익명성을 보장하는 차량 인증서 발급 방안 설계

김택중*, 전문석*
*숭실대학교 컴퓨터학과
e-mail:kimmycode23@ssu.ac.kr

A Design of Vehicle Certification to Pseudonym

Taekjung Kim*, Moon-Soeg Jun*
*Dept of Computer Science & Engineering, Soongsil University

요 약

본 논문은 지능형 교통시스템의 상용화에 따라 점차 주목받고 있는 차량 간의 통신 과정에서 안정성이 필수적이라고 판단하였다. 그 중 현재 차량 간의 통신 과정에서 필수적으로 활용되고 있는 인증서에 대한 취약점에 주목하였고 본 논문에서는 기존의 인증서 발급 절차의 위협으로 판단되는 CA의 인증서 발급절차를 개선함으로써 CA접근에 대한 위협으로부터 안전할 수 있는 방안을 제안한다.

1. 서론

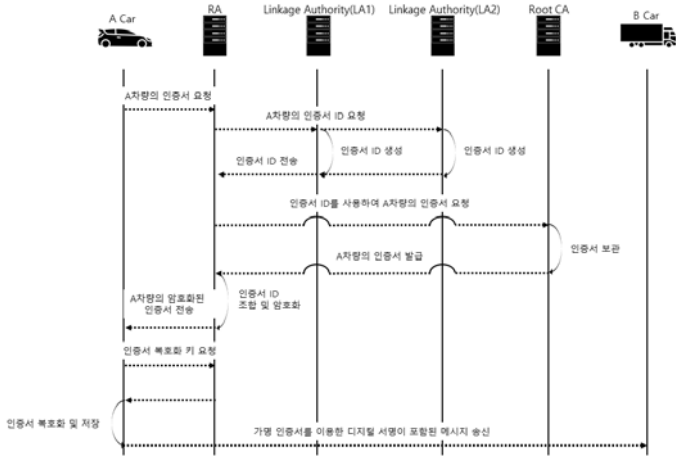
지능형 교통시스템은 고속으로 이동하고 있는 차량에게 현재 도로의 상황을 전달하여 실시간 교통정보를 제공함으로써 차량 추돌 방지부터 인명사고 예방 등 다양한 방면에 활용될 것으로 예측된다. 무선통신 기술 활용이 증가함에 따라 중간자(Man in the Middle, MITM) 공격과 재전송 공격들도 증가하여 차량에 관련한 보안상의 위험이 노출되었다. 만약 차량 충돌 사고의 메시지가 제 3자에게 노출되어 변조된다면 이에 대한 사실을 알지 못하는 주변 차량은 더 큰 사고가 발생 할 수 있다. 이러한 상황을 방지하기 위해 현재 차량 통신의 시스템은 신뢰성 있는 인증을 지향하는데 고속으로 이동하는 차량의 특성 상 인증서를 통한 서로의 인증을 기반으로 하고 있다[1].

인증서는 접근이 용이하고, 쉽게 복사할 수 있는 장점이 있지만 인증서 관리를 소홀히 하거나, 클라우드 등과 같은 온라인에 보관한다면 해킹과 바이러스 같은 공격으로 인해 인증서 파일을 탈취 당할 수 있는 위험이 있다. 실제로 인증서 탈취에 관련된 사고는 많이 발생하고 있다. 2016년 9월 날씨에 관련된 정보를 담고 있는 사이트를 이용했다가 해당 웹 사이트를 통해 악성코드가 침입함으로써 사용자의 PC가 공격자로부터 해킹당하여 공인인증서가 유출되어 금전적인 피해가 발생하거나 PC의 제어권한을 완전히 장악당한 사례가 있다[2]. 이와 같은 인증서 탈취가 고속으로 이동하는 차량에서 이루어지게 된다면 운전자의 생명과 직결되는 위험 상황에 놓일 수 있다. 또한 차량 통신의 경우 차량의 ID를 탈취당하지 않아야하기 때문에 차량 통신에서의 인증서는 익명으로 이루어져야한다.

2. 본론

2.1 CAMP VSC3

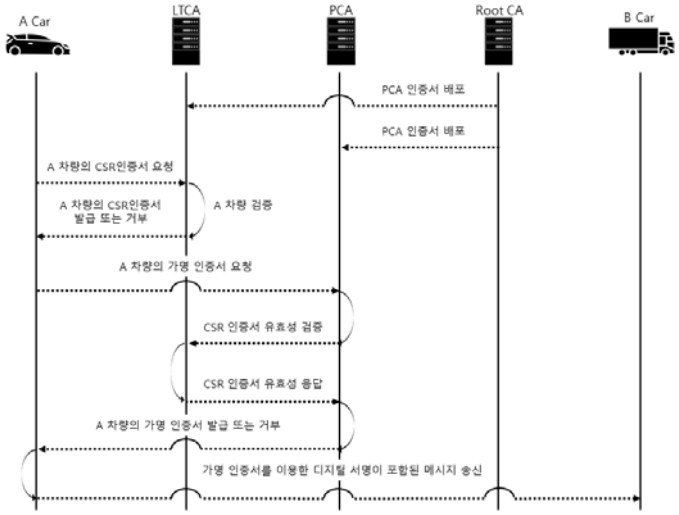
Crash Avoidance Metrics Partnership(CAMP)는 미국의 교통부(Department of Transportation, DOT)와 그 산하기관인 National Highway Traffic Safety Administration(NHTSA)과 협력하여 PKI 관련 규격을 제정하고 Vehicle Infrastructure Integration(VII) 프로젝트를 진행하면서 등장하였다. CAMP 규격에서는 익명성 보장을 위해 전통적인 PKI 구조에 Linkage Authority(LA)를 만들어 차량의 가명 ID를 발급한다. 해당 가명 ID를 기반하여 인증서를 발급하기 때문에 ID를 알고 있는 LA들과 Certificate Authority(CA)를 전부 해킹하지 않는 이상 차량과 인증서 간의 생성정보를 확인할 수 없다.



(그림 1) CAMP-VSC3 Communication

2.2 C2C-CC

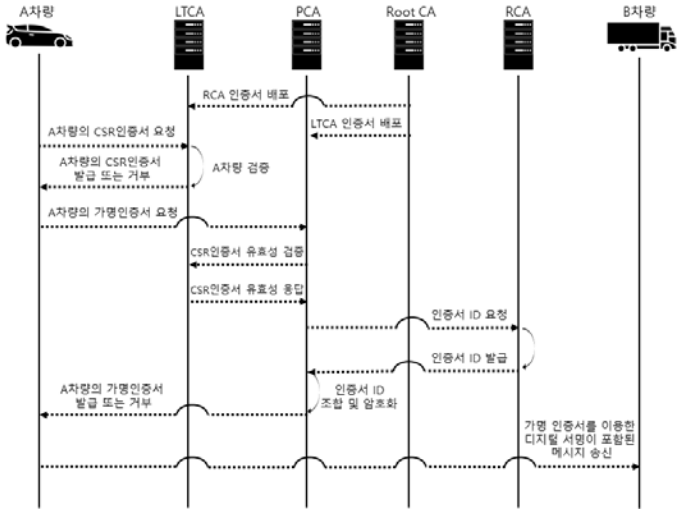
C2C-CC는 인증서를 발급하는 방식이 CAMP VSC3와 다르다. CSR 인증서는 Long Term CA(LTCA)에서, 가명 인증서는 Pseudonym CA(PCA)에서 발급한다. CSR 인증서를 활용하여 가명인증서 발급을 원하는 차량이 PCA에게 발급 요청을 하게 되면, PCA에서는 Root CA로부터 받은 LTCA의 인증서를 이용하여 LTCA에게 가명 인증서를 요청한 차량의 CSR 인증서 유효기간을 확인한다. 유효성을 확인한 PCA는 가명 인증서를 발급해 준다. LA의 가명 ID를 활용하여 가명인증서를 생성하는 CAMP의 방식에서는 내부자라 하더라도 CSR 인증서와 가명 인증서를 생성하는 ID 정보를 발견할 수 없다. 하지만 C2C-CC의 방식에서는 PCA가 가명 ID를 생성하고 가명 인증서를 발급하기 때문에 내부자가 CSR 인증서와 가명 인증서의 ID를 찾을 수 있으므로 취약점이 존재한다[3].



(그림 2) C2C-CC Communication

3. 제안

3.1 RCA의 랜덤 ID를 활용한 인증서 발급



(그림 3) RCA V2V Communication

C2C-CC의 문제점은 PCA가 가명 인증서를 발급할 때 해당하는 차량 ID에 대한 가명을 생성하여 차량에게 발급하는데 이때, 가명에 해당하는 차량의 ID를 추적하기 위해 차량 ID 정보를 저장할 수 있다. 그렇기 때문에 PCA에 접근할 수 있는 자 혹은 악의적 공격자가 PCA에 접근할 경우 차량 ID를 탈취당할 수 있는 위험이 존재한다. 그러므로 RCA를 이용해 인증서를 만들 수 있는 ID를 PCA가 알지 못하게 함으로써 차량 ID에 대한 정보 유출을 막을 수 있다.

4. 결론

본 논문에서는 점점 상용화 되어가는 지능형 교통시스템의 필수 기술인 차량 간의 통신과정에 있어서 기존의 인증서 발급절차의 해킹 가능성을 줄여 보안성을 높일 수 있는 인증서 발급 절차 방안을 제안하였다.

참고문헌

[1] 박승수, 김기천, "개인정보 보안성 강화를 위한 간소화된 V2V통신 인증 절차 방안", 한국통신학회, pp. 117-118, 10, 2016.

[2] 안홍일, 강성재, 김민준, 정재일, "Open Source 기반의 IEEE WAVE 1609.2 ECDSA Performance에 관한 연구", 한국통신학회, pp. 856-857, 01. 2015

[3] 이유식, 심상규, 김덕수, "V2X 통신을 위한 보안기술", 한국정보보호학회, pp.28-34, 04. 2014