CAN FD 네트워크상에서 AUTOSAR 를 이용한 암호화된 신호 전송

오늘날 차량 네트워크 분야에서 대부분의 데이터 전송이 특별한 보안 조치 없이 이루어지고 있다. 이 때문에, 차량 버스 시스템에 직접 접속만 가능하다면 전송된 데이터를 원본 그대로 읽어내거나 데이터를 수정하여 버스 시스템상에서 전송할 수도 있다. 암호화된 데이터 전송을 이용하여 이러한 정보를 인증된 수신자만이 해석하도록 보장하고, 메시지를 가로채거나 변경하려는 시도를 더욱 어렵게 만들 수 있다.

언론은 차량 조작[1],[2]과 관련하여, 차량 네트워크상의 데이터가 실제로 조작 가능한지에 대한 의문을 제기하고 있다. 원격 제어 기능을 갖춘 조작된 장치나 내부 장치가 차량 작동에 영향을 줄 수 있을까? 그리고 이러한 조작을 막을 수 있는 대책은 무엇인가?

오늘날의 자동차는 네트워크화된 다양한 센서와 액추에이터로 구성되어, 버스 시스템을 통해 중요한 데이터를 지속해서 전송하는 매우 복잡한 시스템이다. 대부분의 경우, 전송되는 정보는 원시 데이터(raw data) 형식이다. 유효성 검사를 수행할 수 있다고 하더라도 그 효과는 매우 제한적이다. 수신자는 데이터가 원하는 발신자에 의해 전송되었는지, 혹은 외부 ECU 를 통해 입력된 데이터인지, 즉, 허가된 데이터인지를 확인할 수가 없다. 그뿐만 아니라, 데이터에 대한 접근이 자유롭기 때문에, 네트워크 신호의 내용을 파악하기 위한 버스 정보 분석이 가능하고, 데이터 전송의 기밀화나 인증화가 되어있지 않다.

이러한 문제를 해결하기 위해 벡터의 엔지니어들은 유연하면서도, AUTOSAR-3.x Basic Software 와 통합할 수 있는 CAN 네트워크에 대한 보안 통신 체계를 구상했다. 사용자 인증 및 재전송 공격의 방지를 데이터 보호의 주요 목표로 하여, 외부에서 모니터 될 수 없는 통신을 구현하고자 하였다.

데이터 암호화를 위해 전문가들은 AES 알고리즘을 선택하였다[3]. 현재, 이는 매우 안전한 암호화 방법으로 알려졌으며, 128 비트의 블록 길이를 가지는 대칭형 블록 암호화를 기반으로 한다. 이 알고리즘은 데이터를 16 바이트 혹은 16 바이트의 배수로 생성하고, 이를 수신자에게 전송한다. 추가적인 장점으로는 일부 마이크로컨트롤러가 이미 이 알고리즘을 처리하는 고속 하드웨어를 내장하고 있다는 점이다.

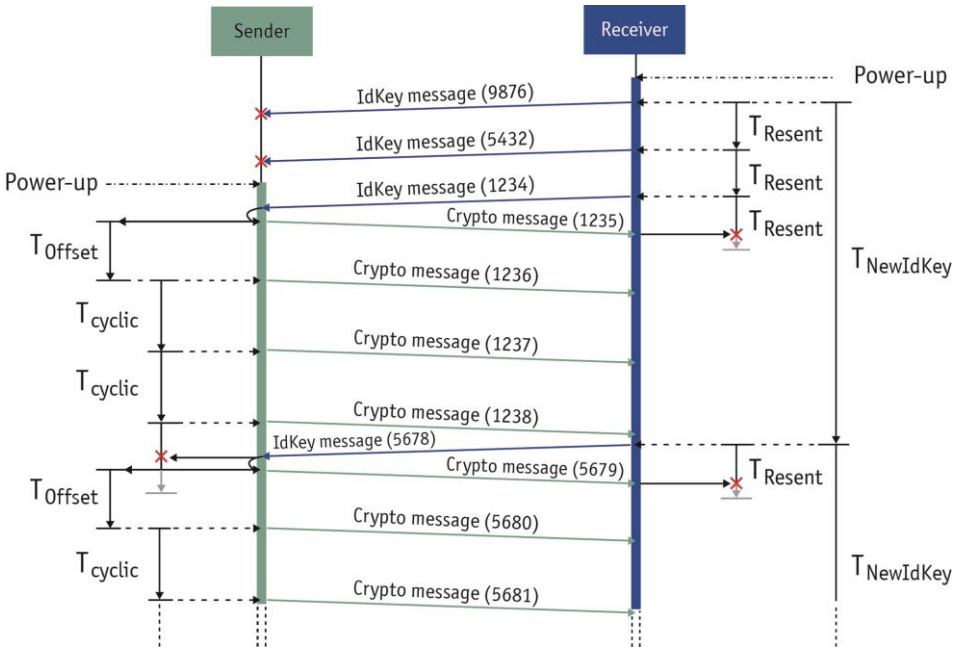
CAN 메시지는 프레임 당 최대 8 데이터 바이트까지 전송 가능하므로, 통신 스택에 이미 포함된 ISO 전송 프로토콜(TP)을 선택하였다. 설정을 간소화하고 프로토콜 오버헤드를 줄이기 위하여, 발신자와 수신자 간의 고정된 1:1 관계를 갖는 일방향 통신을 선택하였다.

대칭 암호를 사용하기 위해서 발신자와 수신자 모두가 동일한 키를 가지고 있어야만 한다. 사용자 또는 OEM 이 원하는 키를 자유롭게 선택할 수 있도록, 사용된 소프트웨어 모듈은 동작 중에 키의 동적 할당을 허용한다. (비대칭) 키 교환 방법과 같은 고급 방법도 구현할 수 있으며, EOL

프로그래밍에서의 정적 할당도 가능하다. 차량별로 특정한 키를 사용하는 경우, ECU 를 교체할 때에는, 어떠한 상황에서도 보안을 유지할 수 있는 인증 방법으로 신규 ECU 를 설정하여야 한다.

재전송 공격 방지

위와 같은 설정을 통해 메시지의 암호화된 전송이 가능하지만, 전송 대상인 정보가 여전히 정적이다, 예를 들면, 고유의 키 텍스트를 일반 텍스트 신호에 할당할 수 있다. 즉, 원하는 통신의 일부는 저장하고, 이를 후에 시스템에 다시 전송하는 재전송 공격은 여전히 가능하다. 수신자는 해당 메시지가 원하는 발신자로부터 전송되었는지를 확인할 수 없기 때문이다. 이를 확인하려면, 통신 초기에 수신자가 ID 키라 불리는 임의의 값을 생성하여 발신자에게 전송해야 한다. 매 전송 시 발신자는 해당 값을 증가시킨 후 전송 메시지에 덧붙인다. 메시지가 도착하면, 수신자는 해당 ID 키가 예상 값과 일치하는지 확인한다. ID 키가 유효하면 메시지가 처리되지만, 그렇지 않으면 거절된다. 발생할 수도 있는 메시지 손실을 허용하기 위하여, 수신자는 약간의 큰 값도 수락할 것이다. 즉, 신호의 내용이 변경되지 않더라도, 전송 메시지의 카운터가 지속해서 암호화된 데이터를 변경하는 것이다(그림 1).



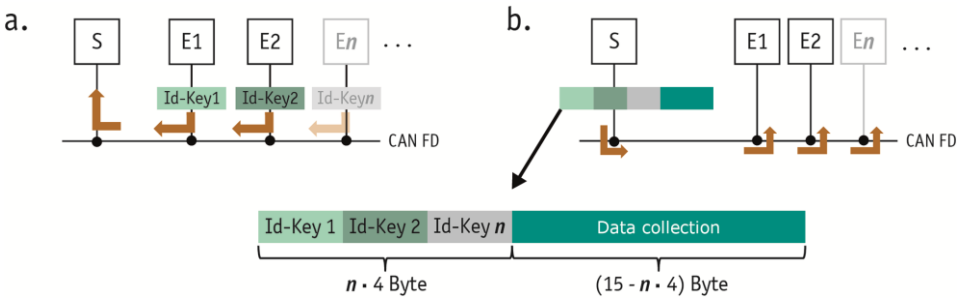
[그림 1: 메시지 전송 및 암호화된 통신의 타이밍]

ID 키의 문자 수와 메시지의 전송 빈도에 따라, 해당 메시지의 카운터 값 오버런이 발생할 수 있으며, 이로 인해 암호화 메시지의 반복 전송 현상이 발생할 수도 있다. 이를 방지 하려면, ID 키가 일정 기간만 유효해야 한다. 이러한 유효 기간이 만료되면, 수신자가 새로운 값을 생성하여 발신자에게 전송해야 한다. 새로운 ID 키가 수신됨과 동시에, 발신자는 암호화된 메시지를 전송한다. 따라서 수신된 ID 키가 내부 키와 일치하지 않을 경우, 수신자가 메시지 반복을 개시할 수 있으므로 대기 시간이 줄어든다. 발신 노드가 T(오프셋) 동안 새로운 ID 키 메시지를 수신하고 처리하기는 하지만, 버스 시스템상의 과부하를 막기 위해 이러한 메시지가 바로 암호화된 메시지의 재전송으로 이어지지는 않는다. 더욱 견고한 프로토콜을 만들기 위해, 수신자는 새로운 카운터 값을 기준으로 발신자의 응답을 감시하는 타이머 T(재전송)를 사용한다. 발신자로부터 확인 메시지를 받지 못할 경우, 수신자는 새로운 ID 키를 생성하여 재전송한다. 이를 통해, 전송 ECU 의 작은 오류도 감지할 수 있을 뿐 아니라, 재전송 시간도 단축할 수 있다. 또한, 비휘발성 메모리에 ID 키가 저장되는 것을 방지할 수 있다.

데이터 분할 없이 CAN FD 로 데이터 전송하기

ISO-15765 전송 프로토콜에 대한 데이터를 분할하여 CAN 을 통해 전송하는 것은 심각한 문제를 내포하고 있다. 데이터 전송 시간이 길어질 뿐만 아니라, ISO-15765 프로토콜에 대한 데이터를 분할하여 복수의 노드로 전송하는 것이 매우 어려우므로 이러한 방법은 고정된 1:1 관계에 국한될 수밖에 없다. 반면, CAN FD 를 통해서는 다수의 수신자들에게 암호화된 메시지 전체를 동시에 전송하는 것이 가능하다[4]. 각 수신자는 암호화된 메시지를 해독하기 위해 동일한 대칭 키가 필요하다. 이때, 인증 과정을 거치기 위해서는 ID 키에 관한 두 개의 배리언트를 고려해야 한다: 1) 모든 수신자가 합의된 값에 동의한다. 혹은, 2) 모든 수신자가 별도의 ID 키를 생성하여 발신자에게 전송한다. 발신자는 모든 카운터를 관리하며, 이를 데이터 메시지에 첨부한다. 암호화된 메시지에 포함된 카운터 값의 위치는 반드시 해당 수신자에게 고유하게 할당되어야 한다. 그림 2 는 다수의 수신자들을 대상으로 한 데이터 전송을 나타내고 있다. 먼저, 수신자가 임의로 생성된 시작 값을 발신자에게 전송한다. 그런 다음, 해당 발신자가 전송 주기별로 모든 ID 키 값을 증가시킨 후 이를

암호화된 메시지 내의 지정된 위치에 삽입한다. 그러면, 해당 수신자가 ID 키를 확인한 후 데이터를 수락 혹은 거절한다(그림 2).



[그림 2: CAN FD – 다수의 수신자들을 대상으로 하는 ID 키 구조]

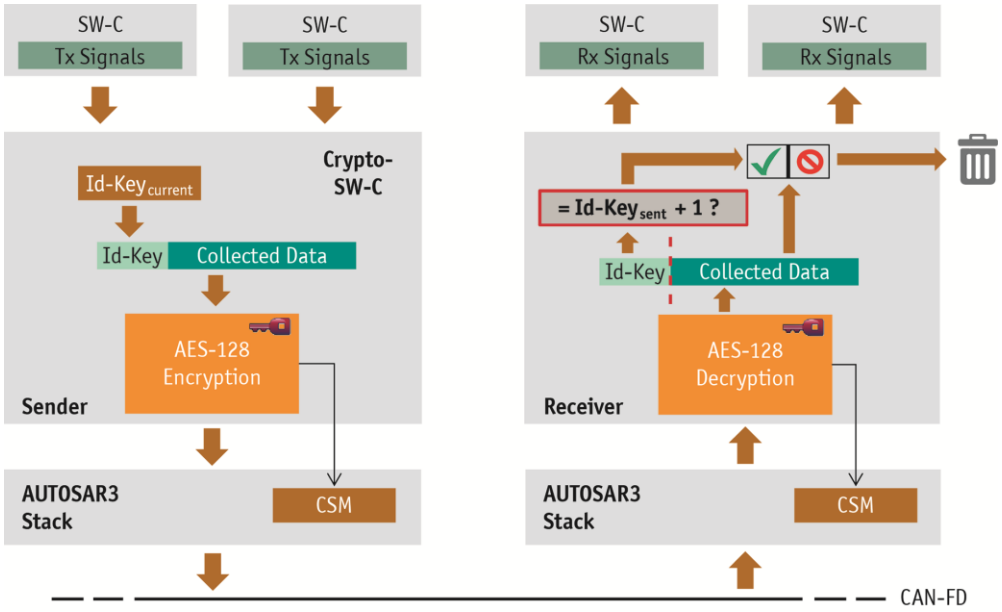
하지만, 수신자의 수가 증가할수록, 가용한 데이터를 위한 메시지 공간이 줄어든다. 또한, 가용한 데이터의 바이트 수는 채택된 ID 키의 문자 수에 따라 편차가 크다. 그림 1 에 묘사된 통신 타이밍이 적용되었다. ID 키 수신 시 발신자를 위한 변경만 요구된다. 암호화된 메시지를 바로 전송하는 대신, 발신자는 다른 수신자로부터의 다른 ID 키 메시지를 수신하기 위하여 설정 가능한 시간 T(IdKeyReply)를 기다린다. 특별한 경우 T(IdKeyReply)=0 설정을 통해 초기화도 가능하다.

벡터는 CANoe 환경에서 CAN FD 를 위한 프로토콜을 구현하였다. 벡터의 전문가들은 ECU 및 네트워크를 개발하고 이를 시뮬레이션 및 테스트할 수 있는 소프트웨어를 사용하여 해당 프로토콜에 대한 광범위한 테스트를 실시하였다. 재전송 공격에 대해 요구되는 방어 성능은 물론이고 발신자와 수신자의 메시지 손실, 오류, 재입력, 그리고 타이밍 오류와 강력한 공격에 대한 연구가 이루어졌다. 테스트 결과, 위의 언급된 모든 상황에서 암호화된 시스템을 통해 데이터를 안정적으로 전송할 수 있었다.

요약 및 전망

CAN FD 의 경우, 특히 복수의 노드를 이용해 암호화된 데이터를 안정적으로 전송할 수 있으며, 이는

기존의 AUTOSAR 환경에도 적합한 방법이다. 단 한 가지 취약한 부분은 어플리케이션 수준에서의 데이터 직렬화 및 병렬화이다(그림 3). 즉, 각각의 신호 별로 RTE 의 모델링 속성이 사용될 수 없다는 것이다. 이러한 시스템상에서 전형적인 공격 포인트에 대해 항상 유념해야 한다. 예를 들어, 스타트업 단계에서 취약한 ID 키를 위한 임의 번호 생성기 또는 대칭 키 도용 등이 이에 해당한다.



[그림 3: 암호화된 전송을 위한 소프트웨어 컴포넌트]

보안 기술 업계에 따르면, AES-128 알고리즘의 미래는 긍정적이며, 알고리즘의 구현이 더욱 발전하여, 심지어 하드웨어 액셀레이터에 의한 지원까지도 가능할 것으로 보고 있다. 본 기술 기사에 소개된 암호화된 신호 전송을 이용하여, CAN/CAN FD 통신에 대한 공격을 매우 어렵게 만들 수 있을 뿐 아니라, "내부인의 도움" 없이는 조작이 거의 불가능하게 만들 수 있다. 이미 수년간 양산 차량에서 사용됐으며, 일부 차량은 자동차 보험금 할인 혜택도 받고 있다. 이 옵션을 장착하면, 보안이 강화되어 데이터 보호뿐 아니라, 최종 사용자는 직접적인 비용 절감의 혜택까지 누릴 수 있는 것이다.

가까운 미래에 Car2x 통신, WLAN, Bluetooth, Ethernet 과 같은 원격 접속에 대한 수요가 지속적으로 증가하여, IT 보안과 관련한 요건은 더욱 강화될 전망이다. 이러한 접속 모드는 공격에 대한 방어 기능을 갖추어야 하며, 어떠한 원격 조작도 허용해서는 안 된다. 특히, 이는 다른

교통수단이나 인프라로부터 안정적인 정보를 수신해야 하는 운전자 보조 시스템에는 더욱 중요한 부분이다. 벡터는 운전자 보조 시스템 개발 및 분석을 위한 기술 지원 서비스 또한 제공 하고 있다.

독일 출판물 CAN Newsletter, 2014 년 04 월호 기사 번역판

그림 제공:
Vector Informatik GmbH

참조:

[1]http://www.chip.de/news/CAN-Hacking-Tool-Autos-hacken-fuer-20-Dollar_67066892.html
[Only German]
[2]http://www.can-newsletter.org/engineering/engineering-miscellaneous/140822_list-of-potentially-vulnerable-cars_blackhat/
[3]Advanced Encryption Standard (AES), FIPS PUB 197
[4]CAN with Flexible Data Rate – Specification Version 1.0, Robert Bosch, GmbH; April, 2012
http://www.bosch-semiconductors.de/en/ubk_semiconductors/safe/ip_modules/can_fd/can.html

링크:
벡터 홈페이지: www.vector.com

저자:

아민 하펠(Armin Happel)
Vector Informatik GmbH 의 'Research and Development for Innovative Application' 부서에서 근무하는 수석 소프트웨어 개발 엔지니어로, 보안 응용 분야를 담당하고 있다.

본 자료 배포시 최종 인쇄물을 당사에 보내주시면 감사하겠습니다.
배포와 관련하여 문의사항이 있으시면 언제든지 연락주시기 바랍니다.

벡터코리아 편집자 연락처:
마케팅팀 전은영
서울특별시 용산구 한남대로 11 길 12 고봐스빌딩 5 층
Tel. 02-807-0600 Ext.5014, Fax. 02-807-0601
E-mail: eunyoung.jeon@vector.com