옵저버를 이용한 WPKI 인증서 검증방법

정회원 김 진 철*, 오 영 환**

WPKI Certificate Verification Using Observer

Jin-cheol Kim*, Young-whan Oh** *Regular Members*

요 약

이동통신 기술과 인터넷 기술을 접목시킨 무선인터넷을 이용한 다양한 서비스가 제공되고 있다. 무선 인터넷 서비스의 경우에도 유선 인터넷 환경에서와 같은 보안 알고리즘 및 인증 서비스를 활용한 서비스가 제공되어야 하나 무선 단말기의 제약으로 인해 유선 인터넷 기술을 그대로 적용하는 것은 용이하지 않다. 본 논문에서는 무선 인터넷 환경에서 인증서의 신뢰성을 보장하기 위해서 인증서의 상태를 확인하고 검증하는 방법들을 분석하고, 검증정보를 최소화하고 실시간 검증이 가능한 새로운 인증서 상태 확인 및 검증방법을 제안하였다. 제안한 검증방법은 사용자가 폐지된 인증서를 사용시 옵저버를 이용하여 핸드셰이크 과정에서 옵저버 정보를 추가하여 전송함으로써 실시간 검증 뿐 아니라 인증서 검증으로 인한 전송시간을 절감할 수 있다.

Key Words WPKI, CRL, certificate revocation

ABSTRACT

A huge growth the wireless internet services, which are based on the wireless mobile network technology and internet technology, poses demand for the end-to-end secure connections. Restrictions of wireless mobile environment and mobile devices make difficult to adapt present secure protocols to wireless internet services.

In this paper, we analyze existing certificate status verification methods in WPKI and propose a new method, adding a observer information in handshake protocol. The method with observer makes it more efficient for relying parties to verify both the current status of the X.509 certificate and the short-lived WTLS server certificate.

I 서 론

무선 단말기를 이용한 무선 인터넷 서비스의 경우에도 유선 인터넷 환경에서와 같은 보안 알고리즘 및 인증 서비스를 활용한 서비스를 제공할 수 있어야 한다. 이에 가장 큰 제약 사항은 소용량 시스템인 무선 단말기에 적용할 수 있는 보안 알고리즘과 인증서 관리 프로토콜을 들 수 있다.

WPKI(Wireless Public Key Infrastructure)는 기존의 PKI(Public Key Infrastructure)에 근간을 두면서, 무선 단말기에 탑재되는 인증서, 관련 프로토콜 등을 간결하고 단순한 형태의 규격으로 제공함으로써 무선 인터넷 구간에서도 전자서명 및 암호화를 수행할 수 있는 기반이 된다 [1].

인증서의 유효성을 확인하기 위하여 인증서의 상태를 확인하는 것은 인증서의 신뢰성을 보장하게 되며, 이를 위하여 X.509 에서는 효력정지 및 폐지 목록 (CRL : Certificate Revocation List) 및 CRL 분배점을 사용하는 것을 제시하고 있다.

무선 인터넷은 유선환경과 달리 전송속도가 낮고, 접속 유지상태가 불안하며, 접속 비용 또한 높기 때문에, 양대 진영인 WAP(Wireless Application Protocol) 진영과 Microsoft의 ME에서는 별도로 인증서 상태확인 방법을 제시하지 않고 있다 [2].

* 한전KDN(주) 기술연구소(kjc@kdn.com), ** 광운대학교 전자통신공학과 C&N Lab (yhoh@daisy.gwu.ac.kr)
논문번호 030287-0703, 접수일자 2003년 7월 3일

우리나라의 최상위 인증기관인 한국정보보호진흥원(KISA Korea Information Security Agency)는 무선 인터넷상의 공인인증 및 보안 기반을 마련하고, 나아가 인증서의 생성, 및 처리에 대한 국내 공인인증기관간의 상호 연동성 및 국제적인 호환성을 보장하기 위하여 WPKI 기술규격을 제정하였다 KISA에서 제정한 WPKI 기술규격은 전자서명 및 키분배 시 사용되는 알고리즘, 인증서를 발급받기 위한 인증서 요청양식, 그리고 발급받은 인증서를 관리하고 검증하기 위한 인증서 관리 규격 등이 있다

본 논문에서는 무선 인터넷 환경에서 인증서 상태를 확인하고 검증하는 방법들을 분석하고, 무선 인터넷 환경을 고려하여 인증서 검증정보를 최소화하고 실시간 검증이 가능한 새로운 인증서 상태 획득 및 검증 방법을 제안하고자 한다

제안한 방법은 서버와 사용자가 인증서를 사용하여 거래를 할 경우 핸드세이크(Handshake) 과정에서 사용자 단말기 또는 서버에 설치된 옵저버의 정보를 추가함으로써 인증서의 상태를 확인하고 검증할 수 있는 방법이다

본 논문은 다음과 같은 구성을 가진다 2장에서는 WPKI 인증서 상태 확인 및 검증방법을 분석하고 3장에서는 옵저버를 이용한 인증서 상태 확인 및 검증 방법을 제안하고, 4장에서는 기존 방법과 제안한 방법을 비교 및 고찰하고, 마지막으로 5장에서는 결론을 맺는다

Ⅱ WPKI 인증서 상태 확인 및 검증 방법

인증서의 폐지 여부를 확인할 수 있는 방법은 일반적으로 인증기관이 CRL을 공개하는 방법을 택하고 있다 사용자는 인증서 검증시 CRL을 수신하여 해당 인증서가 목록에 포함되는지 여부를 판단한다 이 경우 CRL의 인증서가 늘어나게 되면 부하가 커지므로 갱신을 주기적으로 하게 되어 실시간적인 서비스가 어렵게 된다 또한 해당 인증서의 검색이 손쉽게 이루어지지 않는다

무선 인터넷에서는 유선환경과 달리 전송속도가 낮고, 접속 유지상태가 불안하고, 접속 비용이 높다는 무선환경의 제약과 제한된 컴퓨팅 파워와 메모리 용량을 가지는 무선단말기의 제약으로 인하여 인증서 검증에 대한 부하를 줄이기 위한 다음과 같은 여러 가지 방법을 적용하고 있다

1 CRL 및 CRL 분배점

인증서에는 유효기간이 포함되어 있으며 그 기간 동안은 유효한 것으로 가정한다 그러나 실제 인증시의 이용에 있어 인증서 내용의 변경, 키 유출, 키 변경 등 여러 사유에 의해 유효기간 내에 인증서가 폐지될 수 있다 이런 경우 인증서의 폐지 사실을 사용자에게 알려야 하며 X.509에서 인증서 폐지 방법으로 제안된 것이 CRL이다 [3]

David A Cooper는 CRL을 제공하는 시스템에서 사용자의 평균 요구 비율보다 최대 요구 비율이 더욱 중요하다고 한다 [4] 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 시작지점이 t t+dt dt >0, v 검증 비율)

사용자의 인원수가 증가할 경우에는 증가하는 인원 수 만큼씩 식의 값에 곱해 주면 된다 사용자 N명이 t시간에 CRL을 요구하는 비율인 R(t)는 식(2)와 같다

$$R(t) = Nve^{-vt} \quad (2)$$

CRL의 그림1은 기본 CRL의 특성을 나타낸 것이며, CRL을 발표한 후 시간이 경과할 수록 사용자의 요구비율이 줄어드는 것을 알 수 있다

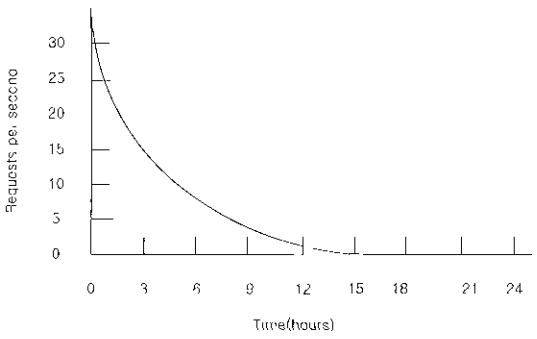


그림 1 CRL 특성

CRL은 인증기관에 의해 서명된 인증서 폐지 목록으로 시간 정보가 결합되어 공공의 저장소에 저장된다 인증서 사용자가 CRL획득 노드를 줄이기 위해 제안된 것이 CRL 분배점(distribution point)이다

인증서의 폐지 여부를 확인할 수 있는 방법은 일

반적으로 인증기관이 취소된 인증서 목록(CRL)을 공개하는 방법을 택하고 있다. 사용자는 인증서 검증시 CRL을 수신하여 해당 인증서가 목록에 포함되는지 여부를 판단한다. 이 경우 CRL의 인증서가 늘어나게 되면 부하가 커지므로 갱신을 주기적으로 하게 되어 실시간적인 서비스가 어렵게 된다. 또한 해당 인증서의 검색이 손쉽게 이루어지지 않는다.

CRL 분배점은 인증기관이 CRL을 분할하고, 각기 다른 분배점을 사용하여 각 부분들을 발행한다. CRL의 분배는 영역이나 취소 이유 등에 의해 나뉠 수 있다. 예를 들어 한 회사에 대해 CRL을 발행할 경우 인증기관이 각 부서 별로 CRL을 나누어 발행한다면 사용자는 전체 CRL을 검사하지 않고 해당 부서의 CRL을 검사하면 된다. 인증서의 취소로 나뉜다면 이름의 변화에 의해 취소된 인증서들의 CRL들과 안정성의 문제로 취소된 CRL을 나누어 발행할 수 있다. CRL 분배점은 인증서의 확장영역에 표기된다.

2. 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 CRL은 표 1 과 같다. 델타 CRL을 사용하는 PKI 시스템에서 기본CRL을 요구하는 비율은 기본 CRL 사용자 요구비율인 식(2)와 같다.[5]

$$R(t) = Nve^{-vt} \quad (2)$$

(t: 마지막으로 기본 CRL을 발급한후에 경과한 시간)

델타 CRL의 사용자 요구 비율은 다음 식(3)과 같다.

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

(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. 델타 CRL

CRL Number	base CRL	delta-CRL
1	thisUpdate=00:00 nextUpdate=04:00	thisUpdate=00:00 nextUpdate=00:10 BaseCRLNumber=1
2	.	hisUpdate=00:10 nextUpdate=00:20 BaseCRLNumber=1
.	.	.
24	.	hisUpdate=03:50 nextUpdate=04:00 BaseCRLNumber=1
25	hisUpdate=04:00 nextUpdate=08:00	hisUpdate=00:00 nextUpdate=04:10 BaseCRLNumber=1
26	.	hisUpdate=00:00 nextUpdate=04:10 BaseCRLNumber=25
.	.	.

3. OCSP

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. 사용자에서 OCSP서버에게 인증서 상태를 요구하면 서버는 인증서의 상태를 응답하는 구조로 되어 있다. IETF의 RFC 2560는 인증서 상태를 체크하는 응용 프로그램과 상태 정보를 제공하는 서버상에서 오가는 데이터의 구조를 정의하였다. [3]

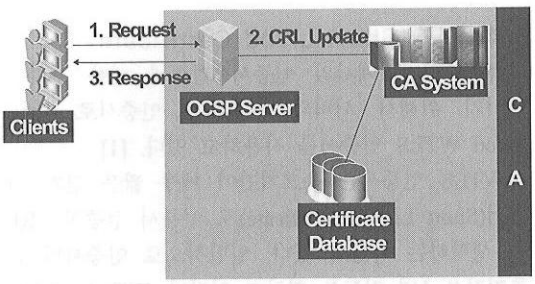


그림 2. OCSP를 이용한 인증서 검증방법

■ 요구(Request)

OCSP 메시지는 다음의 요소들을 포함한다

- 프로토콜 버전
- 서비스 요구
- 대상 인증서의 구별자
- OCSP 서버가 처리할 수 있는 확장정보(선택)

요구에 따라OCSP 다음을 확인하며 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 응답메시지의 최종 타입은 반드시 전자서명된 형식이어야 한다 서명에 이용되는 전자서명 생성키는 다음 중 하나이다

- 응답 메시지 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 세가지로 구분된다

- 양호 (good)
- 폐지 (revoked)
- 알 수 없음 (unknown)

4 SLC(Short Lived Certificate)

무선 단말기에서의 인증서 검증에 대한 부하를 줄이기 위해서 서버의 키관리용 인증서로 Short Lived WTLS 인증서를 사용하고 있다 [1]

WTLS 인증서는 유효기간이 매우 짧은 단기 인증서(Short Lived Certificate)로 인증서 검증시 CRL을 생략하는 특징이 있다 일반적으로 인증서의 유효기간은 1년 정도를 취하고 있지만, WTLS 인증서의 유효기간은 인증기관에서 CRL을 배포하는 주기인 24시간 정도로 함으로써 별도의 CRL에 대한 검증을 하지 않아도 된다는 가정이다

즉, 인증기관의 정책에 따라 24시간 또는 48시간과 같이 짧은 유효기간을 갖는 WTLS 인증서를 발급받은 후, 사용자가 별도로 폐지 또는 효력정지 요청을 하지 않는 경우, 인증기관내 WTLS 인증서를 발급하는 WTLS CA 시스템은 해당 인증서의 유효기간이 만료되기 전에 자동으로 인증서를 생신한다

또한 가입자가 인증서에 대한 효력정지를 요청하면 WTLS CA시스템은 해당 가입자 정보의 인증서 효력정지 필드에 표시하여 인증서를 자동 갱신할 때에 해당 인증서가 해당 인증서가 갱신되지 않도록 한다

그림 3 WTLS 인증서

Ⅲ 옵저버를 이용한 WPKI 인증서 검증 방법

2장에서 설명한 WPKI 인증서 상태 확인 및 검증방법들은 각각 실시간 검증이 어렵거나 또는 특정 공격에 약하다는 문제점이 있다 본 논문에서는 이러한 문제점을 해결하기 위해서 옵저버를 이용한 새로운 인증서 상태 확인 및 검증방법을 제안한다 제안한 방식은 사용자 단말기에 옵저버를 설치하여 인증서에 대한 실시간 검증이 가능하므로 적시성을 개선할 수 있으며 특히 별도의 인증서 검증과정이 없는 WTLS 인증서 검증 방법인 SLC의 보안적인 측면과 OCSP의 문제점을 개선할 수 있다

[가 정]

■ 서버는 인증기관으로부터 사용자의 인증서 검증을 위한 CRL을 일정시간 주기로 배포받는다

■ 서버는 사용자와 핸드세이크(Handshake) 과정 중 키 분배용 WTLS 인증서를 사용한다

■ 서버 또는 사용자는 등록기관에 인증서 폐지를 요청 한다

■ 등록기관은 인증기관에게 서버 또는 사용자의 인증서 취소를 통보한다.

■ 등록기관은 인증서 폐지를 요청한 서버 또는 사용자의 단말기에 설치된 옵저버에게 서버 또는 사용자가인증서 취소 요청을 한 사실을 통보하고 옵저버 ID를 부여 및인증기관에 인증서 취소 통보 날짜 및 시간을 기록한 TIMESTAMP를 옵저버에 전송한다.

[핸드세이크(Handshake) 절차]

서버와 사용자가 인증서를 사용하여 거래를 할 경우 서버와 사용자간 핸드세이크 (Handshake)의 절차는 다음과 같다.

[단계 1]

■ 사용자는 client_hello메시지를 전송한다.

[단계 2]

■ 서버는 Server_hello 메시지를 사용자에게 전송한다.

[단계 3]

■ 서버는 메시지키 분배용 WTLS 인증서가 포함된 Server Certificate메시지를 사용자에게 전송한다.

[단계 4]

■ 서버는 비밀키와 옵저버 정보를 자신의 개인키로 전자서명한 데이터가 포함된 Server Key Exchange메시지를 사용자에게 전송한다.

■ 만일, 서버의 인증서가 폐지된 인증서인 경우 옵저버 정보는 등록기관으로부터 부여받은 옵저버 ID, 인증서 취소 통보날짜 및 시간을 기록한 Timestamp가 메세지 header부분에 삽입된다.

■ 이런 메시지를 수신한 사용자는 header부분에 서버의 개인키로 서명된 데이터를 WTLS인증서의 공개키로 복호화하여 추가된 옵저버의 정보를 확인함으로써 서버의 인증서가 만료된인증서임을 검증할 수 있다.

[단계 5]

■ 서버는 Server Hello Done 메시지를 전송한다..

■ 만일 서버의 인증서가 폐지되었을 때 이를 검증한 사용자는 Alert 메시지를 보냄으로써 서버의 인증서가 폐지되었음을 알리고 거래를 중지함을 Alert 메시지의 Body 부분에 삽입하여 전송한다.

[단계 6]

■ 사용자는 인증서 URL정보, 공개키 등의 데이터가 포함된 Client Certificate메시지를 전송한다.

[단계 7]

■ 사용자는 옵저버 정보를 서버의 공개키로 암호화한 데이터가 포함된 Client Key Exchange 메시지를 전송한다. 이 단계에서 사용자는 세션키를 생성하는데 이용되는 임의의 비밀정보인 48바이트 pre_master_secret을 생성한다. 그런 뒤 선택된 공개키 알고리즘에 따라 pre_master_secret 정보를 암호화하여 서버에 전송한다.

■ 만일, 사용자의 인증서가 폐지된 인증서인 경우 옵저버 정보는 등록기관으로부터 부여받은 옵저버 ID, 인증서 취소 통보날짜 및 시간을 기록한 Timestamp가 메세지 header부분에 삽입된다.

■ 이런 메시지를 수신한 서버는 header부분에 서버의 개인키로 복호화하여 추가된 옵저버의 정보를 확인함으로써 사용자의 인증서가 만료된 인증서임을 검증할 수 있다.

[단계 8]

■ 사용자는 Finished 메시지를 서버에게 전송한다.

[단계 9]

■ 서버는 Finished 메시지를 사용자에게 전송한다.

■ 만일,사용자의 인증서가 폐지되었을 때 이를 검증한 서버는 Alert 메시지를 보냄으로써 사용자의 인증서가 폐지되었음을 알리고 거래를 중지함을 Alert 메시지의 Body 부분에 삽입하여 전송한다.

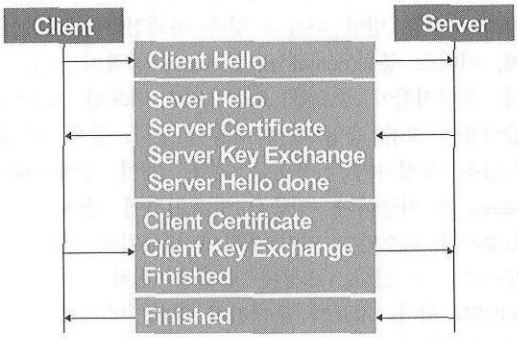


그림 3. 핸드세이크 절차 흐름도

Ⅳ 비교 및 고찰

PKI와 WPKI의 명백한 차이점은 인증서를 검증하는데 있다 첫째, OCSP사용에 있어서 유선에서는 Private Extension필드의 발급자 정보접근(Authority Information Access)필드를 사용하여 OCSP사용을 권고하고 있는 반면 무선에서는 OCSP를 사용할 경우 Domain Information 필드의 사용을 강하게 권고하고 있다

둘째, 현 기술로 단말기에서 CRL 혹은 OCSP를 사용한 검증이 용이하지 않기 때문에 WAP에서는 기존 X.509V3인증서의 기본필드와 유사한 WTLS 인증서를 정의하여 CA가 24시간마다 short lived 형태의 WTLS인증서 발행하여 CRL효과를 낼 수 있는 WTLS인증서 사용을 권고하고 있다

셋째, 유선에서는 전체 CRL를 가져와서 인증서 상태를 검증하지만 무선에서는 CRL를 잘게 자른 후 최근 CRL를 가져와서 검증할 수 있는 메카니즘인 Delta CRL 사용을 선택 사항으로 추가하여 정의하였다 인증서 요청형식은 유선에서 사용되고 있는 PKCS#10, RFC2511를 사용하는 것이 아니라 WAP에 기반한 SignText함수를 정의하여 무선환경에 맞는 인증서 요청 및 관리 프로토콜 규격을 정의하여 사용을 권고 있다

CRL 분배점은 첫째, 해당 인증서에 대한 실시간 확인이 어렵다는 점과 둘째, CRL의 크기에 따라 전송시간이 길어질 수 있다는 단점이 있다

Delta CRL을 사용하면 기존CRL방식에 비해 CRL검증 시간 단축 및 사용자의 최대 요구 비율을 줄일 수 있고, 트래픽 지연문제를 해결하여 적시성에 효율적인 성질을 가지고 있다 하지만 해당 인증서에 대한 실시간 확인은 역시 어렵다

OCSP는 실시간으로 인증서를 검증할 수 있다는 장점이 있는 반면 다음과 같은 문제점이 있다 첫째, 서비스 불능(denial of service) 공격에 노출되다 응답시간이 중요한 요소이므로 과도한 요청이 들어올시 오류 응답 발생 확률이 높다 둘째, 미리 응답을 생성하여 사용하는 경우, 재연 공격(replay 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 있다 셋째, HTTP상에서 OCSP를 구현할 경우 HTTP 캐쉬의 신뢰성이 고려되어야 한다

제안한 방식은 첫째, 사용자 단말기에 유저비를 설치하여 인증서에 대한 실시간 검증이 가능하므로 적시성을 개선할 수 있다 둘째, 별도의 인증서 검증과정이 없는 SLC방식인 서버용 WTLS 인증서에 대한 검증도 가능하다 셋째, 인증기관이 배워 전체 WTLS 인증서를 생신시켜야 하는 분편함도 해소시킬 수 있다 넷째, 인증서 검증시 매번 인증기관의 OCSP서버에 인증서 검증을 요구하고 응답받음으로 발생되는 신송시간을 줄일 수 있을 뿐 아니라 OCSP서버로의 트래픽 집중 및 보안 문제점을 보완할 수 있다

Ⅴ 결 론

무선 인터넷은 유선환경과 달리 전송속도가 낮고, 접속 유지상태가 불안하며 접속 비용 또한 높기 때문에 인증서 검증이 용이하지 않다 본 논문은 CRL 분배점, Delta CRL, OCSP등의 WPKI 인증서 상태 확인 및 검증방법을 분석하였다 인증서 검증정보를 최소화하고 실시간 검증이 가능한 유저비를 이용한 인증서 확인 및 검증 방법을 제안하고 기존의 방법과 비교 및 고찰하였다 제안한 인증서 검증방법을 인증서 사용자와 서버간 핸드세이크 과정에 적용함으로써 적시성과 보안적인 측면 및 성능 면에서 향상됨을 알 수 있다

참 고 문 헌

[1] 김현희, "WPKI 기반의 무선 공인인증 서비스 개요", *지급결제와 정보기술*, 2003

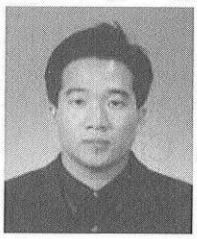
[2] 이석래, "무선보안기술동향", *전자서명 인증센터*, 한국정보보호진흥원, 2002

[3] 채승화, "CRL 분배 및 온라인 인증서 상태 확인 비교", *전자서명 인증관리센터*, 한국정보보호진흥원, 1999

[4] D A Cooper, "A Model of Certificate Revocation," *Proceedings of the 15th Annual Computer Security Application*, pp 256-263, 1999

[5] D A Cooper, "A More Efficient Use of Delta-CRL," *In Preceeding of the 2000 IEEE Symposium on Security and Privacy*, pp 190-202, 2000

김 진 철(Jin-cheol Kim) 정회원



1995년 2월 : 광운대학교 전자통신공학과 졸업
1997년 2월 : 광운대학교 전자통신공학과 석사
1996년 12월~현재 : 한전KDN 기술연구소 근무
2000년 3월~현재 : 광운대학교 전자공학과 박사과정
<관심분야> PKI, WPKI, USN, MANET

오 영 환(Young-whan Oh) 정회원
한국통신학회 논문지 제27권 제 7C호 참조