WAVE 시스템 OCSP 서버를 위한 CRL 업데이트 프로토콜

최범진*, 김은기*
*한밭대학교 정보통신공학과
e-mail : bj20428@naver.com

A CRL Update Protocol for an OCSP Server of WAVE System

Beom-Jin Choi*, Eun-Gi Kim*
*Dept. of Information and Communication Engineering, Han-Bat National University

요 약

WAVE(Wireless Access in Vehicular Environment)에서 V2V(Vehicle to Vehicle) 통신 시 OBU(On Board Unit)인 자동차 단말은 수신한 정보가 제대로 된 정보인지를 확인하는 과정에서 공인인증서가 필요하다. 동시에 자동차 단말은 이 공인인증서의 상태가 유효한 지를 확인해야 한다. 이것을 확인하는 방법은 자동차 단말이 도로변에 설치돼 있는 RSU(Road Side Unit)인 OCSP(Online Certificate Status Protocol) 서버에게 공인인증서의 상태 확인 요청을 하는 것이다. OCSP 서버는 자동차 단말의 요청에 응답하기 위해서 인증서 폐지 목록인 CRL(Certificate Revocation List)을 가지고 있어야 한다.

본 논문에서는 WAVE 시스템의 OCSP 서버가 공인인증서 상태 정보를 자동차 단말로 알려줄 수 있도록 하기 위해 CA(Certificate Authority)의 CRL 저장소로부터 CRL 을 업데이트 하는 프로토콜을 제안한다. OCSP 서버가 CRL 을 업데이트 할 때, OCSP 서버가 가지고 있는 CRL 과 CRL 저장소가 가지고 있는 CRL 의 값을 비교하여 두 값이 같은 경우에는 CRL 을 업데이트 하지 않도록 한다. OCSP 서버가 선택적으로 CRL 을 업데이트 함으로써 불필요한 부하를 줄일 수 있을 것으로 기대된다.

1. 서론

자동차 수가 증가하면서 교통혼잡, 교통사고 등의 문제가 심각해지고 있다. 이러한 문제에 대한 해결책으로써 ITS(Intelligent Transport Systems)가 나타났다. ITS 는 교통수단 및 교통시설과 첨단 IT 기술이 융합된 교통체계이다[1]. ITS 를 통해서 교통에 대한 안전성 및 편리성 등을 향상시킬 수 있다. ITS 기술 중 WAVE 기술이 연구, 개발되고 있다. WAVE 기술은 V2I(Vehicle to Infrastructure), V2V 통신이 모두 가능하며 응답시간이 빠른 무선 통신기술이다. V2V 통신 시에 자동차 단말은 수신한 정보가 변조되지 않았는지 확인하는 과정이 필요하고 이때 공인인증서가 사용된다. 또한 자동차 단말은 사용하려는 공인인증서가 유효한 인증서인지를 확인해야 한다. 공인인증서의 유효성을 확인하는 방법은 자동차 단말이 도로변에 설치되어 있는 RSU 인 OCSP 서버에게 공인인증서의 상태 확인 요청을 하는 것이다. OCSP 서버는 자동차 단말의 요청에 응답하려면 인증서 폐지 목록인 CRL 을 보유하고 있어야 한다.

본 논문에서는 WAVE 시스템의 OCSP 서버가 CRL 을 업데이트 하는 프로토콜을 제안한다. OCSP 서버가 CRL 을 업데이트 할 때 OCSP 서버가 가지고 있는 CRL 과 CRL 저장소가 가지고 있는 CRL 의 해시 값을 비교하여 두 값이 같은 경우는 OCSP 서버가 CRL 을 업데이트 하지 않도록 한다. OCSP 서버가 선택적으로 CRL 을 업데이트 함으로써 불필요한 부하를 줄일 수 있을 것으로 기대된다.

본 논문의 2 장에서는 제안하는 주제에 대한 전반적인 내용을 언급하고 3 장에서는 결론을 다룬다.

2. 본론

OCSP 서버가 CRL 을 업데이트 할 수 있는 메커니즘에는 LDAP(Lightweight Directory Access Protocol), FTP(File Transfer Protocol), FTPS(FTP over SSL), HTTP(Hyper-Text Transfer Protocol) 등이 있다[2, 3]. 이러한 프로토콜들은 범용 사용을 목적으로 하기 때문에 프로토콜의 크기가 크며 TLS 와 같은 추가적인 시스템이 필요하다. 본 논문에서는 추가적인 시스템이 필요 없고 프로토콜의 크기가 작은 WAVE 시스템 OCSP 서버용의 CRL 업데이트 프로토콜을 제안한다.

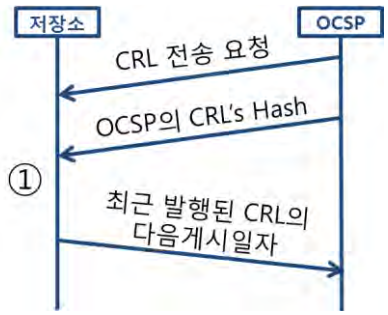
OCSP 서버가 CRL 저장소와 통신하며 CRL 을 업데이트 할 때, 둘 사이에 상호인증이 이루어져야 한다. OCSP 서버가 CRL 저장소를 인증하지 않으면 OCSP 서버는 Pharming 공격에 노출될 수 있고 잘못된 CRL 을 업데이트 할 수도 있다. CRL 저장소가 OCSP 서버

를 인증하지 않으면 CRL 저장소는 DOS(Denial Of Service) 공격에 노출될 수 있으며 OCSP 서버는 CRL 을 업데이트 하지 못할 수도 있다. 따라서 제안하는 방법에서는 OCSP 서버와 CRL 저장소 간에 상호인증을 한다.

OCSP 서버는 CA 의 CRL 발행 주기에 따라서 CRL 저장소로부터 CRL 을 업데이트 한다[2, 4].

OCSP 서버는 최근에 발행된 CRL 의 해시 값과 자신이 가지고 있는 CRL 의 해시 값이 같다면 CRL 을 업데이트 하지 않는다. CRL 의 내용 중에서 해시를 하는 부분은 “폐지된 인증서의 일련번호”, “폐지 일자” 등이다. 만약 OCSP 서버가 최근에 발행된 CRL 을 업데이트 하지 않는다면 CRL 저장소는 OCSP 서버에게 최근 발행된 CRL 의 다음게시일자를 알려준다. OCSP 서버가 최근 발행된 CRL 의 다음 게시 일자를 모르기 때문이다. 그럼으로써 OCSP 서버는 다음 CRL 업데이트 요청을 할 수 있게 된다.

다음 (그림 1)은 제안하는 CRL 업데이트 방식이다.



(그림 1) CRL 업데이트 방식

(그림 1)에 대한 설명은 다음과 같다.

1) CRL 업데이트 시간이 되면 OCSP 서버가 저장소로 CRL 업데이트 요청을 한다
2) 동시에 OCSP 서버는 자신이 가지고 있는 CRL 의 해시 값을 저장소로 전송한다.
3) 저장소는 ①의 처리를 하는데 ①은 두 가지 경우로 나눌 수 있다.
   3-1) 저장소가 가지고 있는 최신 CRL 의 해시 값과 OCSP 서버가 보낸 CRL 의 해시 값이 동일한 경우
   3-2) 저장소가 가지고 있는 최신 CRL 의 해시 값과 OCSP 서버가 보낸 CRL 의 해시 값이 다른 경우
4) 저장소는 3)의 3-1)인 경우에 저장소에 게시된 최신 CRL 의 다음게시일자 정보를 OCSP 서버로 전송해 준다. 3-2)인 경우에 저장소는 OCSP 서버가 요청한 CRL 을 전송한다.
5) OCSP 서버는 3)의 3-1)인 경우 CRL 을 업데이트 하지 않는다. 3-2)인 경우는 정상적으로 CRL 을 업데이트 한다.

RSU 인 OCSP 서버들이 도로변에 다수 설치되어 있을 수 있다. 이 경우 OCSP 서버들이 CRL 을 업데이트 할 때 CRL 저장소로 트래픽이 집중되는 문제가 발생한다. 따라서 이러한 트래픽을 분산시킬 필요가 있다. 제안하는 논문에서는 각 OCSP 서버들이 CRL 업데이트 시간이 되면 임의의 시간을 휴식한 후에 CRL 저장소로 접근하도록 한다.

3. 결론

본 논문은 WAVE 시스템의 OCSP 서버가 CRL 을 업데이트 하는 프로토콜을 제안한다. OCSP 서버의 CRL 업데이트 시기는 CRL 발행 주기에 따른다. OCSP 서버는 자신이 가지고 있는 CRL 의 해시 값과 CRL 저장소가 가지고 있는 CRL 의 해시 값이 같다면 CRL 저장소로부터 CRL 을 업데이트 하지 않는다. OCSP 서버는 도로변에 다수 설치되어 있을 수 있는데, 이 경우 CRL 업데이트 시에 트래픽이 증가될 수 있다. CRL 업데이트 시기에 CRL 저장소로 몰리는 트래픽을 분산하기 위하여 OCSP 서버들은 CRL 업데이트 시기가 되면 임의의 시간을 휴식한 후에 저장소로 접근하도록 한다. OCSP 서버가 선택적으로 CRL 을 업데이트 함으로써 불필요한 부하를 줄일 수 있을 것으로 기대된다.

감사의 글

본 연구는 교육부와 한국연구재단의 지역혁신인력양성사업(No. 2013H1B8A2032154) 및 미래창조과학부와 연구개발특구진흥재단의 연구개발특구육성사업으로 수행된 연구결과임.

참고문헌

[1] http://www.its.go.kr/opInfo/info.jsp.

[2] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC5280, IETF, May 2008.

[3] R. Housley, P. Hoffman, “Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP”, RFC2585, IETF, May 1999.

[4] Joshua Davies, “Implementing SSL/TLS Using Cryptography and PKI”, Wiley Publishing, Inc., 2001.