커네티트 카의 취약점 분석 및 보안 시스템 설계

김태형* · 장종욱*

*동의대학교

Analyzing of connected car vulnerability and Design of Security System

Tae-Hyoung Kim* · Jong-Wook Jang**

*Dong Eui University

E-mail : fingersnoop@gmail.com , jwjang@deu.ac.kr

요 약

과거, 자동차 보안은 'Door Lock'과 같은 물리적인 접근을 방지하는 것이었다. 그러나 시대가 발달함에 따라, 자동차 보안의 트렌드는 이러한 물리적인 보안에서 굉장히 지능적으로 바뀌었다. 이러한 변화는 해커들로 하여금 차량 통신 시스템을 공격할 계기를 만들게 되었고 현재 차량 통신 시스템은 몇 가지 취약점이 존재하는 CAN Protocol을 사용하고 있다. 첫 째로 ID 스푸핑, 둘 째로 서비스 분산 공격, 셋 째로 안드로이드 좀비 어플리케이션이다.

현재 자동차들은 엔진 제어나, 도어 락 제어, 그리고 핸들의 제어를 위해 수많은 ECU들을 사용하고 있다. 그리고 CAN Protocol은 신호를 Broad - Cast 방식으로 제공하기 때문에 해커들은 굉장히 쉽게 그 신호에 접근 가능하다. 그리고 차량 통신 시스템을 공격하기 위해 Android나 IOS와 같은 범용성이 높은 어플리케이션을 자주 이용한다. 차량의 소유주가 블루투스 동글을 통해 신호를 넓게 퍼뜨리게 되면 해커는 이 신호에 쉽게 접근하게 되고, 해당 데이터를 수집해 분석하고 그들은 차량의 ECU를 공격하기 위해 특정한 데이터를 만들고 ECU에 전송해 ECU를 제어하게 된다. 그래서 본인은 인증 시스템과 안드로이드의 말단에서 이러한 공격을 막을 방법을 제시한다.

ABSTRACT

In the Past, Trend of car security was Physical Something like doorlock system, and The Generation did not have skills connecting External devices. Through Car Development is up, that trend of car security Changed Physical Security to Intelligence Security. This Changes give a chance to hackers to attack this system. This System use CAN(Controller Area Network) Protocol which have three vulnerabilities. First, ID Spoofing, Twice, D - Dos Attack, Third, Android Application Injected

Modern cars have many ECU(Electronic Control Unit) to control devices like Engine ON/OFF, Door Lock Handling, and Controlling Handle. Because CAN Protocol spread signal using broadcast, Hackers can get the signal very easily, and Those often use Mobile devices like Android or IOS to attack this system. if bluetooth signal is spread wide, hackers get the signal, and analysis the bluetooth data, so then They makes certain data to attack ECU, they send the data to ECU, and control ECU installed car. so I suggest that I will prevent this attack to make Auth system and prevent this attack in end of Android.

키워드

connected car, CAN, Security, vulnerability

I. Introduction

CAN 프로토콜은 TCP/IP와 같이 의존성을 가지며 자동차간의 통신에 안정성을 제공한다. 그러나 ECU는 16비트 마이크로프로세서로 만들어져 있어서 코드는 매우 간단해야하며 이러한 문제 때문에 CAN통신은 보안에 있어서는 부적합 할 수 밖에 없다.
CAN 통신은 브로드캐스트로 신호를 주변에 퍼뜨리게 되는데 이러한 문제점 때문에 해커들은 손쉽게 이 신호를 수집 가능하다. 그리고 그들은 보통 ECU를 공격하기 위해 안드로이드나 맥과 같은 모바일 장치들을 사용하며 2015년, 크라이슬러의 지프 체로스키는 CAN Protocol을 이용한 ECU 공격 취약점이 발견되면서 140만대의 차량을 전량 리콜하는 사태가 벌어지기도 했다. CAN의 취약점은 전 세계적으로 현재 이슈이며, 대 부분의 차들이 이 프로토콜을 사용 중에 있다.
그리고 안드로이드 어플리케이션은 보안에 굉장히 취약하며 감염된 앱은 차에 부착된 ECU를 공격한다. 그리고 블루투스 동글은 특정한 데이터를 차에 부착된 ECU에 전송할 수 있으며, 이를 이용해 앱은 차량의 엔진을 키거나 끄고, 핸들을 조작한다거나 브레이크를 통제할 수 있다. 아래는 3가지 취약점들에 대한 소개와 방어 방법에 대한 설명이다.

II. System Design and Main Functions

현대의 자동차들은 특수한 기능들을 사용하기 위해 블루투스 동글을 많이 대 부분 설치한다. 그것 때문에 해커들은 Data - Frame을 쉽게 얻을 수 있게 된다. 아래의 그림이 그 예시이다.

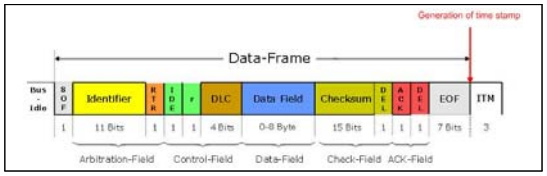

Fig. 1. Data - Frame(CAN)

ECU가 차량의 드라이버에게 메시지를 보낼 때 버스의 상태를 확인하여 Idle일 경우 ECU는 메시지를 보낸다. 반대로 그렇지 않다면 ECU의 상태는 리세시브 모드로 전환된다. ID값이 낮을수록 우선순위가 높다. 그리고 CSMA/BA 통신 방식을 사용하는 CAN은 두 가지의 논리적 상태를 가지고, 도미넌트 Bit 0 리세시브 비트 1을 가진다. 그래서 ECU들이 메시지를 동시에 보내면 Identifier 필드를 확인해 노드가 1인 비트가 존재하면 우선 순위를 잃게 되고, 최종적으로 하나의 메시지만 수신된다.

2.1 Identifier Spoofing

위의 설명과 같이 CAN 통신은 브로드 캐스팅 방식으로 신호를 주위에 뿌리는데, 악의적인 ECU를 제작하여 공격하고자 하는 대상 차량의 버스 상에 이를 설치하면, 모든 데이터들이 수집되고, 가짜 메시지들을 만들어 차량의 엔진제어나 핸들제어, 차량의 문제어 등 여러 기능을 제어할 수 있다.

2.2 DOS

CAN의 주요 취약점 중 중재기능이 있다. 이 기능은 여러 메시지가 한 번에 들어왔을 경우 해당 ID의 Identifier 필드의 우선순위를 조사해 우선순위가 높은 메시지를 받아들이는 기능이다. CAN의 브로드캐스팅의 취약점을 이용해, 가장 우선순위가 높은 ID를 수집한 후, 특정 메시지를 만들어 해당 차량의 CAN버스에 공격을 하게 되면 해당 메시지가 가장 높은 우선 순위를 가지고 있기 때문에 기존의 시스템에서 통신하는 모든 메시지들이 무력화된다.

2.3 Android Application Injected

현대의 자동차들은 차량의 OBD-II를 블루투스나 와이파이를 이용해 모바일 장치와의 연동을 많이 하고 있으며, OBD-II를 이용해 차량에 접근하는 어플리케이션들이 굉장히 많다. 이는 해커들에게 기존의 방식과는 다른 원격 공격이 가능하다는 것을 의미하며, 만약 사용자가 특정한 기능을 수행하는 감염 된 어플리케이션을 배포하고 사용자가 이러한 어플리케이션을 설치하게 될 경우, CAN 버스에 연결된 블루투스나 와이파이 동글을 통해 차량의 ECU에 접근이 가능하다. 현재 전 세계의 차량 어시스트를 위해 수많은 엔지니어가 임의의 동글을 차량에 설치하고 있으며, 이는 해커들에게 내부에서 인증이나 데이터의 암호화가 존재하지 않는 현대의 차량은 수많은 공격기회를 제공할 수 있음을 의미한다.

Ⅲ. How to Prevent this Attack

CAN Protocol의 근본적인 취약점들은 구조상 해결하기는 사실 힘들다. 그러나 데이터의 모니터링과 데이터의 빈도 수, 데이터의 유형의 감시와 필터링을 통해 어느 정도 보완을 할 수 있다.

3.1 Spoofing Prevention

ECU는 차량 운전자에 의해 메시지의 순서가 매겨진다. ECU의 메시지가 흘러가는 중간 지점에서 메시지의 순서를 모니터링하고,해시 알고리즘을 사용해 메시지가 정상 메시지인지 아닌지 인증을 통해 방어한다. 정상적으로 보내는 메시지라면 해시 데이터를 생성 시 사용하는 키 값을 해커가 알 수 없으므로 검증을 할 수가 없다.

3.2 DOS Prevention

DOS 공격으로 중앙 모니터링 ECU에서 빈도수가 높은 순으로 최상위 우선권을 가지는 데이터들을 검사 해 DOS공격을 탐지하고, 같은 기능을 하는 ECU를 하나 더 장치해 스위치하고 DOS로 들어온 데이터의 ID를 바탕으로 스위치한 ECU에서 그것 보다 높은 메시지를 만들어 통신하게 한다. 그렇게 되면 새롭게 생성된 메시지는 Dos로 들어오는 메시지보다 항상 우선권을 가지므로, 중재기능에 의해 무의미하게 된다.

3.3 End of Android Prevention

안드로이드 애플리케이션에서의 공격은 해커에게 있어 원격으로 자동차를 제어할 수 있는 가장 강력한 공격 방법 중 하나로 생각된다. 특히 안드로이드 애플리케이션은 IL기반의 언어기 때문에,디컴파일링이나, 역 공학에 굉장히 취약해 변조가 쉽게 이루어지고, 또한 사람들이 가장 많이 사용해 접근성이 높다.

그래서 안드로이드 커널 드라이버 단으로 모든 태스크를 감시해 ECU로 향하는 메시지의 주요 필드 값을 수집하고, 사용자의 통제하에 최종적으로 차량의 ECU에게 전달되는 방법을 사용해야 할 것이다.

Ⅳ. Conclusion

지금까지 생각하고 수집한 정보를 통해 보안 방법에 대해 강구하고, 분석하여 장치를 개발하고, 후에 자동차 보안에 기여하는 데 도움이 되었으면 한다.

감사의 글

이 논문은 2016년도 한국연구재단의 지역혁신창의 인력양성사업과 Brain Busan 21 협력 기술개발사업의 지원을 받아 수행된 연구임을 밝힙니다.(NRF-2015H1C1A1035898, C0249807)

Ⅴ. References

[1]http://www.dailysecu.com/news_view.php?article_id=7967
[2]http://paulhwang.tistory.com/8
[3]http://www.zdnet.co.kr/news/news_view.asp?artice_id=20141108113343