SMV를 이용한 2차 proposal

Konkuk Univ. IT융합정보보호학과
오예원

목차

- Back ground
- Proposal
  - 검증 계획 및 필요성
  - Automata
  - Property
- 참조

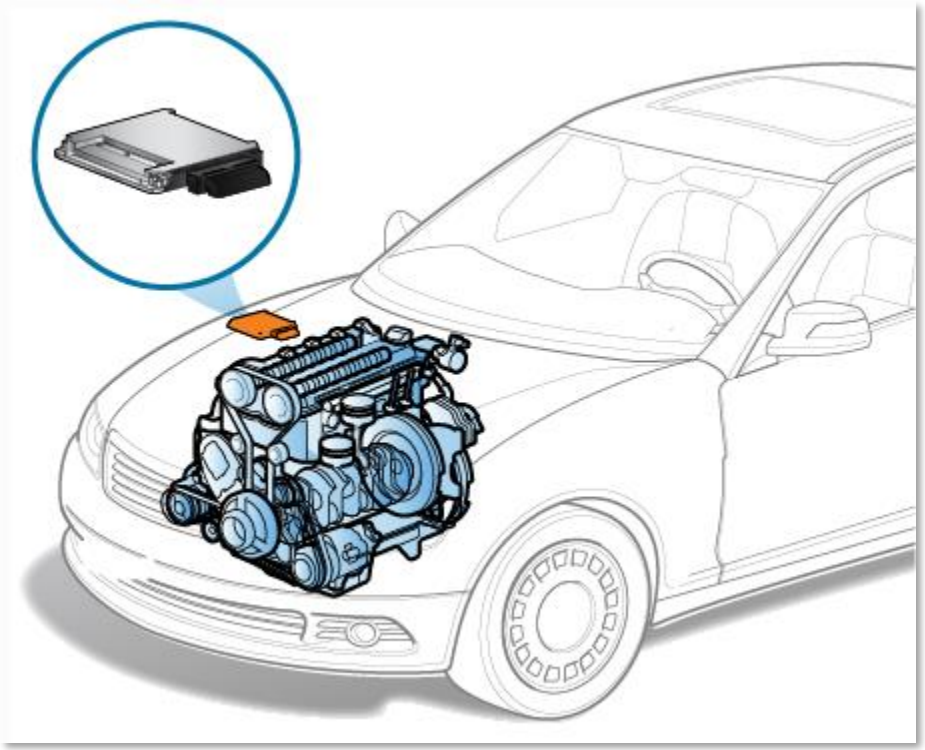
Background

인증서 기반 암호시스템 검증

Background

What's the Engine Control Unit(ECU)

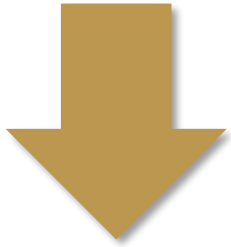
- 엔진의 내부적인 동작을 다양하게 제어하는 전자제어장치



Background

What's the Engine Control Unit(ECU)

- ECU의 동작은 Firmware에 지정된 데이터를 기반으로 RPM조절과 공기 유입량 등을 제어.



불법적 튜닝(ECU Remapping)

- 목적 : 차량의 엔진 출력 및 연비 향상

Background

What's the problem of ECU Remapping

- ECU remapping의 문제점?

1. 차량이 승인 받은 **안정성**을 보장할 수 없음
2. 배기가스 배출 증가
3. 엔진의 내구성 저하

Background

What's the solution of ECU Remapping

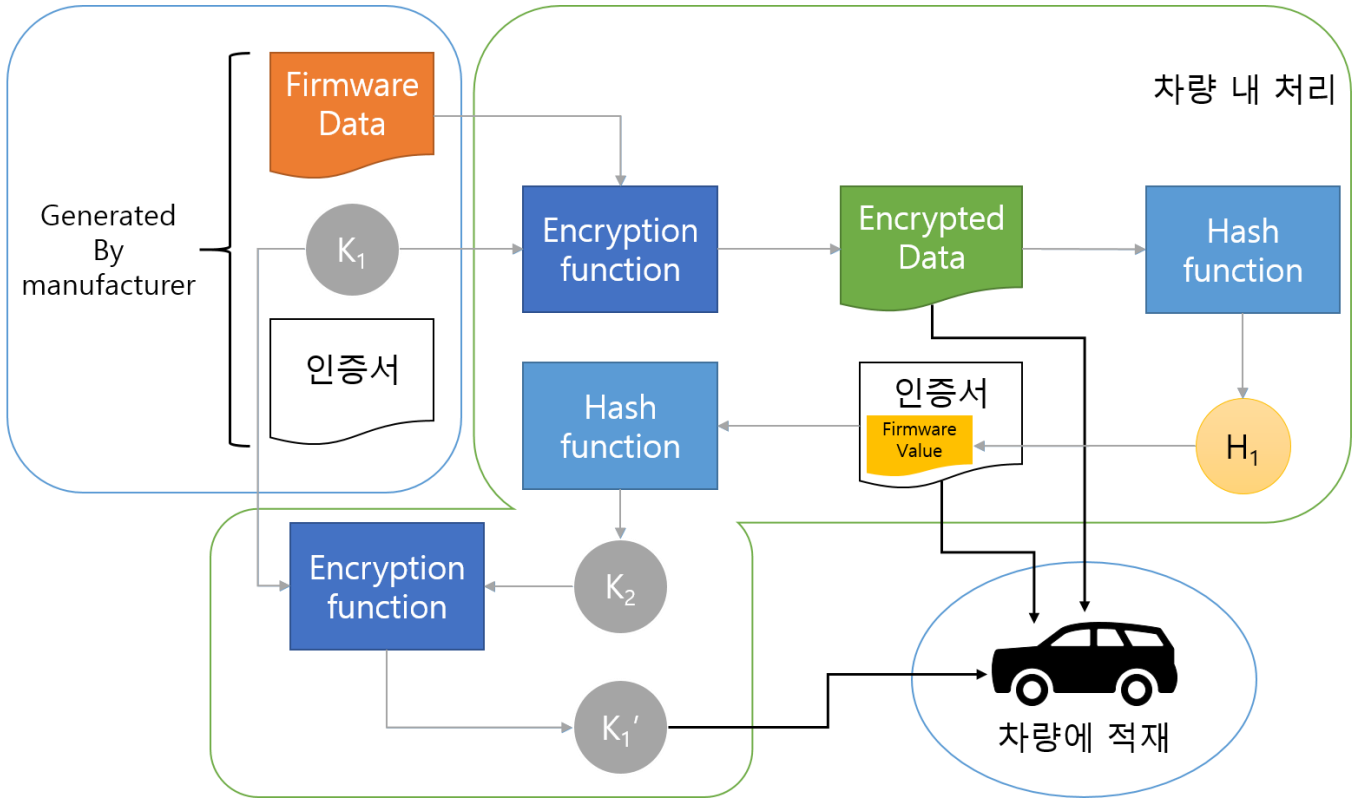
- ECU remapping 차단 방법 & ECU firmware 데이터 보안

인증서 기반 암호시스템 설계

Background

인증서 기반 암호시스템

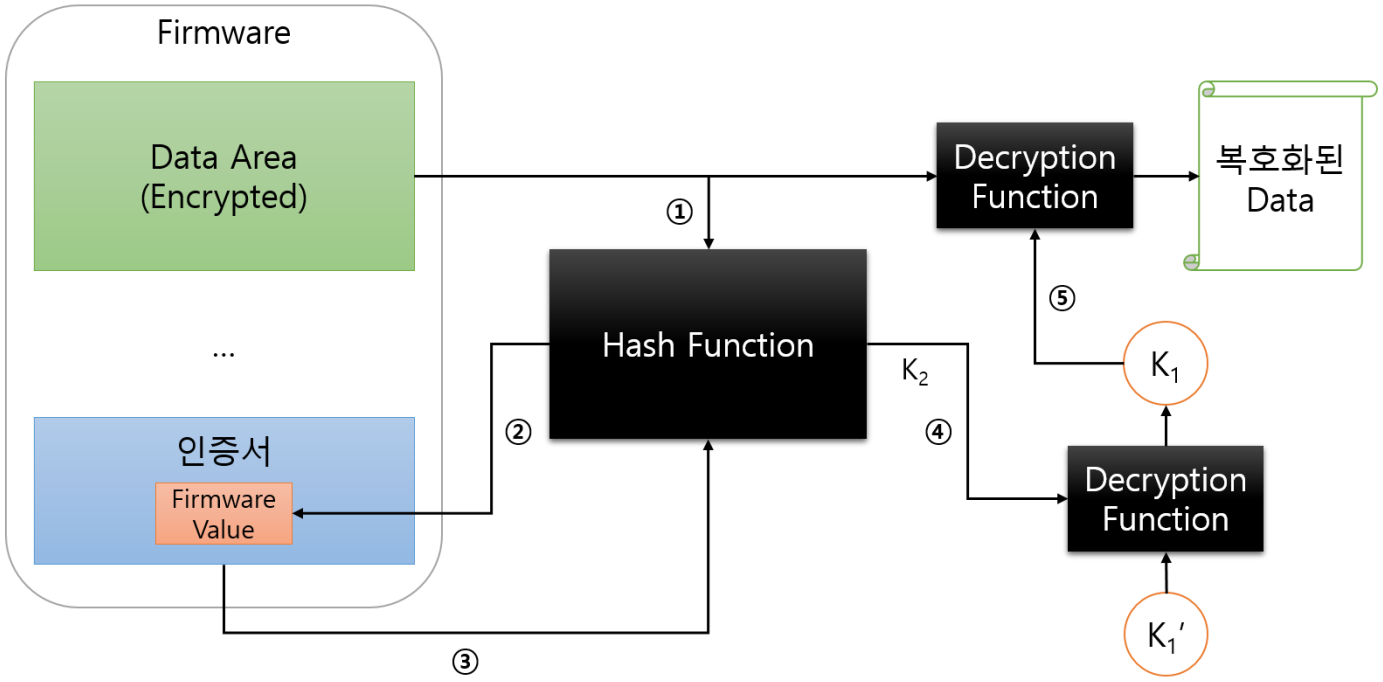
➢ 데이터의 생성 및 차량 적재 과정



Background

인증서 기반 암호시스템

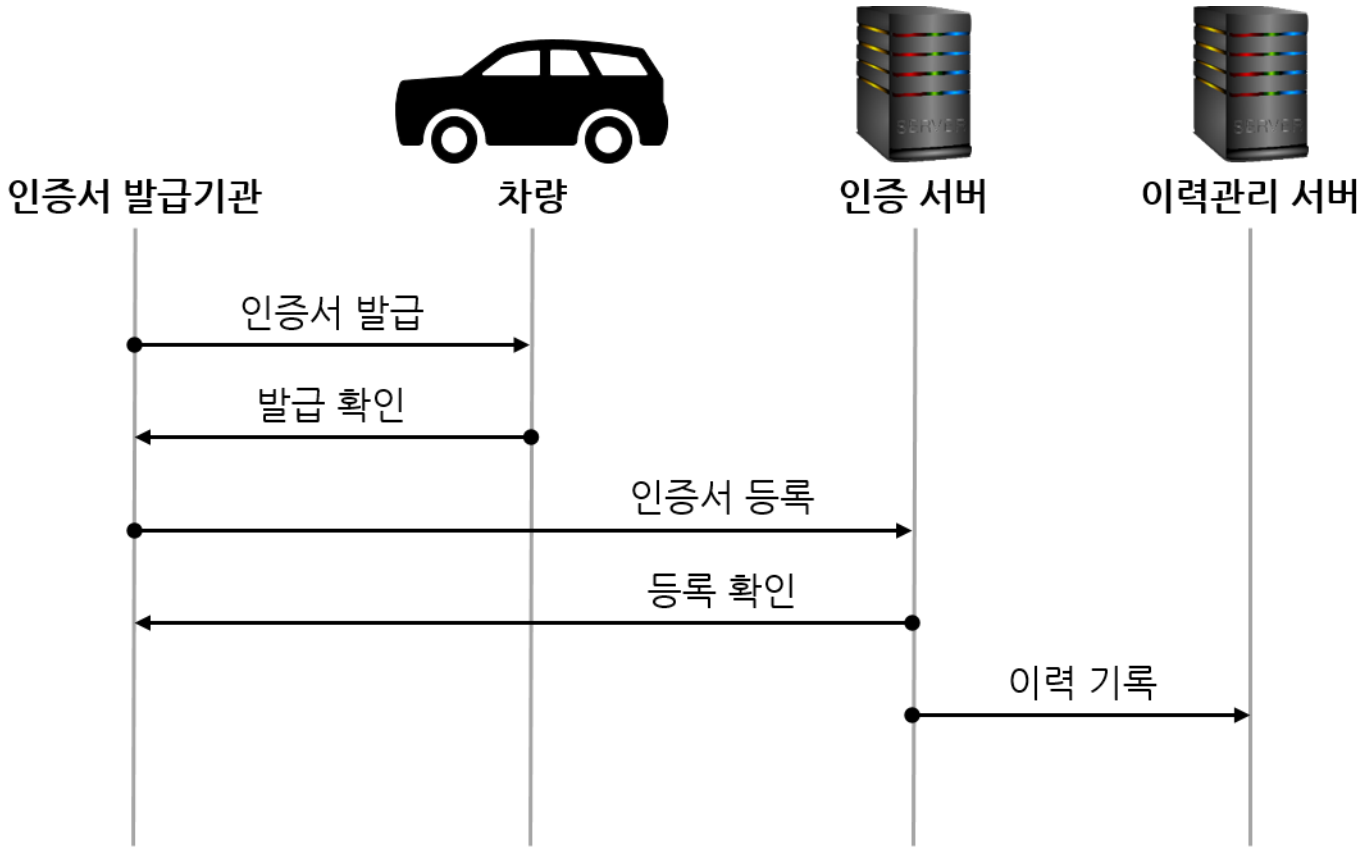
➢ Firmware Value 및 K2 생성 및 K1 을 통한 Firmware Date 복호화



Background

인증서 기반 암호시스템

- 차량 출고 시 인증서 발급



2차 proposal

인증서 기반 암호시스템 검증

2차 proposal

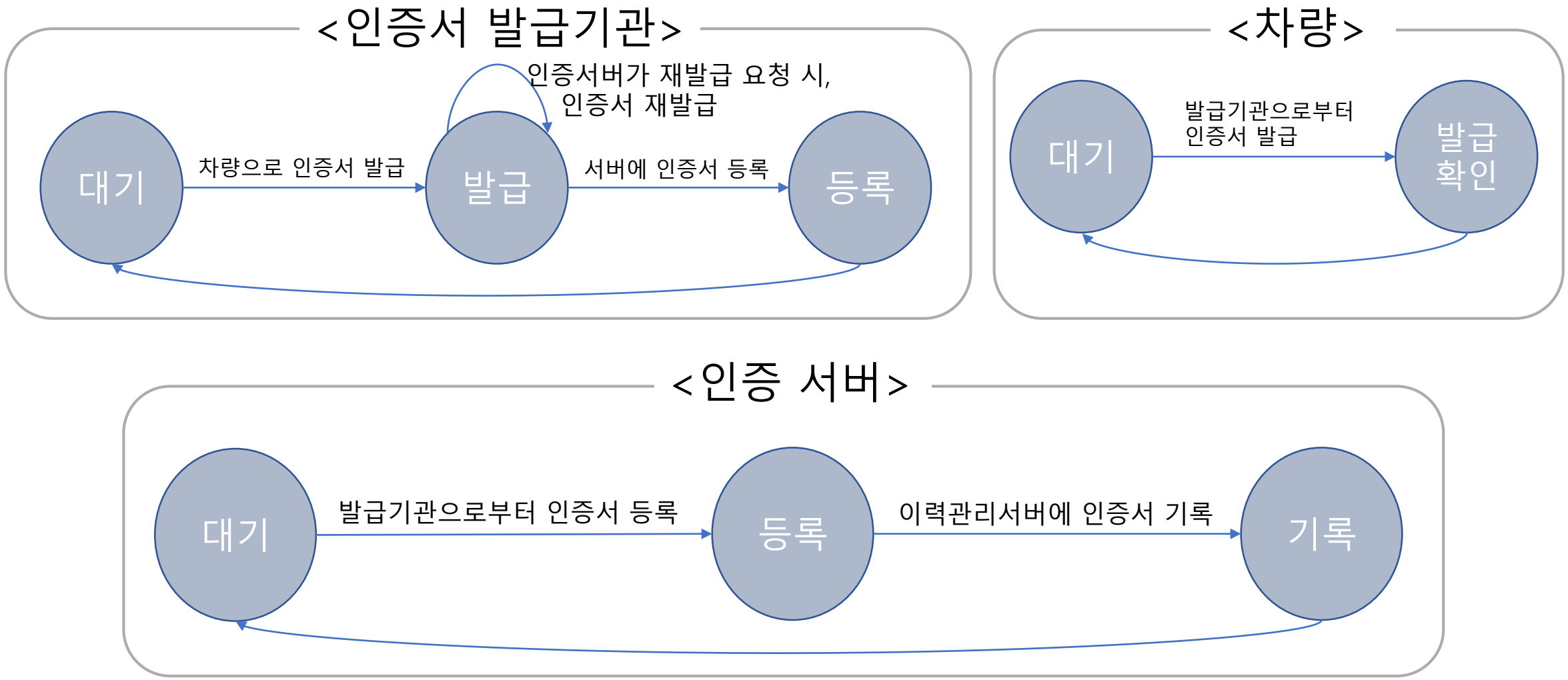
검증 계획 및 필요성

- 모델링 언어: SMV
- 검증 언어: CTL
- 검증 툴: NuSMV

- 주요 매핑 데이터를 안전하게 보호하는 목적에 따라 잘 설계되었는지 Property를 통해 Model checking

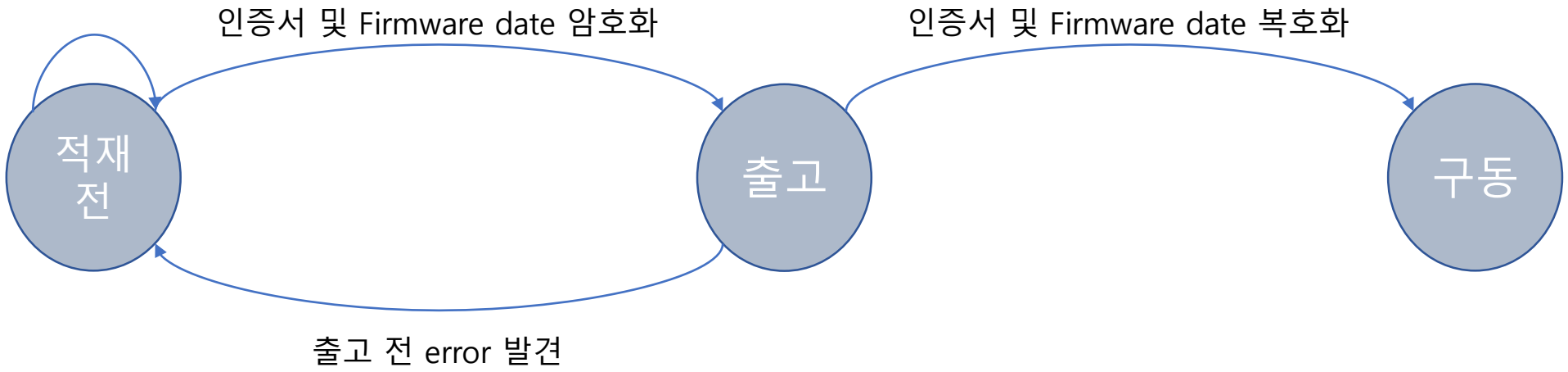
2차 proposal

Authentication Automata



2차 proposal

Car Automata



2차 proposal

property

- 차량에 암호화된 비밀키(K1′)가 있는가?
- 차량에 인증서가 있는가?
- 차량에 암호화된 데이터가 있는가?

참조

[1] 유요셉, 김기천 “ECU 보안성 유지를 위한 인증서 기반 암호시스템 설계“, 2017년 춘계학술발표대회 논문집 제 24권 제 1호,2017년 4월

[2] 박철우, 윤상준, 김기천 “긴급메세지 전송 시스템의 모델링을 통한 안전성 검사”, 제40회 한국정보처리학회 추계학술발표대회 논문집 제 20권 제 2호, 2013년 11월

[3] https://carpartsglossary.wordpress.com/

Thank You