WAVE 시스템을 위한 차량용 CRL 다운로드 프로토콜

선설희*, 유권정*, 최범진*, 김은기*
*한밭대학교 정보통신공학과
e-mail : whrhghgh@naver.com

The CRL Download Protocol for Vehicle in WAVE System

Seol-Hee Sun*, Kwon-Jeong Yoo*, Beom-Jin Choi*, Eun-Gi Kim*
*Dept. of Information and Communication Engineering, Han-Bat National University

요 약

WAVE 기술은 차량이 고속 이동환경에서 차량간 또는 차량과 인프라간 패킷을 짧은 시간 내에 주고 받을 수 있는 무선통신 기술이다. 본 논문의 목적은 차량이 WAVE 시스템에서 통신 할 때 상대방의 인증서가 폐기 되었는지 확인하기 위한 CRL(Certificate Revocation List) 다운로드 프로토콜을 설계하는 것이다. CRL 다운로드 프로토콜은 WAVE 시스템 환경에 맞추기 위해 TCP(Transmission Control Protocol)가 아닌 UDP(User Datagram Protocol) 상에서 동작한다. 그리고 보안기능을 지원하기 위해 ECDSA 를 사용하여 상호 인증을 하고 ECIES 를 사용하여 인증서의 기밀성을 보장한다. 또한 이 프로토콜은 MAC 을 CRL 데이터에 붙여 데이터의 무결성을 보장하고, UDP 상에서 동작할 때 발생할 수 있는 데이터의 손실을 줄이기 위해 에러 및 흐름제어 방식으로 Selective repeat ARQ 를 사용한다.

1. 서론

최근에 주행 중인 차량정보와 주변 교통 정보를 수집하기 위해서 WAVE(Wireless Access in Vehicular Environments) 시스템이 개발되고 있다. 본 연구에서는 WAVE 시스템에서 차량이 CA(Certificate Authority)로부터 CRL 을 다운받을 때 기밀성과 무결성을 보장하는 프로토콜을 설계하였다.

CRL 다운로드 프로토콜은 ISP(Initial Setup Protocol), DTP(Data Transfer Protocol), RLP(Record Layers Protocol)로 구성되어 있다.

ISP 에서는 Diffie-Hellman Key Exchange 알고리즘을 이용하여 공유된 비밀 키를 생성하고, ECDSA(Elliptic Curve Digital Signature Algorithm) 를 사용하여 상호인증을 하고 ECIES(Elliptic Curve Integrated Encryption Scheme)를 사용하여 인증서의 기밀성을 보장한다.

DTP 는 CRL 을 전송하는 프로토콜로서, 데이터의 무결성을 보장하기 위하여 CRL 뒤에 MAC(Message Authentication Code)을 붙여서 RLP 로 전송한다.

RLP 에서는 ISP 나 DTP 에서 수신한 데이터를 RLP 의 MTU(Maximum Transmission Unit)만큼 fragmentation 시킨 후, 각 fragment 에 RLP Header 를 붙여 하위 계층으로 전송한다. 그리고 전송과정에서 패킷들의 손실을 줄이기 위해 Selective repeat ARQ(Automatic Repeat Request) 방식의 에러제어 및 흐름제어를 지원한다.

본 논문의 2 장에서는 ISP, DTP, RLP 의 동작을 자세히 설명하고, 3 장에서는 결론을 다룬다.

2. 본론

2.1 ISP

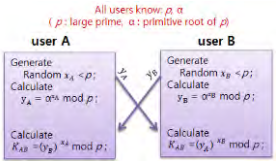
Server 와 Client 간의 안전하고 신뢰도가 높은 통신을 하기 위해서는 상호 인증이 필요하다. ISP 는 상호 인증을 수행하기 위해 공유된 비밀 키를 생성하고 전자서명, 인증서의 암호화 등을 거쳐 ISP data 뒤에 Authentication Code 를 추가한다. 다음 (그림 1)은 ISP data 에 Authentication Code 가 추가되는 것을 나타낸 그림이다.

(그림 1) ISP : Add Authentication Code

2.1.1 Diffie-Hellman Key Exchange Algorithm

두 종단이 공유된 비밀 키를 생성하기 위해서는 Diffie-Hellman Key Exchange 방식을 사용한다. 이 방식은 p 와 α를 먼저 공유해야 하는데, p 는 큰 소수이고 α는 p 의 원시 근이다.

각 종단에서는 p 보다 작은 임의의 개인 키를 생성한다. 그리고 p, α, 개인 키를 이용하여 각자의 공개 키를 생성한다. 이 공개 키를 서로에게 전송한 후, 수신한 상대방의 공개 키와 자신의 개인 키, p 를 이용함으로써 비밀 키를 생성하게 된다[2]. Diffie-Hellman Key Exchange 의 과정은 (그림 2)와 같다.

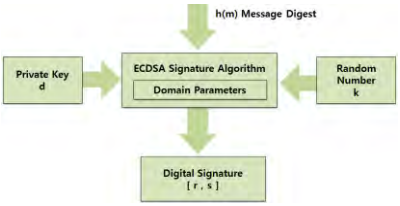


(그림 2) Diffie-Hellman Key Exchange

2.1.2 ECDSA 와 ECIES

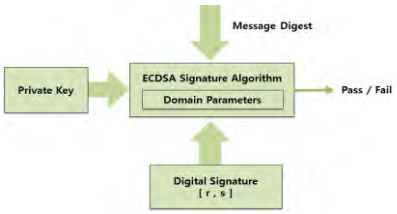
차량과 CA 는 전자서명을 통해 서로에게 본인임을 증명함으로써 신뢰도를 높인다. CRL 다운로드 프로토콜에서는 타원곡선 암호(Elliptic curve cryptosystem)를 이용한 전자서명 방식인 ECDSA 를 이용한다. 타원곡선 암호 방식은 다른 암호 방식에 비해 키의 길이가 짧기 때문에 암호화, 복호화가 빠르다. 그리고 더욱 강력한 보안성을 가지는 특징이 있다.

메시지에 서명을 하기 위해서는 임의의 개인 키를 생성한 후, ECDSA parameters 를 이용하여 공개 키를 생성한다. 그리고 random number k, ECDSA parameters, 메시지의 hash 값과 개인 키를 이용하여 메시지의 서명인 r, s 를 생성한다[1]. 이 r 과 s 는 ISP 의 Authentication Code 에 포함된다. 다음 (그림 3)은 ECDSA 의 서명이 계산되는 과정을 나타냈다.



(그림 3) ECDSA 서명 계산 과정

ECDSA 의 서명 검증은 증명자가 동일한 hash 알고리즘을 사용하여 메시지를 hash 한 후, 생성된 hash 값, 서명자의 공개 키와 s 를 계산한 값을 수신된 r 과 비교하여 이루어진다[1]. ECDSA 의 서명 값으로 서명을 검증하는 과정은 (그림 4)와 같다.

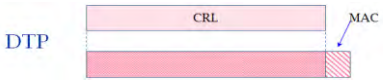


(그림 4) ECDSA 서명 검증 과정

상호 인증 과정에서 차량은 CA 의 공개 키를 알고 있다고 가정한다. 차량이 CA 로부터 인증을 받기 위해서는 CA 에게 차량의 인증서를 보내 주어 CA 가 차량의 공개 키를 알 수 있게 해야 한다. 이때, 차량의 인증서는 ECIES 를 사용하여 암호화된다. ECIES 는 공개키 암호화 방식으로 메시지를 암호화 시키고, 무결성을 위해 암호화된 인증서의 MAC 값을 계산한다. 여기서 ECIES parameter, 암호화된 인증서와 MAC 값은 Authentication Code 에 포함된다. CA 는 수신한 차량의 인증서를 Authentication Code 와 개인 키로 계산하여 복호화 할 수 있다.

2.2 DTP

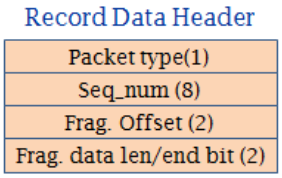
DTP 는 CRL 이 전송되는 프로토콜로서 데이터의 무결성을 보장하기 위해 MAC 을 추가한다. 이때, MAC key 는 ISP 에서 공유한 비밀 키의 일부를 이용한다. 그리고 Reply 공격을 방지하기 위하여 MAC 에 사용되는 메시지에 sequence number 를 추가한다. 다음 (그림 5)은 DTP data 에 MAC 이 추가되는 것을 나타낸 그림이다.



(그림 5) DTP : Add MAC

2.3 RLP

(그림 1)과 (그림 5)와 같이 ISP 또는 DTP 에서 전송할 데이터들의 format 이 갖추어지면 RLP 로 데이터가 전송된다. 그리고 수신한 데이터를 RLP 의 MTU 만큼 fragmentation 시킨 후, 각 fragment 에 Record Data Header 를 붙여 하위 계층으로 전송한다. RLP 의 Record Data Header 는 다음 (그림 6)과 같다.



(그림 6) RLP Header

IP 계층에서 fragment 의 최대 크기는 512byte 이다[3]. 따라서 IP header, UDP header, RLP header 를 제외한 나머지 크기가 RLP 의 MTU 가 된다.

UDP 는 TCP 와 다르게 에러제어와 흐름제어를 하지 않는다. 따라서 RLP 는 UDP 상위의 전송과정에서 발생할 수 있는 데이터의 손실을 줄이기 위해 Selective repeat ARQ 방식의 에러 및 흐름제어를 지원한다.

데이터의 전송이 실패 시, N 번(system parameter)의 재전송이 이루어지고 N 번을 초과한다면 데이터의 전송을 포기하고 상위 계층에 이를 고지한다.

3. 결론

본 논문에서는 WAVE 시스템 환경에서 차량이 CA 로부터 CRL 을 다운로드 하는 프로토콜을 설계하였다. WAVE 시스템에 맞춰 통신속도를 높이기 위해 프로토콜을 UDP 상위에서 동작시킴으로써 TCP 에서 연결설정으로 인해 발생할 수 있는 통신 지연 문제를 해결하고자 하였다. CRL 다운로드 프로토콜의 전체적인 기능은 먼저 ISP 에서 보안이 강력한 Elliptic curve cryptosystem 의 ECDSA 로 상호인증을 하고, ECIES 로 인증서를 암호화한다. 또한 상호인증 과정에서 Diffie-Hellman Key Exchange Algorithm 으로 미리 공유된 비밀키의 일부를 DTP 에서 MAC key 로 사용함으로써 데

이터의 기밀성과 무결성을 보장할 수 있게 하였다. 그리고 RLP 에서 Selective repeat ARQ 를 이용하여 데이터의 에러 및 흐름제어 기능을 추가하였다.

감사의 글

본 연구는 교육부와 한국연구재단의 지역혁신인력양성사업(No. 2013H1B8A2032154) 및 중소기업청에서 지원하는 2014 년도 산학연협력 기술개발사업(No. C0199293)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] S. Blake-Wilson, G. Karlinger, T. Kobayashi, Y. Wang “Using the Elliptic Curve Signature Algorithm (ECDSA) for XML Digital Signatures”, RFC 4050, IETF, April 2005

[2] Pravir Chandra, Matt Messier, John Viega “Network Security with OpenSSL”, June 2002

[3] Behrouz A. Forouzan “TCP/IP Protocol Suite, Fourth Edition”, McGRAW HILL INTERNATIONAL EDITION, 2010