Chapter
02

자동차 사이버보안 표준 및 보안 기술 동향

고의석_MDS인텔리전스 매니저

I. 서론

기존 자동차에서 가장 큰 이슈는 안전(Safety)이었다. 차량에 탑재되는 부품 자체 결함 혹은 오작동에 의한 위험(hazard)에 대해 안전은 운전자의 목숨, 재산 등과 직결되기에 중요하게 다루어졌다.

최근에는 자동차에 정보통신기술이 결합됨에 따라 자동차에서 안전은 기존의 안전 외에 또 다른 안전인 보안(security)이 추가되어 큰 이슈로 다루어지고 있다. 자동차에 적용된 정보통신기술에 대해 보안 취약점(vulnerability)이 식별되고 있으며, 보안 취약점은 곧 보안 위협(threat)으로 연결될 수 있어 보안이 새로운 이슈로 떠오르는 것이다.

많은 해커는 자동차를 대상으로 사이버 공격을 시도했다. 대표적인 사례로는 “지프 체로키 해킹 사건”을 들 수 있다[1]. 정보보안전문가인 찰리 밀러와 클리스 볼로섹이 피아트 크라이슬러사의 자동차인 지프 체로키에 탑재된 ECU(Electronic Control Unit)의 취약점을 이용하여 해킹에 성공한 사례이다. 해당 해킹은 영상으로 공개되었으며, 원격에서 자동차의 기능을 마음대로 제어하는 것을 보여주었다. 실제 해킹 사례가 아닌 보안전문가에 의한 해킹 시연 영상임에도 자동차를 대상으로 한 해킹이 가능하다는 것을 보여주어 큰 이슈가 되었다. 또한, 해킹으로 인해 생명, 재산 등 주요 자산들이 위협받을 수 있다는 것을 보여준 사건이다. 피아트 크라이슬러는 지프 체로키를 비롯한 동일 취약점을 보유한 차종들에 대해 140만 대를 리콜해야 했다. 해당 사건을 계기로 자동차 사이버보안에 대한 필요성이 사회적으로 대두되었다.

* 본 내용은 고의석 매니저 (031-627-3053, nkm@mdsit.co.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

II. 자동차 사이버보안의 법규 및 표준 동향

자동차 사이버보안에 대해 가장 발 빠르게 움직인 기관은 유럽 경제위원회(United Nations Economic Commission for Europe, UNECE)이다. 2020년 6월 UNECE에서는 29번째 Working party를 통해 Regulation No.155를 제정했다[2]. 이후 2021년 1월 유럽에서 Regulation No.155에 대한 법규가 발효되었다. 최초의 자동차 사이버보안 관련 법규이다.

발효된 법규에 따르면, 완성차 제조업체는 CSMS(Cyber Security Management System) 인증과 각 차종에 대한 형식승인을 받아야 한다. 2022년 7월까지 차량 제조사가 출시하는 신차가 형식승인을 받지 못한다면 유럽과 일본에서 차량 판매가 불가능하다. 또한, 2024년까지 모든 차에 대해 차종 형식승인을 받는 것이 필요하며, 형식승인을 받아야 하는 차량 유형으로는 카테고리 M, N, O, L6, L7이 해당한다. UNECE WP.29에서 정의하는 차량 분류 및 의미는 [표 1]과 같다.

[표 1] 차량 카테고리별 의미

차량 카테고리	설명
M	4개 이상의 바퀴를 가지며, 승객 운송에 사용되는 차량
N	4개 이상의 바퀴를 가지며, 화물 운송에 사용되는 차량
O	자체 구동력을 가지고 있지 않으며, 견인 장치가 장착된 트레일러
L6	바퀴가 4개이고, 공차 중량 기준 350kg 이하이며, 최고 속도가 45km/h 이하이거나 전기 엔진 출력이 4kW를 초과하지 않는 차량
L7	L6에 속하지 않는 바퀴가 4개이고, 공차 중량 기준 400kg 이하거나 전기 엔진 출력이 15kW를 초과하지 않는 차량

〈자료〉 UNECE, "Consolidated Resolution on the Construction of Vehicle(R.E.3)," UNECE WP.29, ECE/TRANS/WP.29/78/Rev.3 pp.6-8.

차종 형식승인을 받기 위해서는 CSMS에 대해 인증을 받은 상태이어야 한다. CSMS 인증과 차량 형식승인을 받기 위해서는 두 가지 표준을 준수해야 한다.

1. ISO/SAE 21434:2021

ISO/SAE 21434:2021(ISO/SAE 21434)은 자동차 사이버보안에 대해 엔지니어링 관점에서 보안을 서술하는 것으로 국제표준화기구인 ISO와 미국자동차기술자협회인 SAE가 발

표한 표준이다[3]. UNECE WP.29 Regulation No.155에서 상세 보안 사항은 ISO/SAE 21434 표준을 참조하라고 명시된 만큼 자동차 사이버보안에 중요하게 적용되는 표준으로 알려져 있다. CSMS 인증은 ISO/SAE 21434의 Audit과 형식승인은 Assessment와 대응되기 때문이다.

ISO/SAE 21434 표준에서 자동차 사이버보안은 자산이 외부의 위협 시나리오로부터 충분히 보호된 상태를 의미한다. 이때, 외부 위협 시나리오의 대상은 자동차와 자동차에 특정 기능을 수행하기 위해 탑재되는 전기/전자 부품이다. 따라서 자동차 부품에 대해 위협을 식별하고 위협으로부터 발생하는 리스크를 관리하는 것이 해당 표준의 주된 내용으로 볼 수 있다.

해당 표준에 따르면, 부품 제조사는 자동차 부품의 전체 생명7 주기(개념-제품개발-생산-운영-유지) 동안 발생할 수 있는 위협을 식별하고, 위협에 따른 리스크를 평가할 수 있다. 평가로 인해 예상되는 피해에 따라 조치해야 하는데 위협을 식별하고, 위협에 따른 리스크의 평가는 TARA(Threat Analysis and Risk Assessment)라고 정의된 방법에 따라 진행하도록 명시되어 있다. 이후 평가를 기반으로 V 모델에 따른 개발이 요구된다.

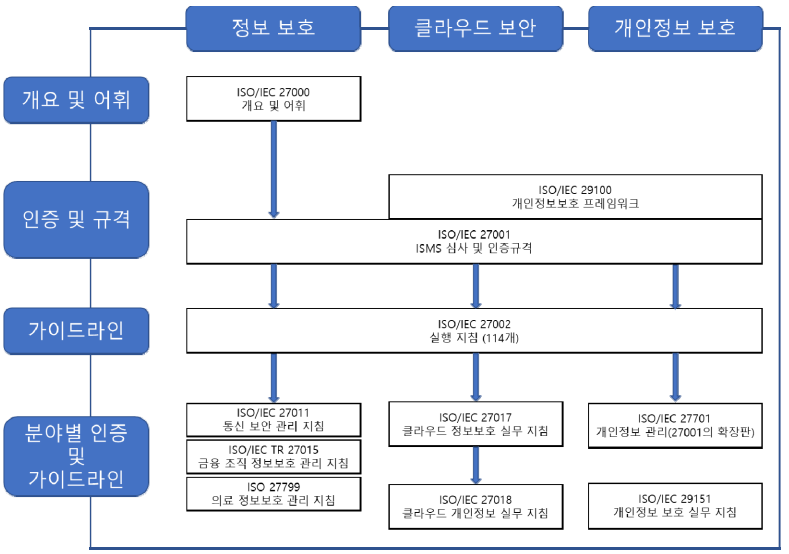
또한, 본 표준에서는 차량의 전기/전자 부품에 대한 보안뿐만 아니라 부품 생산에 필요한 인프라에 대한 보안에 대해서도 고려되어 있으며, 이는 ISO/IEC 27001을 따라야 한다.

2. ISO/IEC 27001:2013

ISO/IEC 27001(ISO 27001)은 정보보호 경영시스템에 대한 보안 표준으로 가장 인정받는 국제 표준이다[4]. 해당 표준은 [그림 1]과 같이 ISMS(Information Security Management Systems) 보안 시리즈에 근간이 되는 표준으로 조직이 설정한 보안 정책 및 목표를 비롯하여 조직 정보 보안에 대해 포괄적으로 규정하고 있다[5].

ISO 27001은 ISO 21434에서 제공되지 않는 차량 부품 공급망에 대한 전반적인 보안을 위해 반드시 필요하다. 다만, 해당 표준은 자동차 산업을 위한 표준이 아니므로 모든 항목을 다 준수할 필요는 없고 주요 항목에 대해 준용하는 것만 요구된다.

자동차 사이버보안을 위해 준수해야 하는 주요 항목은 [표 2]와 같다. 이 중 특히 자동차 및 부품 제조업체들이 가장 중요하게 적용하는 부분은 “암호 키 관리”이다. 자동차 부품 제어기에 이미 들어간 암호 키가 유출된다면, 해당 암호 키를 주입한 모든 자동차는 리콜이 되기 때문에 가장 먼저 고려되고 있다.



〈자료〉 ISO, “Information technology – Security techniques – Information security management systems Overview and vocabulary,” ISO/IEC 27000, 2018, p.19, ‘ISMS family of standards relationships’ 재구성

[그림 1] ISMS 보안 시리즈 도식화

[표 2] ISO 27001에서 암호 키 관리에 대한 준수 사항

A.10 암호화		
A.10.1 암호 통제		
목적: 정보에 대한 기밀성, 인증, 무결성/진본성을 보호하도록 암호화의 적절하고 효과적인 사용을 보장하기 위함		
A.10.1.1	암호 통제 사용 정책	- 통제: 정보보호를 위한 암호 통제의 사용 정책을 개발 및 구현해야 한다.
A.10.1.2	키 관리	- 통제: 암호 키의 사용, 보호, 수명에 대한 전체 생명 주기의 정책을 개발 및 구현해야 한다.

〈자료〉 ISO, “Information technology Security techniques information security management systems Requirements,” ISO/IEC 27001, 2013, p.28, A.10 재구성

III. 보안 기술 동향

위의 표준들에서 이야기하는 사이버 보안을 위해서는 위협을 적절한 수준까지 감소시킬 수 있는 보안 기술이 필요하다. 이러한 보안 기술은 크게 두 파트로 나누어진다. ISO 21434에 대응하기 위한 “자동차 내부에 대한 보안 기술”과 ISO 27001에 대응하기 위한 “공급망에

대한 보안 기술"이 있다.

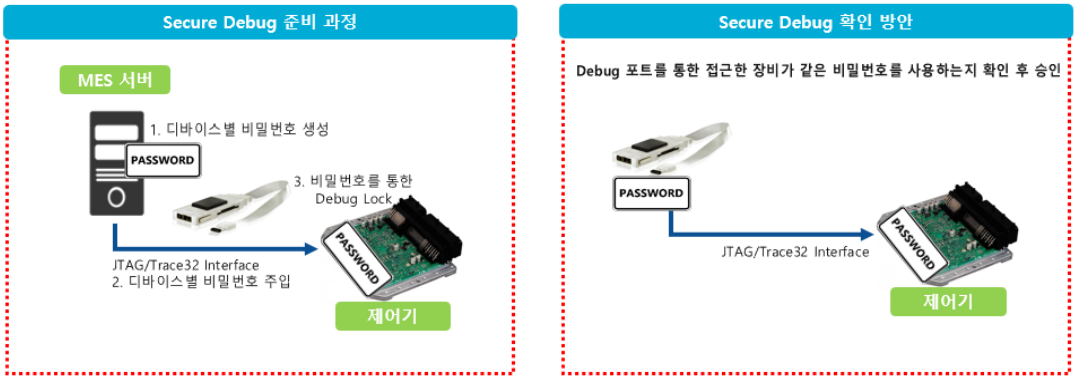
1. ISO 21434 대응을 위한 자동차 내부에 대한 보안 기술

ISO 21434를 만족하기 위해 자동차 내부에 대한 보안 기술이 필요하다. 자동차 내부에 대한 보안 기술은 부품 특성에 맞는 보안 기술이 적용되어야 한다. 자동차 완성차 제조업체와 부품 제조사의 합의를 통해 부품에 적용되어야 하는 보안 기술을 결정한다. 대표적으로 적용되는 보안 기술은 다음과 같다.

가. Secure Debug

자동차 부품 제어기에 존재하는 디버그 포트를 암호 키, 비밀번호 등의 방법으로 막는 보안 대응 방안이다[6].

해커가 디버그 포트를 통해 부품 제어기에 접근한다면 악의적 리버싱, 코드 변조 등 다양한 공격이 시도될 수 있으므로 인증을 받은 사용자 혹은 장비만이 자동차 부품 제어기에 접근할 수 있어야 한다[7]. 인증의 방식은 암호 키 혹은 비밀번호를 사용하는 것이 일반적이다. 제어기에 접근하기 위해서는 제어기 내부 있는 암호 키 혹은 비밀번호와 동일한 값을 제시하도록 하여 안전성을 제공한다. [그림 2]는 비밀번호를 사용하여 Secure Debug를 수행하는 과정이다.



〈자료〉 J. Backer, D. Hely, and R. Karri, "Secure and Flexible Trace-Based Debugging of Systems-on-Chip," ACM Transactions on Design Automation of Electronic Systems, Vol.22, No.2, Article 31, 2016, pp.9-15.

[그림 2] Secure Debug 시나리오 도식화

제어기 내부의 암호 키 혹은 비밀번호는 부품 제어기 내부에 양산 시 주입되어야 하며, 부품 제조사 및 자동차 완성차 제조업체는 이를 보관해야 한다. 이후 제어기에 접근이 필요할 때 해당 암호 키 혹은 비밀번호를 접근 장비에 제공할 수 있어야 한다.

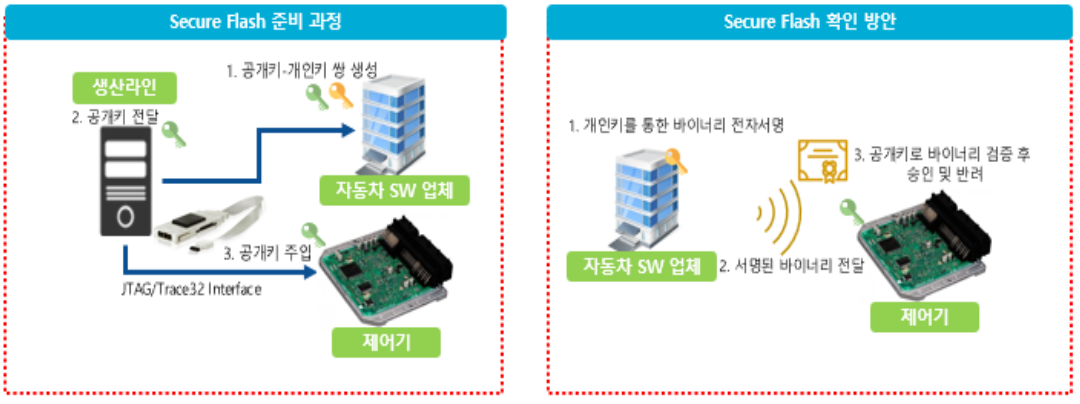
Secure Debug에서 보안성을 결정하는 요소는 암호 키 혹은 비밀번호로 KISA의 “암호 키 관리 안내서”, NIST SP 800-132 등에 적합하게 생성 및 관리되어야 한다[8],[9].

나. Secure Flash

자동차 부품 제어기의 소프트웨어 업데이트가 필요한 경우, 업데이트 예정인 소프트웨어가 승인받은 소프트웨어인지 확인 후 반영하는 보안 대응 방안이다[10].

업데이트 예정인 소프트웨어를 확인하기 위해서는 공개키 암호 기반의 전자 서명과 해시 함수 같은 암호학적으로 안전한 방법이 사용된다. 자동차 소프트웨어 생산업체에서 업데이트 예정인 소프트웨어에 개인키를 사용한 전자서명을 하고, 제어기에서는 사전에 주입된 공개키를 이용하여 전달받은 소프트웨어의 출처를 확인하며, 해시 함수를 사용하여 해당 소프트웨어가 변경되지 않았는지 확인한다. 이를 통해 변경되지 않은 소프트웨어가 정상적인 발송처로부터 온 것을 확인한 후 해당 소프트웨어를 반영한다. 해당 과정은 [그림 3]과 같이 확인할 수 있다.

Secure Flash를 위해서는 자동차 부품 제어기에는 자동차 소프트웨어 생산업체의 공개키



〈자료〉 K. Lemke, C. Paar, and M. Wolf, “Embedded Security in Cars: Securing Current and Future Automotive IT Applications,” Springer, Springer-Verlag Berlin Heidelberg, 2006, p.6 내용 도식화

[그림 3] Secure Flash 시나리오 도식화

가 양산 전 탑재되어야 한다. 공개키는 해당 값이 공개되어도 상관없지만 변조되는 경우 정상적인 Secure Flash 동작이 불가하다. 따라서 정상적인 Secure Flash를 위해서는 공급망 전 과정에서의 공개키의 무결성이 필요하다[11].

다. Secure Boot

자동차 부품 제어기의 소프트웨어적 무결성을 보장할 수 있도록 하는 보안 대응 방안이다. 자동차 부품 제어기에 들어가는 소프트웨어가 주입 전에 변경되어 있다면, 자동차 주행 시 문제가 발생할 위험성이 높고, 부팅 과정에서 메모리에 소프트웨어를 로드하는 동안 무결성을 검증해야 한다[12].

소프트웨어 로드 과정에서 무결성을 검증하는 방법으로는 공개키 암호 기반의 전자서명과 해시 함수 같은 암호학적 방법이 사용된다. 부팅 과정에서 메모리에 소프트웨어를 로드할 때, 해당 소프트웨어의 해시값과 인증서를 공개키로 복호화하여 나온 값이 같다면 로드를 하고 아니라면 로드를 하지 않는 방법이다[13].

라. Secure Access

인증 받은 진단기만 자동차에 장착될 수 있도록 하는 보안 대응 방안이다. Secure Debug가 적용되어 있어도 해커는 진단기를 통해 자동차 부품 제어기에 접근할 수 있다. 이를 제어하기 위해 진단기에 대해 인증을 수행해야 한다. 인증은 Secure Debug와 유사한 방법으로 진행된다.

위와 같은 보안 방식을 적용함으로 자동차 자체에서의 보안을 유지할 수 있지만 한 가지 선행조건이 필요하다. 보안 기술에 적용되는 암호 키, 비밀번호 등 기밀 데이터가 자동차 완성차 제조업체 및 부품 제조사에 안전하게 생성/관리/전달/폐기가 되어야 한다.

2. ISO 27001 대응을 위한 공급망에 대한 보안 기술

자동차 내부에서 보안 기술이 적용되더라도 부품 제조사에서 기밀 데이터가 유출되거나 자동차 완성차 제조업체가 암호 키를 제대로 관리하지 못한다면, 보안 기술의 적용이 무의미해진다. 이를 방지하기 위해서는 ISO 27001 기반의 공급망에 대한 보안 기술이 적용되어야 한다. 대표적 공급망에 적용될 수 있는 보안 기술은 다음과 같다.

가. 암호 키 관리 시스템

자동차 사이버보안의 핵심인 암호 키 및 비밀 데이터를 생성 및 관리함으로 보안을 제공하는 시스템이다. 자동차 부품 제어기에 보안 기술을 적용하기 위해서 제어기의 양산 과정에서 암호 키 및 비밀번호가 주입되기 때문에 가장 먼저 적용해야 할 시스템이다. 주입되는 암호 키 및 비밀번호는 생성, 전달, 보관, 갱신, 폐기 등 전 과정에 걸쳐 안전하게 관리된다. 이를 위해 암호 키는 반드시 개발 및 양산 시스템과 물리적으로 분리된 안전한 공간에 보관해야 하며, NIST SP 800-57[14], NIST SP 800-130[15] 등 암호 키 관련 표준을 준수해야 한다. 특히, 암호 키를 전달할 때는 암호 키에 대한 표준 프로토콜인 KMIP(Key Management Interoperability Protocol)을 준수해서 전달하는 것이 중요하다[16].

나. 사설 인증 시스템

자동차 완성차 제조업체와 자동차 부품 제조사, 2차 부품 제조사 등 자동차 공급망 전 과정에 상호 인증을 통해 보안을 제공하는 시스템이다. 암호 키 관리 시스템은 단독 구성 시, 사용하는 업체에 대해서만 안전한 관리가 된다는 한계가 존재한다. 이러한 한계를 극복하기 위해 사설 인증 시스템이 필요하다[17]. 인증 시스템은 암호 키를 전달한 업체에 대한 정보와 암호 키의 무결성 정보 등을 담은 인증서를 기반으로 안전하게 암호 키를 공유할 수 있는 환경을 제공한다. 사설 인증 시스템과 암호 키 관리 시스템을 결합하면, 자동차 공급망 전 과정에 안전한 암호 키 및 기밀 데이터 공유가 가능하다.

다. 분리 기법

주요 정보에 접근할 수 있는 인원 및 시스템을 최소화하여 보안을 제공하는 기법이다[18]. 방화벽과 같은 망 분리나 비밀 취급 인가 등급에 따른 정보 접근 등의 방법을 통해 분리 기법 적용이 가능하다.

자동차 생산 환경에서는 암호 키를 기준으로 분리해야 한다. 자동차 사이버보안에서 암호 키는 통상 개발용 암호 키와 양산용 암호 키로 나누어진다. 개발 망과 양산/운영 망을 분리하여 개발용 암호 키와 양산용 암호 키가 혼용을 막고, 개발자와 양산 담당자 등 각 담당자들이 해당하는 암호 키만 가져갈 수 있게 하는 것으로 분리 기법을 적용할 수 있다.

IV. 자동차 보안 기술 적용 동향

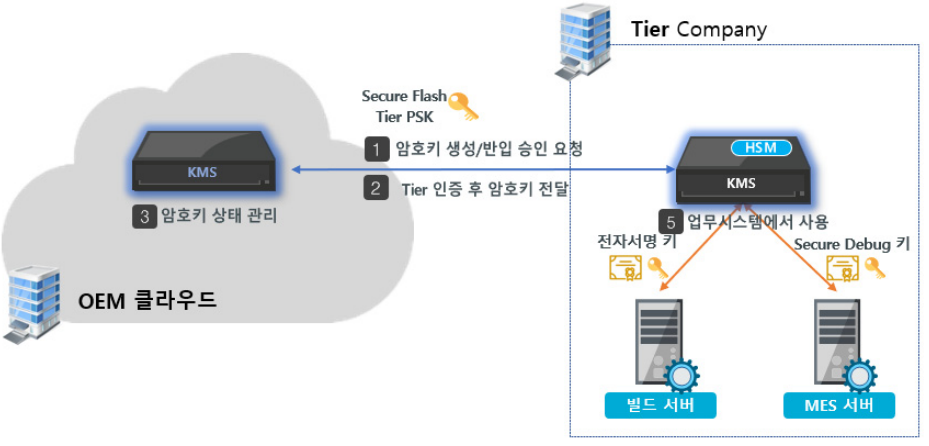
위의 보안 기술들을 모든 자동차 및 부품 제조업체가 적용하는 것이 이상적이다. 하지만 비용, 인력 등의 문제로 모든 보안 기술을 적용하기는 어려우므로, 자동차 완성차 제조업체들은 보안 요구사항을 부품별로 정해두고 보안 요구사항을 만족하도록 요구하고 있다.

본 절에서는 실제 국내외 자동차 완성차 제조업체의 보안 요구사항을 만족하기 위해 현업에 적용된 보안 기술 중 일부를 소개한다.

1. 클라우드 기반의 암호 키 및 주요 데이터 전달

해외 한 자동차 완성차 제조업체의 경우, 부품 제조사에 암호 키 및 주요 데이터를 전달하는 과정에 클라우드 웹을 통한 배포 방법을 사용한다. 이는 자동차 부품 제어기에 Secure Flash, Secure Debug 등 앞서 설명한 자동차 내부의 보안 기술 적용을 위해 배포하며, 방식은 암호 키 관리 시스템과 사설 인증 체계를 기반으로 클라우드 웹을 구성하고 해당 웹을 통해 부품 제조사가 암호 키 및 주요 데이터를 받아가도록 한다. 이때 부품 제조사 또한 암호 키 관리 시스템과 사설 인증 기능을 반드시 구축하고 이를 활용하여 보안을 유지하며 받아가도록 요구한다.

[그림 4]의 경우 해외 자동차 완성차 제조업체의 보안 요구사항 중 클라우드 기반의 암호



〈자료〉 고의석, 고객사 구축 사례 도식화, MDS 인텔리전스, 2022.

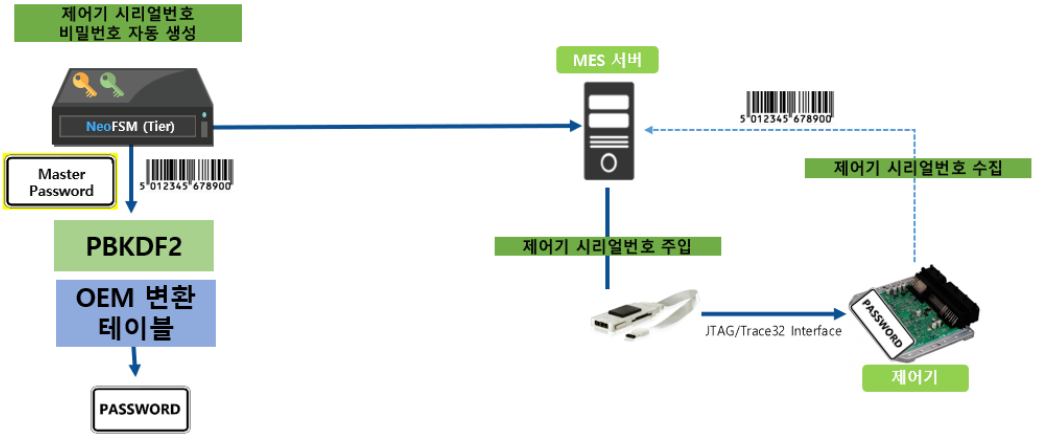
[그림 4] 클라우드를 통한 암호 키 및 주요 데이터 전달 과정

키 전달 체계를 도식화한 내용이다. [그림 4]를 보면, 자동차 부품 제조업체(도식도 상 Tier) 암호 키 관리 시스템은 자동차 완성차 제조업체(도식도 상 Original Equipment Manufacturer: OEM)의 클라우드 키 관리 서비스와 연동되어 암호 키가 필요할 때 받아가도록 구성되어 있다. 자동차 완성차 제조업체의 암호 키 관리 시스템은 부품 제조사의 암호 키 관리 시스템에 인증서를 확인하고 전달한다. 이 과정에서 인증서가 사용되기 때문에 사설 인증 기능이 있는 암호 키 관리 시스템을 사용하고 있다.

2. 제어기별 자체 비밀번호 생성/관리

해외 업체의 경우, 부품 제조사에 Secure Debug를 위해 자체적으로 비밀번호를 생성/관리하도록 요구한다. 이때 비밀번호를 생성하는 방식은 NIST 승인 알고리즘 중 PBKDF2와 자체 보안 테이블을 사용한다. PBKDF2에 메인 비밀번호와 디바이스 고유 시리얼 번호 등 변수들을 집어넣고 1차 변환 키를 유도한다. 이 1차 변환 키는 자동차 완성차 업체의 자체 변환 프로토콜을 통해 최종 비밀번호로 변환된다. 이때 부품 제조사는 비밀번호 생성에 필요한 메인 비밀번호는 반드시 암호 키 관리 시스템을 통해 보관해야 하며, 부품 제어기별로 모두 다른 비밀번호를 완성차 제조업체의 요청에 따라 전달할 수 있도록 해야 한다.

[그림 5]는 해외 자동차 완성차 제조업체의 보안 규격에 맞춰 자동차 부품 제조업체가



〈자료〉 이동재, 박성진, “NeoFSM을 활용한 CSMS 암호키/인증서 관리 방안”, 한컴인텔리전스, Automotive SW Conference, 2022, p.6.

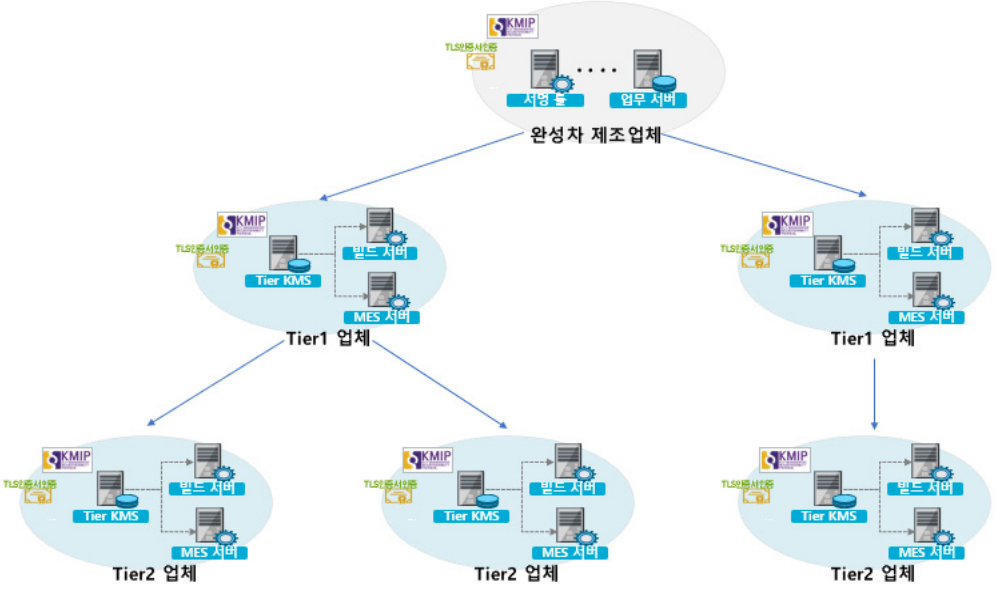
[그림 5] Secure Debug를 위한 제어기별 비밀번호 생성/주입/관리 사례 도식화

Secure Debug를 적용한 방안이다. 해당 부품 제조업체는 제어기의 고유값을 자동으로 스캔하여 키 생성/관리 서버인 NeoFSM에 전달을 한다. NeoFSM은 고유값에 맞는 비밀번호를 NIST 표준과 해외 자동차 완성차 업체의 기준에 맞춰 만들어진 비밀번호는 제어기에 주입되어 Secure Debug를 위해 사용된다.

3. 기밀 데이터 전송 환경 구축

또 다른 업체의 경우, 타 업체와 기밀 데이터를 주고받기 위한 목적으로 기밀 데이터 전송 환경 구축을 시도하고 있다. 이를 위해, 업체별 암호 키 관리 시스템 간의 연동을 추진하고 있고, 연동을 위한 프로토콜로는 KMIP를 선정하였다. KMIP는 암호 키 전달을 위한 시스템 연동을 편하게 하는 것과 더불어 안전한 키 관리에 내용을 포함하는 프로토콜이기 때문에 해당 프로토콜을 선정하였다.

안전한 기밀 데이터가 공유 가능한 환경은 [그림 6]과 같다. 이는 국내외 자동차 완성차 제조업체의 보안 정책 문서를 기반으로 구성한 환경이다. 트리 구조의 암호 키 관리 체계를



〈자료〉 이동재, 박성진, “NeoFSM을 활용한 CSMS 암호키/인증서 관리 방안”, 한컴인텔리전스, Automotive SW Conference, 2022, p.8.

[그림 6] 기밀 데이터 전송 환경 도식화

통해 각 참여 업체별 관리는 물론 자동차 완성차 제조업체의 통합 관리 기능까지 제공할 수 있다.

V. 결론

본 고에서는 자동차 사이버보안에 대한 법규 및 표준과 이를 위한 보안 기술 및 현업 사례에 대한 전반적인 동향을 살펴보았다. 자동차 사이버보안은 크게 두 가지로 분류된다. 차량 내부에서의 보안과 자동차 및 부품 제조사를 포함하는 공급망에서의 보안이다. 차량 내부에서의 보안은 Secure Boot, Secure Debug, Secure Flash 등이 있으며 모두 암호에 기반을 둔 방식이라 암호 키가 중요하다는 것을 확인할 수 있었다. 차량 내부에서의 보안은 암호 키에 따라 보안 강도가 결정된다. 암호 키의 보안 강도를 일정 수준 이상 유지하기 위해서 자동차 및 부품 제조사를 포함하는 공급망 전체에서의 보안이 필요한 것 또한 확인했다. 공급망에서 암호 키를 잘 관리하는 방법으로는 암호 키 관리 시스템, 사설 인증 시스템, 망 분리, 인증을 받은 프로토콜 등의 방식이 필요하다. 결론적으로 자동차 및 부품 제조업체는 인증을 받은 프로토콜을 쓰는 암호 키 관리 시스템에 사설 인증 시스템이 결합된 체계를 망 분리해서 도입하는 것이 가장 이상적인 보안 방법으로 사료된다.

자동차 사이버보안은 자율주행 기술이 발전함에 따라 점점 더 중요성이 높아질 것으로 예측된다. 글로벌리서치 회사 MarketsandMarkets는 글로벌 자동차 사이버보안 시장의 규모를 2021년 20억 달러에서 2026년 53억 달러로 증가할 것으로 전망한다[19]. 자동차 사이버보안 시장이 증가함에 따라 다양한 보안 기술 추가될 것이다. 본 고에서 소개한 자동차 사이버보안에 주요 요소들을 바탕으로 진보된 보안 기술이 계속해서 등장하기를 희망한다.

참고문헌

[1] C. Miller, and C. Valasek, “Remote exploitation of unaltered passenger vehicle,” Black Hat USA, 2015, p.6.
[2] UNECE WP.29, “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system,” UN Regulation, No.155, 2021, p.1.
[3] ISO, “Road vehicles Cybersecurity engineering,” ISO/SAE 21434, 2021, pp.1-81.
[4] ISO, “Information technology Security techniques information security management systems

Requirements," ISO/IEC 27001, 2013, p.28.
[5] ISO, "Information technology - Security techniques - Information security management systems Overview and vocabulary," ISO/IEC 27000, 2018, pp.18-19.
[6] J. Backer, D. Hely, and R. Karri, "Secure and Flexible Trace-Based Debugging of Systems-on-Chip," ACM Transactions on Design Automation of Electronic Systems, Vol.22, No.2, Article 31, 2016, pp.9-15.
[7] 국토교통부, "자동차 사이버보안 가이드라인", 2020, p.51.
[8] 한국인터넷진흥원, "암호키 관리 안내서", 2014, pp.28-29.
[9] NIST SP 800-132, "Recommendation for Password-Based Key Derivation," Dec. 2010, pp.5-8.
[10] K. Lemke, C. Paar, and M. Wolf, "Embedded Security in Cars: Securing Current and Future Automotive IT Applications," Springer, Springer-Verlag Berlin Heidelberg, 2006, p.6.
[11] R. L. Rivest, A. Shamir, and L. Aldleman, "A menthod for obtaining digital signatures and public-key cryptosystems," Communications of the ACM Vol.21, 1978, pp.120-126.
[12] S. Sanwald et al., "Secure Boot Revisited: Challenges for Secure Implementations in the Automotive Domain," SAE Int. J. Transp, Cyber & Privacy, 2019, pp.69-81.
[13] R. Wikins, and B. Richardson, "UEFI secure boot in modern computer security solution," UEFI Forum, 2013, p.7.
[14] E. Barker, "Recommendation for Key Management," NIST SP 800-57 Part.1 Rev.4 2016, pp.1-5.
[15] E. Braker at el., "A Framework for Designing Cryptographic Key Management Systems," NIST SP 800-130, 2013, pp.1-112.
[16] T. Cox, "Key Management Interoperability Protocol Specification Version 1.4," OASIS, Open, 2017, pp.1-242.
[17] Y. DaeHyun, and L. PilJoong, "Identity-Based Cryptography in Public Key Management," European Public Key Infrastructure Workshop, EuroPKI 2004: Public Key Infrastructure, 2004, pp.71-84.
[18] N. Mhaskar, M. Alabbad, and Ridha Khedri, "A Formal Approach to Network Segmentation," ELSEVIER, Computers&Security Vol.103, 2021, p.1.
[19] MarketsandMarkets, "Automotive Cybersecurity Market," MARKET RESEARCH REPORT, 2022, p.369.