증가로 인해서 많은 부담이 된다. 최근에는 온라인상으로 유효성을 검사하는 OCSP(Online Certificate Status Protocol)이 대안 방안으로 발표되었다. 그러나 이 또한 하나의 인증서 저장소에 집중화됨으로써 문제가 발생하게 된다. 이에 본 논문에서는 OCSP_Server를 분산된 지역에 배치하고 이 OCSP_Server에 정보를 안전하게 전달하는 방안을 제안하고자 한다.

Abstract

PKI(Public Key Infrastructure) issues a certificate for providing integrity of public key, and it inspects the validity by downloading CRL(Certificate Revocation List) for checking the validity of certificate. But, it imposes a burden on processing of certificate due to increase of user and the size of CRL. Lately, OCSP(Online Certificate Status Protocol), which examines the validity on online, is published as an alternative plan. But, it makes a problem due to concentration of just one certificate repository. Accordingly we propose the scheme that OCSP server is arranged in distributed area and then the information is safely transmitted to OCSP server.

Keyword : network security, internet security, encrypt protocol, information security, wireless internet security

Ⅰ. 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 한다. 하지만 이 방법은 인증서를 검증하고자 할 때마다 인증서 폐지 목록 전체를 다운받아야 하고 인증서 폐지 목록의 크기가 커질수록 다운받아야 하는 목록의 크기가 커짐에 따라 다운받는 시간과 통신량의 증가로 이어진다는 단점을 가지고 있다. 또한 기존의 인증서 상태 검증 방법들이 주로 주기적으로 발행되는 CRL에 기반을 두고 있기 때문에 인증서 현재 상태에 대한 시간 차이에 따른 문제가 발생된다. 최근에는 온라인상으로 유효성을 검사하는 OCSP (Online Certificate Status Protocol)이 대안방안으로 발표되었다[6]. 그러나 이 또한 하나의 인증서 저장소에 집중화됨으로써 서비스 집중화 문제를 야기한다. 이에 대한 해결책으로 OCSP_Server를 분산된 위치에 배치하는 방안을 제시한다. 그러나 이 또한 정보 전달 과정에서 제 3자에게 정보가 노출 될 수 있다. 이에 본 논문에서는 OCSP_

* 정 회 원 : 대진대학교 컴퓨터공학과
skoh21@daejin.ac.kr(제 1저자)
** 정 회 원 : (주) 디지캡스 선임연구원
neon@digicaps.com(공동저자)
*** 정 회 원 : 숭실대학교 컴퓨터학과
shin@comp.ssu.ac.kr(공동저자)

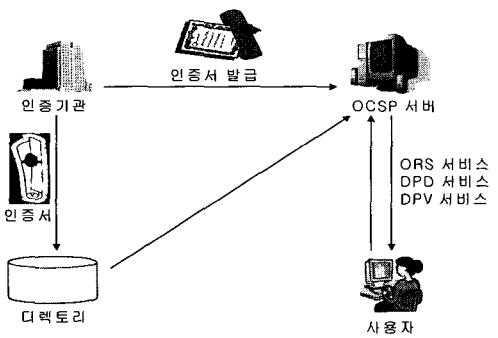
Server에게 비밀키 방식과 공개키 방식을 혼합한 암호화 방식을 이용해서 안전하게 갱신정보를 전달하는 방법을 연구하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장은 OCSP에 대한 설명을 하고, Ⅲ에서는 기존의 OCSP 구성도를 대해서 설명한다. Ⅳ장은 본 논문에서 분산된 OCSPServer를 설명한다. Ⅴ장에서는 제안한 모델 에 대한 분석을 하고 Ⅵ장에서는 결론을 설명하고자 한다.

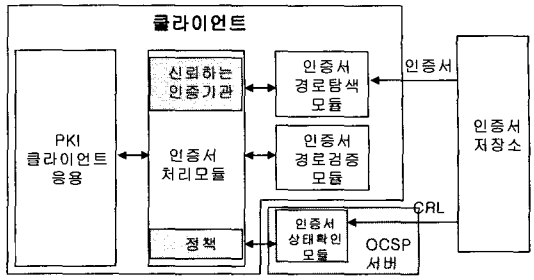
Ⅱ. OCSP

OCSP(Online Certificate Status Protocol) 방식은 인증기관과 디렉토리와는 별도로 서버를 두고 이 서버에서 사용자의 검증 요구에 대한 검색 결과를 제공해 주는 방식이다. OCSP는 클라이언트가 온라인 취소 상태 확인 서비스(ORS), 대리 인증 경로 발견 서비스(DPD)[7], 그리고 대리 인증 경로 검증 서비스(DPV)[8] 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. 그림 1은 OCSP의 구조를 나타낸 것이다[1,2].

인증서는 클라이언트들의 공개키 정보와 이름



〈그림 1〉 OCSP 구조



〈그림 2〉 OCSP를 이용한 인증서 검증

을 바탕으로 하여 인증기관의 비밀키로 서명을하게 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. 그림 2에서 보는 것과 같이 클라이언트는 실시간에 가까운 인증서 폐지 상태 정보를 OCSP 서버를 통해서 실시간으로 얻을 수 있다.

OCSP의 데이터 구조는 클라이언트가 서버로 보내는 요구 메시지(Request)와 서버에서 클라이언트에게 보내는 응답 메시지(Response)로 구성된다[1][2].

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].

메시지 구성은 아래와 같다.

[메시지 구성]

- tbsRequest : 버전, 요구자의 이름
- OptionalSignature : 서명용 키를 검증하기 위한 공개키의 인증 경로 등을 포함

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].

메시지 구성은 아래와 같다.

[메시지 구성]

- responseStatus : 응답의 상태
- responseByte : 구체적인 응답의 내용을 나타낸다.

3. DPD 프로토콜

DPD 서비스는 서버가 인증서 결로 구축정책에 따라서 클라이언트를 대신하여 신뢰정점(Trust Anchor)까지의 인증서 경로를 구축하는 서비스이다[그림 3].

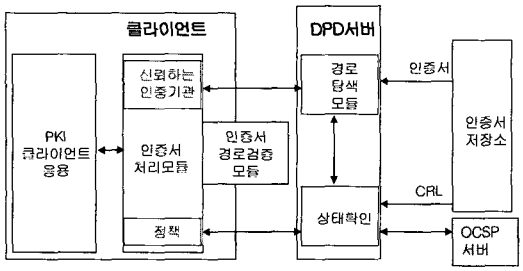
DPD 서비스에서 교환 요청 및 응답 메시지의 처리에 대한 요구사항들은 아래와 같다[1,7].

[요구사항]

(1) 인증서 경로구축 및 인증서 경로상의 인증서 각각에 대한 인증서 상태정보 요청

(2) 에러메시지를 포함하여 응답 메시지를 생성하여야 한다.

(3) 요청메시지에 포함된 사용자 인증서에 대해서 하나 이상의 인증서 경로를 획득할 수 있어야 한다.



〈그림 3〉 DPD 서버를 이용한 인증서검증

4. DPV 프로토콜

DPV 서비스는 서버가 클라이언트로부터 인증서 검증을 위임받은 후, 인증서 검증 정책에 따라서 최신의 인증서 상태정보를 이용하여 인증서 검증을 수행한다[그림 4][1,8].

[요구사항]

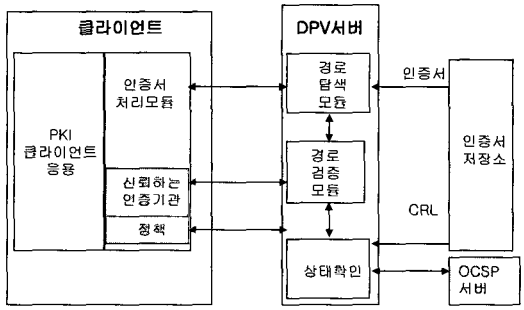
(1) DPV 서버와 DPV 클라이언트는 서로에 대한 각종 에러에 대한 응답 메시지 그리고 각종 응답 메시지를 생성하여야 한다.

(2) DPV 클라이언트는 CA이름, 인증서 일련번호 ESS의 ESSCertID, OtherSigningCertificate의 인증서 해쉬값을 사용할 수 있다.

(3) DPV 서비스는 Replay Attack을 방지할 수 있어야 한다.

(4) 인증을 위해서 응답메시지에 서버의 전자서명이 포함되어야 한다.

(5) DPV 서버는 하나 이상의 다른 DPV 서버의 서비스를 이용할 수 있도록 설정될 수 있어야 한다.



〈그림 4〉 DPV 서버를 이용한 인증서 검증

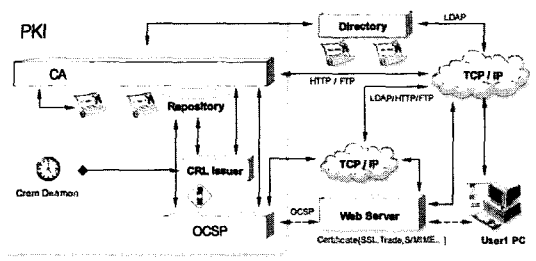
5. 단일 OCSP 문제점

OCSP의 역할은 온라인 상태에서 상대방의 인증서의 무결성을 제공해 주는 역할을 한다. 기존의 인증서 유효성 체크는 CRL이 담당했으나, 사용자의 증가와 CRL의 크기 증가로 인해 많은 부담이 되었다. 이 단점을 해결하고자 온라인 상태에서 인증서의 유효성을 체크해주는 OCSP가 등장하였다. 그러나 단일 OCSP 서버를 구축함으로써 모든 사용자가 이 서버 한대에 서비스를 요청할 경우 서버의 부담 증가로 인해 처리 시간이 증가하게 된다.

Ⅲ. 기존의 OCSP 구성도

그림 5에서는 기존의 OCSP 구성도를 보여주고 있다.

사용자 PC와 네트워크 간에는 Web 또는 Net을 통해 SSL을 적용하여 전달되는 데이터를 보호합니다. RA와 CA간, RA와 관리자간에는 RMP (Reliable Message Protocol)을 적용하여 관리자는 보안채널을 열어서 등록기관이 새로운 사용자의 등록을 받게 된다. CA와의 통신은 RFC 2510 CMP를 적용하여 사용자가 자신의 키 관리 프로그램을 이용하여 생성된 키에 대한 인증서를 안전하게 발급받을 수 있다. 디렉토리 서버는 RFC 2559 LDAP v2를 적용하여 각각의 서비스 모듈이 인증기관의 게시정보를 디렉토리로부터 가져올 수 있게 한다.



〈그림 5〉 기존의 OCSP 구성도

〈표 1〉 적용기술

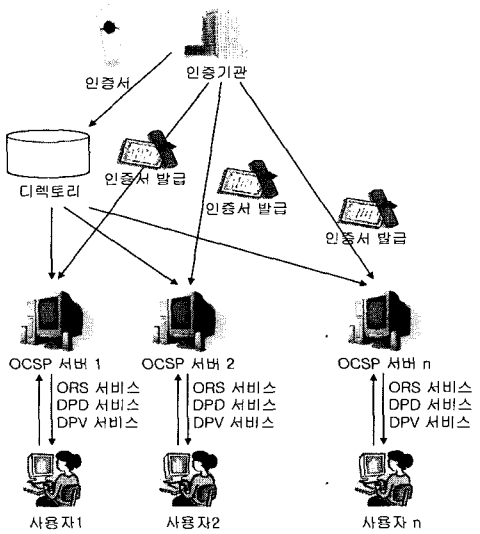
기술요소	적용기술	설명
인증서규격	X.509 v3, RFC 2459	적용된 기술은 인터넷 표준안인 RFC 2459 의 인증서 규격을 채택하여 다른 PKI 영역과의 연동을 위한 최소한의 기능을 갖춤
인증서 폐기 목록 규격	X.509 v2, RFC 2459	인증서와 같이 인터넷 표준안인 RFC 2459 가 적용되어 업체간 연동을 갖춤
인증서 관리 절차	RFC 2510, RFC2511	인증서 발급/폐기/갱신을 위한 상호 메시지 부분에서 인터넷 표준안인 RFC 2510과 실제 메시지의 전송부분의 인터넷 표준안인 draft-ietf-pkix-cmp-transport-protocols-01를 적용하여 종단간 연동성을 갖춤
인증서 검증	RFC 2459	인증서의 유효성 검증을 위한 경로인증 부분은 인터넷 표준안인 RFC 2459를 준용하여 상호인증시에 인증서의 검증에 대한 연동성을 갖춤
인증서 분배	RFC 2559, RFC 2585	발급된 인증서를 배분하기 위해 표준화된 디렉토리 구조를 통한 LDAP 지원 및 HTTP나 FTP 기타 네트워크 프로토콜을 통한 접근자를 위해 RFC 2585를 적용하여 분배 편의를 도모함
상태조회 메시지 관리 절차	RFC 2560	인증서폐기목록 대체로 사용될 상태조회서버 및 클라이언트에서 사용되는 메시지 규격은 인터넷 표준안인 RFC 2560을 준수 연동을 위한 최소한 요소를 갖춤
상태조회 서버	RFC 2560, RFC 2459	상태조회 서버를 인증기관 외부에 두고 서비스할 경우 인증기관은 확장키 사용권한을 이용해 상태조회 기능을 위임할 수 있도록 함

사용되는 기술은 표 1에서 정의한다.

Ⅳ. 분산된 OCSP 서버 모델

Ⅱ장에서 설명한 OCSP 방법을 이용하면 하나의 OCSP 서버를 이용하기 때문에 많은 사용자가 동시에 서비스를 요청할 경우에 서버의 과부하가 생길 수 있는 단점이 있다. 따라서 그림 6와 같이 인증서 저장소를 기준으로 여러 개의 OCSP 서버를 구축하고자 한다.

OCSP 서버와 사용자간의 인증서 취소 목록 체



〈그림 6〉 분산 OCSP 서버모델

크 단계는 기존의 OCSP 서버와 같다. 그러나 OCSP 서버 집중화 문제를 해결하기 위한 방안으로 인증서 저장소인 하나의 디렉토리를 기준으로 몇 개의 OCSP 서버를 두었다. 제안된 분산 OCSP 서버 모델을 구축함에 있어서 고려되어야 할 사항 세 가지가 있다.

1. 분산된 서버 정보의 동시성

본 모델은 OCSP를 이용한 실시간 인증서 상태 검증을 위한 방안이다. 이를 이용할 사용자는 여러 곳에 분산되어 있다. 따라서 각 사용자가 인증서 상태 검증을 요청할 때, 같은 곳의 OCSP 서버에 검증을 요청하지 못할 수 있다. 서로 다른 곳의 OCSP 서버에 검증을 요청할 경우, 서로 다른 곳의 OCSP 서버의 갱신 정보는 같아야 한다.

2. 갱신정보 전달의 안전성

본 모델은 인증서 저장소에서 다수의 OCSP 서버에 갱신정보(U_CRL)를 전달하는 모델이다. 따라서 갱신정보 전달에 보안성을 유지하여야 한다.

3. 특정 OCSPServer 다운문제

다수의 OCSPServer가 운영되기 때문에 특정 OCSPServer가 다운된 혹은 해킹 및 기타 네트워크 문제로 인해서 해당 사용자에 대한 서비스에 문제가 생길 수 있다. 이때는 어떻게 해야 하는지에 대한 고려도 해야 한다.

이와 같은 고려사항을 가지고 분산된 OCSP Server 모델을 설계하였다. 이 모델은 Ⅳ장에서 설명한다.

Ⅴ. 모델 분석

Ⅲ장에서 설명한 3가지의 고려하여 설계하였다.

[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

1. 분산된 서버 정보의 동시성 문제 해결 방안

본 모델의 특성상 다수의 OCSPServer가 동일한 정보를 소유하고 있어야 한다. 네트워크를 통해서 전달되는 데이터는 중간에 유실될 수도 있다. 따라서 인증서 저장소는 모든 OCSPServer의 데이터 송수신에 대한 상태를 파악하고 있어야 한다. 이를 위해서 OCSPServer는 갱신된 인증서 정보 전달에 대한 응답 메시지를 인증서 저장소에 전송할 수 있어야 한다.

인증서 저장소는 모든 OCSPServer로부터 응답

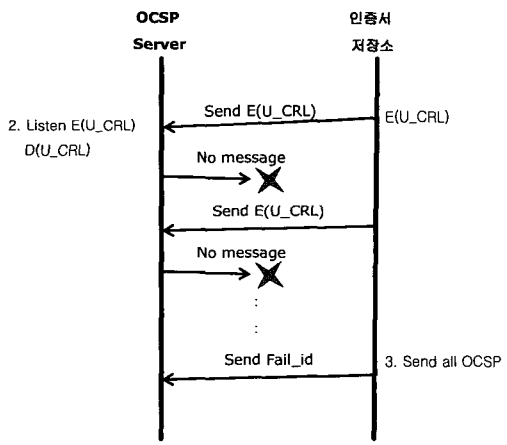
메시지를 수신한 후에 확인 메시지를 OCSPServer에 전송한다. 만약 중간에 하나의 OCSPServer로부터 응답메시지가 오지 않으면 실패 메시지를 OCSPServer에 보내게 되어 바로 전에 보냈던 갱신 정보를 모든 OCSPServer가 취소하게 한다.

즉, 모든 OCSPServer가 정보를 수신했을 경우에 갱신된 인증서 취소 목록이 채택되는 것이고 그렇지 않을 경우에는 취소가 된다. 이런 처리를 함으로써 분산된 OCSP 서버 정보의 동시성에 대한 문제를 해결하게 된다.

그림 7은 인증서 저장소에서 OCSPServer에게 갱신된 인증서 취소 정보를 보냈으나 OCSPServer의 응답이 없는 경우이다. 인증서 저장소는 일정 시간 후에 다시 한번 전송하게 되고, 그래도 응답이 없으면, 인증서 저장소는 모든 OCSPServer에게 Fail메시지를 보내게 되어 모든 OCSPServer가 바로 전에 받았던 갱신 정보를 취소하게 된다.

인증서 저장소와 OCSPServer는 주기적으로 자신의 상태 정보를 교환하게 된다.

OCSPServer는 인증서 저장소에 주기적으로 현재 자신이 소유하고 있는 인증서 취소목록의 시간을 전송하게 된다. 인증서 저장소는 이 시간 정보를 이용해서 OCSPServer의 상태를 파악할 수 있다. 구동되고 있는지와 OCSPServer가 현재 가지고 있는 갱신 정보를 알게 된다. 인증서 저장소에는 각 OCSPServer의 갱신정보를 가지고 있기 때문에 그 값을 이용해서 정보의 동시성도 파악할 수 있다.



〈그림 7〉 OCSPServer로부터 응답이 없는 경우

Send *OCSPServer(Time_Info)* to 인증서저장소

2. 갱신정보 전달의 안전성 문제 해결 방법

동시성이 모든 OCSPServer의 정보에 대한 일치성에 대한 문제라면 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[3]. 이런 비밀키를 전달하는 방식은 공개키 기반의 키 교환 방법을 이용한다. 즉, 안전한 갱신 정보 전송을 위해서 서로 간에 미리 주고받은 공개키를 이용하게 된다. 서로간의 공개키를 이용해서 비밀키를 암호화해서 전송하게 된다. 암호화된 비밀키를 수신한 후 각자 소유하고 있는 개인키를 이용해서 복호화 하게 된다. 이렇게 함으로써 갱신정보의 기밀성을 제공하게 된다.

[단계설명] : 갱신정보 송수신 과정

[1단계] *E(U_CRL)*

send *E(U_CRL)* to OCSPServer

//인증서 저장소는 갱신된 U_CRL을 암호화해서 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.

3. 특정 OCSPServer 다운문제 해결 방법

다수의 OCSPServer를 운영하기 때문에 해킹과 기타 네트워크의 문제 때문에 특정 OCSPServer가 서비스를 하지 못할 수도 있다. 이런 한두개의 OCSPServer 때문에 인증서의 유효성 체크가 불가능하다면 문제가 크다고 볼 수 있다. 따라서 본 모델에서는 특정 OCSPServer의 서비스가 불가능할 경우 사용자는 Root CA에 연락하면 Root CA는 사용이 불가능한 지역의 사용자들에게 인근의 OCSPServer을 알려주어서 문제가 생긴 OCSP Server가 정상상태가 될 때까지 인근의 OCSP Server로부터 서비스를 받도록 한다

Ⅵ. 결론

본 논문은 기존의 Root CA에서 처리하던 인증서 취소 목록에 대한 서비스를 분산된 OCSP Server 들에게 할당함으로써 중앙 집중화 현상을 분산 시켰다.

기존의 오프라인 방법의 단점은 시간이 지남에 따라서 사이즈 증가와 실시간 체크가 어렵다는 것이었다. 이를 보완하기 위해서 온라인 방법이 제안되었지만 이것 또한 인증서 취소 목록 크기 문제는 해결하지 못한다. 또한 온라인 서비스가 가능하지만 사용자 측에서는 다운로드에 대한 부담이 없지만, OCSPServer 측에서는 많은 사용자가 동시에 온라인요청이 들어왔을 때 이들을 혼자 처리해야 하는 부담이 있다. 본 논문은 이러한 부담을 해결하기 위해서 OCSPServer를 분산하는 방안을 제안하였다. 본 모델을 활용할 경우 이동성 인증성을 제공하기 때문에 이동시에도 인근의 OCSPServer를 이용하기 때문에 보다 빠르게 인증서 취소 정보를 서비스 받을 수 있는 장점이 있다. 그러나 분산된 OCSPServer는 저장소 역할이 크다 하겠다. 왜냐하면 수시로 갱신된 인증서 정보를 저장소가 분산된 모든 OCSPServer에게 전달해야 하기 때문이다. 이에 대한 문제는 향후에 해결해야 할 과제로 남아 있다.

참 고 문 헌

[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

[6] M.Myers, R.Ankney, C.Adams. "On-line Certificate Status Protocol, cersion2", IETF Draft, draft-ietf-pkix-ocspv2-01.txt. Nov, 2000

[7] M.Myers. S.Farrell, C.Adams. "Delegated Path Discovery with OCSP". IETF Draft, draft-ietf-pkix-ocsp-path00.txt. Sep, 1999

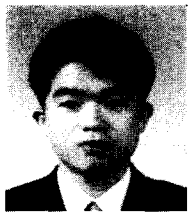
[8] M.Myers, C.Adams, S.Farrell. "Delegated Path Validation", IETF Draft. draft-ietf-pkix-ocsp-valid-00.txt. Aug, 2000

[9] RD.Pinkas. "Delegated Path Validation and Delegated Path Discovery Protocols", IETF Draft draft-ietf-pkix-dpvdld-00.txt, Jul. 2001

[10] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[11] Pinkas, D., Housley, R., "DPV and DPD Protocol Requirements", RFC 3379, September 2002.

◐ 저 자 소 개 ◑



고 훈

1998년 호원대학교 전자계산학과 졸업(학사)
2000년 숭실대학교 대학원 컴퓨터학과 졸업(석사)
2002년 숭실대학교 대학원 컴퓨터학과 박사수료
2002. 9~현재 : 대진대학교 컴퓨터공학과 초빙교수
관심분야 : 네트워크보안, 인터넷보안, 암호프로토콜, 정보보안, 무선인터넷 보안 etc.
E-mail : skoh21@daejin.ac.kr

장 의 진

1999년 9월 : 숭실대학교 컴퓨터학과 졸업(학사)
2002 년 9월 : 숭실대학교 컴퓨터학과 통신연구실(석사)
2002 년 12월~현재 : 디지캡 기술연구소 선임연구원
관심분야 : DRM, 네트워크 보안, 암호화 프로토콜, 정보보안, 인터넷보안
E-mail : neon@digitaps.com

신 용 태

1985년 2월 : 한양대학교 산업공학(학사)
1990년12월 : Univ. of Iowa 전산학(석사)
1994년 5월 : Univ. of Iowa 전산학(박사)
1994년 5월~8월 : Univ. of Iowa computer Science Dept. 객원교수
1994년 8월~1995년 1월 : Michigan State Univ Computer Science Dept. 객원교수
1995년 3월~현재 : 숭실대학교 컴퓨터학과 부교수
2000년 4월~현재 : (주) 디지캡 대표이사
관심분야 : 암호화프로토콜, 정보보안, 인터넷보안, DRM
E-mail : shin@comp.ssu..ac.kr