한국ITS학회논문지 J. Korea Inst. Intell. Transp. Syst.

사례 분석을 통한 IVN의 필수 보안 요구사항 도출

Deriving Essential Security Requirements of IVN through Case Analysis

송 윤 근* · 우 사 무 엘** · 이 정 호*** · 이 유 식****

* 주저자 : 에스크립트 사이버보안사업팀
** 공저자 : 한국전자통신연구원 초연결통신연구소
*** 공저자 : 한국정보인증 서비스운영팀
**** 교신저자 : 에스크립트 사이버보안사업팀

Yun keun Song* · Samuel Woo** · Jungho Lee*** · You sik Lee****

* Cyber Security Division, ESCRYPT
** Electronics and Telecommunications Research Institute(ETRI)
*** Korea Information Certificate Authority Inc.(KICA)
**** Cyber Security Division, ESCRYPT
† Corresponding author : You sik Lee, yousik.lee@escrypt.com

Vol.18 No.2(2019)
April, 2019
pp.144~155

pISSN 1738-0774
eISSN 2384-1729
https://doi.org/10.12815/kits.2019.18.2.144

Received 1 April 2019
Revised 18 April 2019
Accepted 26 April 2019

요 약

오늘날 자동차 산업의 화두 중 하나는 자율주행차량이다. 국제자동차기술자협회(SAE International)가 정의한 레벨 3이상을 달성하기 위해서는 자율주행 기술과 커넥티드 기술의 조화가 필수적이다. 현재의 차량은 자율주행과 같은 새로운 기능을 가지게 됨에 따라 전장 부품의 수뿐 만 아니라 소프트웨어의 양과 복잡성도 늘어났다. 이로 인해 공격 표면(Attack surface)이 확대되고, 소프트웨어에 내재된 보안 취약점도 늘어나고 있다. 실제로 커넥티드 기능을 가진 차량의 보안 취약점을 악용하여 차량을 강제 제어할 수 있음이 연구자들에 의해 증명되기도 했다. 하지만 차량에 적용 되어야 하는 필수적인 보안 요구 사항은 정의되어 있지 않는 것이 현실이다. 본 논문에서는 실제 공격 및 취약점 사례를 바탕으로 차량내부네트워크(In-Vehicle Network)에 존재하는 자산을 식별하고, 위협을 도출하였다. 또한 보안요구사항을 정의 하였고, 위험 분석을 통해 사이버 보안으로 인한 안전 문제를 최소화하기 위한 필수 보안 요구 사항을 도출하였다.

핵심어 : 위험분석, 차량내부네트워크, 보안요구사항, 자율주행차량

ABSTRACT

One of the issues of the automotive industry today is autonomous driving vehicles. In order to achieve level 3 or higher as defined by SAE International, harmonization of autonomous driving technology and connected technology is essential. Current vehicles have new features such as autonomous driving, which not only increases the number of electrical components, but also the amount and complexity of software. As a result, the attack surface, which is the access point of attack, is widening, and software security vulnerabilities are also increasing. However, the reality is that the essential security requirements for vehicles are not defined. In this paper, based on real attacks and vulnerability cases and trends, we identify the assets in the in-vehicle network and derive the threats. We also defined the security requirements and derived essential security requirements that should be applied at least to the safety of the vehicle occupant through risk analysis.

Key words : Risk analysis, In-Vehicle Network, Security requirements, Connected vehicle

Ⅰ. 서 론

1. 개요

오늘날 자동차 산업은 전동화(electrified), 자율주행(autonomous driving), 공유(shared), 커넥티드(connected), 연간 업데이트(yearly updated)라는 키워드와 함께 차량-ICT 융합이 가속화 되고 있다. 이러한 변화에 맞춰 차량에는 ADAS(Advanced Driver Assistance Systems), V2X(Vehicle to Everything)와 같은 기능이 탑재 되고 있으며, 하나의 기계적 장치에서 첨단 ICT기기로 변모하고 있다. (PwC GmbH, 2018; Hiro, 2012)

글로벌 컨설팅회사 PwC의 보고서에 의하면, 2030년에는 51퍼센트의 차량이 레벨 3 이상의 자율주행기능을 탑재 할 것으로 전망하고 있으며, 국제자동차기술자협회(SAE international)에서는 차량의 자율주행 기능의 수준에 따라서 0단계부터 5단계 까지 총 6단계로 정의하고 있다. 자동운전 시스템(ADS)이 차량 주변 환경을 파악하여, 스스로 차량을 제어하는 레벨 3 이상의 자율주행을 실현하기 위해서는 커넥티드 기술과 센서 기반의 자율주행 기술의 유기적인 결합이 필수적이다. 미국 교통부(US DoT)에서는 이를 CAV(Connected and Automated Vehicle)라고 한다. (SAE International, 2018; US DoT, 2017; PwC GmbH, 2017)

CAV는 자율주행을 위한 새로운 기능을 가지게 됨에 따라 전장 부품의수 뿐만 아니라 소프트웨어의 양과 복잡성이 증가되고, 이에 따른 구현상의 취약점이 증가한다. 또한 CAV가 가지는 다양한 연결성은 공격의 접근점이 되는 공격 표면(attack surface)를 확대 시키는 결과를 초래 하는데, 실제 Charlie Miller와 Chris Valasek은 실차 기반의 취약점 분석과 해킹을 통해 차량을 원격에서 강제 제어함으로써 CAV의 위험성이 증명되었다. (Charlie and Chris, 2015)

차량의 안전(safety)을 보장하기 위해서는 기능 안전성과 더불어 사이버 보안(cyber security)이 중요한 요소가 되었다. 이에 사이버 보안을 위해 보호해야 할 자산과 위협을 올바르게 인식하고, 위험을 분석하여 보안 대책을 적용하는 것이 필요하다. 안전한 자동차 생태계를 위해서는 모든 보안 대책을 적용하는 것이 좋지만, 비용적인 측면에 의해서 현실적으로 적용의 한계성을 가지고 있다.

본 논문에서는 이러한 현실적 한계성을 이해하고, 차량의 사이버 보안을 보장하기 위해서 필수로 적용해야 하는 필수 보안 요구 사항을 제시하고자 한다. 연구 방법은 다음과 같다. 2장에서는 실제 차량을 대상으로 하는 공격 사례와 취약점을 분석한다. 3장에서는 이전 장의 분석 결과를 참고하여 차량에 존재하는 자산, 위협을 식별하고, 보안 목표를 도출한다. 그리고 보안 목표에 대한 위험 평가를 수행한다. 4장에서는 위험 평가 결과를 기반으로 차량에 필수적으로 적용되어야 하는 필수 보안 요구사항을 도출하고, 5장에서 관련연구를 살펴본 뒤 6장에서 결론을 맺는다.

Ⅱ. 사이버 보안 취약점 및 공격 사례 분석

차량을 대상으로 하는 사이버 공격 사례는 2010년 Washington & California 대학교의 CAN(Controller Area Network) 패킷 분석 논문에서부터 알려졌다. 초기에는 차량 내부에 물리적으로 접근하여 공격이 수행된 반면, 현재는 차량에 존재하는 다양한 외부인터페이스와 소프트웨어적 취약점을 이용하여 원격지에서 차량에 대한 공격을 수행하는 것이 특징이다. (Karl et al., 2010)

본 논문에서는 세 가지 기준으로 차량의 취약점과 공격 사례를 수집하였다. 첫 번째는 차량의 사이버 보안 문제로 인해 사회 및 산업계에 큰 영향을 준 공격 사례이고, 두 번째는 저명한 학술적 논문 또는 블랙 햇

(Black hat)과 같은 컨퍼런스에서 발표된 공격 사례이다. 마지막은 모든 사이버 보안 취약점 리스트가 관리되는 C.V.E(Common Vulnerabilities and Exposures)에 등록된 취약점이다. <Table 1>은 수집한 취약점과 공격 사례를 나타낸다.

수집한 보안 취약점과 공격 사례는 차종, 공격자 그리고 공격 시기가 모두 다르지만, 크게 네 가지 공격분류로 추상화 할 수 있다. 첫째는 ECU에 악성 펌웨어를 플래싱(flashing)하는 것이다. 우선 공격자는 ECU의 펌웨어를 추출, 분석하여 공격에 사용할 취약점을 찾는다. 이를 기반으로 악의적인 펌웨어를 제작한 뒤 ECU에 강제로 플래싱하여 차량을 공격하는 방법이다. 이러한 방법은 펌웨어 추출부터 분석까지 많은 시간을 필요로 하며, 리버스 엔지니어링을 위한 전문지식을 필요로 한다. 뿐만 아니라 악의적으로 제작된 펌웨어를 ECU에 강제로 플래싱하기 위해 다양한 취약점을 활용할 줄 알아야 한다. <Table 1>에서 제시된 AT.03, AT.06이 이에 해당하는 공격 사례이다. 둘째는 차량의 ECU는 모두 정상인 상태에서 외부 인터페이스를 통해 차량에 전달되거나 차량내부네트워크의 데이터를 재전송(replay)하거나 재전달(relay)하여 차량을 공격하는 방법으로 <Table 1>의 AT.01 AT.05, AT.07이 해당되는 공격 사례이다. 셋째는 ECU의 펌웨어와 전달되는 데이터도 모두 정상인 상태에서 수행된다. 이는 차량 디자인 단계에서부터 잘못 설계된 보안정책을 악용하는 것으로 취약한 Wi-Fi 패스워드를 이용하거나 하드 코딩된 암호학적 정보로 인해서 발생하는 공격으로 <Table 1>의 AT.04가 해당된다. 넷째는 차량에 악성코드를 감염시켜, 정상적인 기능 동작을 저해시키는 공격으로, <Table 1>의 AT.02가 이에 해당 된다. 차량이 하나의 IT기기로 변모 하면서 공격의 다양성 또한 늘어났다. 차량이 다양한 외부 인터페이스와 높은 컴퓨팅 파워를 소유하게 됨에 따라 랜섬웨어(ransomware)와 같은 악성코드에 차량이 감염 될 수 있다는 점이다. 특히 위급한 상황에서 엠뷸런스나 소방차가 랜섬웨어에 감염된다면, 이는 지금까지의 공격 사례들처럼 차량 한 대 또는 차량의 소유주에만 국한된 문제가 아닌 사회전반적인 문제로 대두 될 수 있다.

<Table 1> Vulnerabilities and cyber attacks

Index	Year	Vulnerabilities and cyber attacks
AT.01	2019	Forced vehicle control through Android app repackaging in connected car environment. (Yousik. L et al., 2019)
AT.02	2018	Infect infotainment system with Ransomware, prevent vehicle start-up, and demand money. (Marko W, 2018)
AT.03	2017	Using Tesla's web browser vulnerability, it modifies the firmware and remotely controls the vehicle. (Sen. N et al., 2017)
AT.04	2016	Mitsubishi outlander vehicle control using Wifi module vulnerability in vehicle. (Pen Test Partners, 2016)
AT.05	2016	Remote Key Entry (RKE) Door signal control via RF signal relay. (Conde Nast, 2017)
AT.06	2015	Using Jeep Cherokee's infotainment system vulnerability, it modifies the firmware and controls the vehicle remotely. (Charlie. M and Chris. V, 2015)
AT.07	2013	Vehicle control through CAN packet reversing and packet retransmission of Toyota Prius vehicles. (Charlie. M and Chris. V, 2013)
VUL.01	2018	CAN message can be injected into IVN using vulnerability of infotainment system of BMW vehicle. (CVE, 2018a)
VUL.02	2018	Vulnerability in the update mechanism of the Subaru StarLink head unit can be used to flash malicious firmware. (CVE, 2018b)
VUL.03	2018	Using the Mercedes Benz app vulnerability for iOS to control remote parking pilots, unlock vehicles or get location information. (CVE, 2018c)
VUL.04	2018	Vulnerability of the Tesla vehicle's Passive Keyless Entry and Start (PKES) system (using unsafe algorithms and key lengths). (CVE, 2018d)
VUL.05	2018	Unauthorized firmware update and CAN message injection due to Volkswagen app vulnerability. (CVE, 2018e)
VUL.06	2017	Personal information leaked due to hard-coded cryptographic key in mobile app (CVE, 2017)

Ⅲ. 위험 분석(Risk Analysis)

2장에서는 자동차를 대상으로 하는 사이버 보안 취약점 및 공격 사례에 대해서 살펴보았다. 본 장에서는 차량 보안을 위해 필요한 보안 요구 목표(Security Goals)와 위험도를 판별하였다. 본 장의 연구는 4단계에 걸쳐 진행되었는데, 1단계는 사이버 보안의 기본인 보호해야 할 대상인 보안 자산(Security Assets)을 식별하였다. 2단계에서는 취약점과 공격 사례에서 도출된 위협에 대응하기 위해서 각 자산 별 보안 목적(Security Objectives)을 정의하였고, 3단계에서는 보안 목표가 침해될 경우, 그 위험도를 평가하기 위한 위험 평가 매트릭스에 대해서 설명하고, 4단계에서는 보안 목표와 보안 목표가 침해될 경우에 대한 위험도를 평가하였다.

1. 보안 자산(Security Assets)

보안자산은 차량에 존재하는 보안적인 관점의 '가치 있는' 것을 의미하며, 차량에 저장된 개인정보에서부터 ECU 소프트웨어, ECU간 통신 데이터가 모두 포함된다. 공격자가 차량에 대한 공격을 수행하는 과정은 복합적이고, 공격 벡터는 다양하지만 그들이 최종적으로 취하고자 하는 데이터는 결국 차량에 존재하는 보안 자산이다. 이처럼 보안 자산은 공격자의 최종 목표가 된다. <Table 2>는 보안 자산을 정리한 것이다.

사이버 보안 취약점 및 공격 사례를 기반으로 식별한 보안 자산은 ECU 소프트웨어, 통신 데이터, 유저 데이터이다. ECU소프트웨어는 마이크로컨트롤러(MCU)에서 동작하는 펌웨어와 애플리케이션프로세서(AP)에서 동작하는 OS, 애플리케이션 소프트웨어를 모두 포함한다. 이 보안 자산은 차량 제조사에 의해서 차량 개발/생산 단계에서 생성된다. 통신 데이터는 차량 내/외부의 구성요소 간 통신 시 생성되는 데이터로, 유/무선으로 전송되는 모든 데이터를 의미한다. 이 보안 자산은 차량이 운행됨에 따라 차량에 의해 생성한다. 유저 데이터는 차량 소유자의 행위에 따라서 차량이 생성하는 보안 자산이며, 차량과 차량 소유자의 디바이스 간의 연결성이 확립됨에 따라 생성되는 전화번호부, 통화목록, 문자메시지 내용과 같은 개인정보가 포함된다.

<Table 2> Security Assets

Index	Security Assets	Created by	When
AS.ECU	ECU Software	OEM	Production phase
AS.CD	Communication Data	Vehicle(ECU)	Post-production phase
AS.UD	User Data	Vehicle owner	

2. 보안 목적(Security Objectives)

1) 보안 목적 개요

보안목적은 보안자산의 안전을 보장하기 위해 궁극적으로 달성하고자 하는 최종 목적을 말한다. 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)으로 대변되는 CIA Triad 뿐만 아니라 인증(Authenticity)와 최신성(Freshness)를 추가하여 자산에 필요한 보안 목적을 정의했다. <Table 3>은 정의한 보안 목적을 나타낸다.

<Table 3> Security Objectives

Index	Security Objectives	Corresponding Threats
SO.CONF	Confidentiality	Leakage of data
SO.INTE	Integrity	Modification/Fabrication of data
SO.AVAL	Availability	Denial of service/data
SO.AUTH	Authenticity	Impersonation, Access bypass
SO.FRES	Freshness	Retransmit of data

2) 자산 별 보안 목적

<Table 4>는 자산 별 필요한 보안 목적을 나타내고 있다. 특히 많이 알려진 테슬라 해킹 사례(<Table 1>의 AT.03)나 지프 체로키 해킹 사례(<Table 1>의 AT.06)에서의 핵심은 ECU 소프트웨어를 분석하여 취약점을 알아내고, 이를 이용하여 차량에 악의적인 ECU소프트웨어를 주입하여 발생한 공격이다. 이는 ECU software의 분석과 위/변조, 그리고 인증 없이 ECU에 주입할 수 있었기 때문에 발생한 사례이다. 이에 ECU소프트웨어는 기밀성, 무결성, 가용성, 인증을 제공하는 것이 보안 목표라고 할 수 있다. ECU software의 조작 없이 차량 내부 네트워크로 전송되는 데이터를 분석하고, 악용하는 사례가 발생하고 있다. 예를 들어, 공격자는 정상적인 가속 상황의 데이터를 캡처한 뒤 공격자가 원하는 시점에 캡처한 데이터를 재전송하여 차량을 공격하거나 새로운 메시지를 생성 후 차량 내부 네트워크로 전송하여 공격을 수행할 수 있다. 이에 통신 데이터에 대한 보안 목표는 기밀성, 무결성, 가용성, 인증, 최신성이라고 할 수 있다. 최신 차량에는 블루투스 등을 통해 모바일 폰과 차량이 연결성을 확립할 수 있는데, 이 때 폰에 있는 전화번호부 목록, 문자 메시지 등과 같은 유저 데이터가 차량에 저장되게 된다. 이 데이터에 대해서는 공격자가 데이터의 취득하더라도 의미를 해석할 수 없도록 기밀성을 제공해야 한다.

<Table 4> Security Assets and Security Objectives

Assets	Security Objectives	Vulnerabilities and cyber attacks
ECU Software	Confidentiality	AT.03, AT.06
	Integrity	AT.03, AT.06
	Availability	AT.02
	Authenticity	AT.03, AT.04, AT.06, VUL.02, VUL.05
Communication Data	Confidentiality	AT.01, VUL.03
	Integrity	AT.01, AT.03, VUL.01
	Availability	AT.02
	Authenticity	AT.01, AT.02, AT.05, VUL.01
	Freshness	AT.01, VUL.01
User Data	Confidentiality	VUL.03

3. 위험 평가 매트릭스(Risk Assessment Matrix)

위험 평가 매트릭스는 정량적으로 위험을 판단하기 위한 기준이 된다. 이러한 위험 평가 매트릭스는 공격으로 인해 예상되는 피해(Damage Potential)와 공격의 예상 빈도(Attack Potential)를 기준으로 위험의 심각도를 평가 하고, 최종적으로 해당 위험에 알맞은 보안 대책을 적용할 수 있도록 도움을 준다.

1) Attack Potential(AP) / Damage Potential(DP)

Attack Potential(AP)은 자산에 대한 잠재적 공격의 가능성을 나타내는데, 이는 공격을 수행 하는 것이 얼마나 어려운가를 나타내는 지표이다. AP는 공격 소요시간, 전문지식, 대상에 대한 지식, 장비, 접근 방법과 같은 다섯 가지 항목에 의해 판단된다. 이는 공통 평가기준(Common Criteria, CC)을 기반으로 한다. (ISO/IEC 15408, 2017)

Damage Potential(DP)은 자산에 대한 공격으로 인해 받을 수 있는 모든 손실을 나타내는 지표이다. DP는 안전(Safety), 경제적인 관점, 운영과 같은 세 가지 항목에 의해 판단된다. (Marko and Michael, 2012)

2) 위험 평가 매트릭스(Risk Assessment Matrix) 구성

최종적인 위험의 심각도는 AP와 DP의 조합으로 결정된다. 조합에 따라 해당 위험이 무시할 만한 수준 또는 매우 치명적인 수준임을 인지 할 수 있고, 이를 통해 보안 요구사항 적용에 대한 의사 결정에 도움을 줄 수 있다. <Table 5>는 분류된 AP와 DP를 기준으로 최종적인 위험도를 판단하는 기준을 나타낸다. 위험도는 허용할 수 없는 수준(Inacceptable), 판단이 필요한 수준(Undesirable), 감내할만한 수준(Tolerable), 크게 중요하지 않은 수준(Negligible)으로 나뉘는데, 수용할 수 없는 수준의 위험은 반드시 보안 대책을 마련하여 해당 위험을 줄여야 하는 항목이다.

<Table 5> Risk assessment matrix

DP / AP	Insignificant	Medium	Critical	Catastrophic
Basic	Undesirable	Inacceptable	Inacceptable	Inacceptable
Enhanced Basic	Tolerable	Undesirable	Inacceptable	Inacceptable
Moderate	Tolerable	Undesirable	Inacceptable	Inacceptable
High	Negligible	Tolerable	Undesirable	Inacceptable
Beyond high	Negligible	Negligible	Tolerable	Inacceptable

4. 위험 평가(Risk Assessment)

자산별 보안 목표가 침해될 경우, 그 위험의 정도를 위험 평가 매트릭스를 이용하여 도출하였다. 공격 트리(Attack tree)를 구성하여 자산 별로 보안 목표가 침해 당할 수 있는 방법을 알아보고, 위험 평가 매트릭스를 이용하여 위험도를 산정하였다.

1) 위험 개요(Risk Overview)

<Table 6>는 보안 목표에 대한 위험 평가 결과를 보여주고 있다. 전체 10개의 보안 목표 중 6개가 '허용할 수 없는(Inacceptable)' 수준의 위험으로 판단되었다. 위험도 산정에서 가장 큰 영향을 주는 것은 DP(Damage Potential)에 포함되어 있는 안전(Safety)요소이다. 사이버 보안 위협으로 인해 생명에 조금이라도 영향을 주는 경우 이는 '허용할 수 없는(Inacceptable)' 수준의 위험도로 판단된다. ECU 소프트웨어의 무결성, 인증 그리고 통신 데이터의 무결성, 인증, 신선성이 침해 될 경우 공격자에 의해 차량 강제 제어의 위험이 존재하고 생명에 위험을 줄 수 있기에 모두 '허용할 수 없는(Inacceptable)' 수준의 위험임을 확인 할 수 있다. ECU 소프트웨어의 가용성은 랜섬웨어로 인해 침해될 수 있는데, 이는 생명의 직접적인 영향은 없지만, 경제적, 운영적 손실을 초래할 수 있고, 공격의 수행이 비교적 쉬운 편이기에 이 또한 '허용할 수 없는(Inacceptable)' 수준의 위험이다.

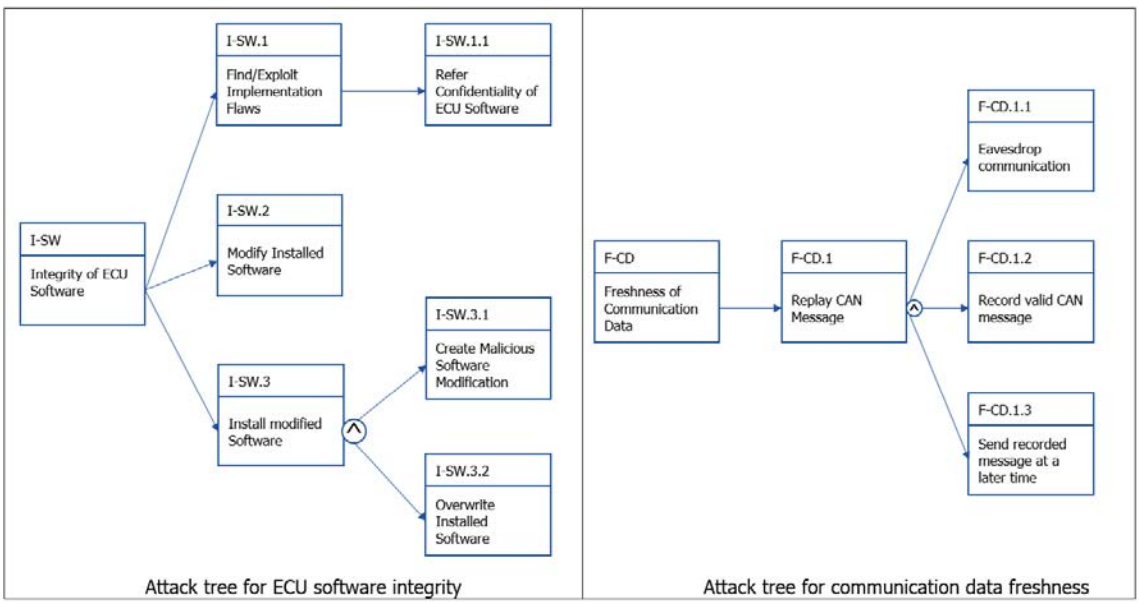
<Table 6> Risk Overview

Index	Security Goals	Risk rating
SG-1	Confidentiality of ECU Software	Undesirable
SG-2	Integrity of ECU Software	Inacceptable
SG-3	Availability of ECU Software	Inacceptable
SG-4	Authenticity of ECU Software	Inacceptable
SG-5	Confidentiality of Communication Data	Undesirable
SG-6	Integrity of Communication Data	Inacceptable
SG-7	Availability of Communication Data	Undesirable
SG-8	Authenticity of Communication Data	Inacceptable
SG-9	Freshness of Communication Data	Inacceptable
SG-10	Confidentiality of User Data	Undesirable

2) 위험 평가 (Risk Assessment)

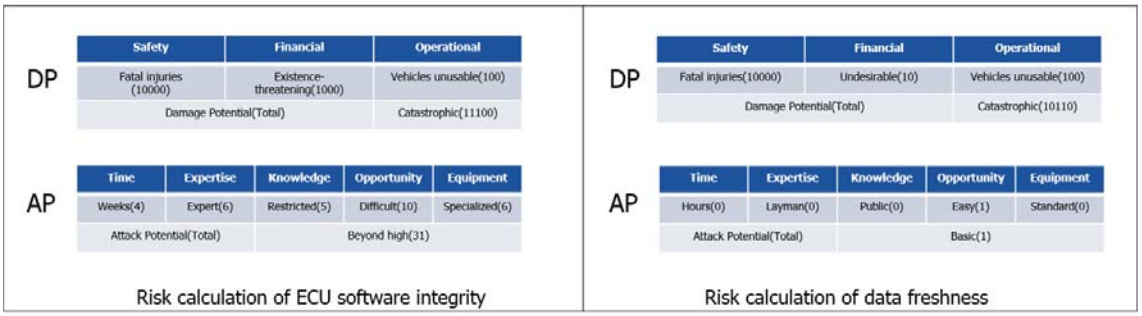
<Fig. 1>은 ECU 소프트웨어의 무결성과 통신 데이터의 최신성(Freshness)을 침해 할 수 있는 공격 트리를 보여주고 있다.

ECU 소프트웨어의 무결성을 침해하는 방법은 세 가지이다. 첫째는 ECU 소프트웨어를 분석하여 구현상 약점을 찾고, 악용하는 것이고, 둘째는 런 타임 동안 소프트웨어나 캘리브레이션 데이터를 수정하는 것이다. 세 번째는 공격자에 의해 변조된 소프트웨어가 대상 ECU에 새롭게 설치하는 것이다. I-SW.3.1과 I-SW.3.2는 I-SW.3이 수행되기 위한 And 조건이다. 통신 데이터의 최신성(Freshness)은 재전송 공격에 의해 침해될 수 있다. 재전송 공격은 공격자가 이미 차량 내부 네트워크에서 통신의 내용을 도청하고 있다가 통신 데이터를 레코딩 한 뒤 공격자가 원하는 시점에 해당 통신 데이터를 재전송하여 공격을 수행하게 된다.



<Fig. 1> Attack tree

<Fig. 2>는 <Fig. 1>에서 설명한 공격트리에 대한 AP와 DP를 계산한 것이다. <Fig. 1>의 I-SW.3에 대한 공격이 성공적으로 수행된 경우를 보면, 공격자는 자신이 만든 소프트웨어가 차량에 설치된 상태이기 때문에 차량을 공격자의 의도대로 제어 할 수 있다. 예를 들어 고속도로 운행 중에 브레이크가 동작하지 않도록 하거나 고속 주행 중 스티어링 휠을 돌려버릴 수 있는 것이다. 이 경우 생명에 치명적이며, 재산상의 문제를 야기 시킬 수 있고, 차량의 운행에 제한을 줄 수 있으므로 DP는 'Catastrophic'가 된다. 공격자가 이러한 공격을 수행하기 위해서는 차량용 소프트웨어를 제작할 수 있는 전문 지식이 있어야 하며, 소프트웨어를 설치할 기회도 많지 않다. 또한 악성 소프트웨어 제작에도 많은 시간이 걸릴 것이므로, 공격의 가능성을 나타내는 AP의 경우는 제일 높은 'Beyond High'가 된다. 이제 AP/DP값을 <Table 5>에 있는 위험 평가 매트릭스에 대입해보면 ECU 소프트웨어의 무결성이 침해되는 경우의 위험도는 '허용할 수 없는(Inacceptable)' 수준이 되는 것이다.



<Fig. 2> Risk calculation

Ⅳ. 필수 보안요구사항(Essential Security Requirement)

본 장에서는 자산 별 보안 목표를 보장하기 위해 적용되어야 하는 보안 요구사항을 도출하고, 3장에서 도출한 자산의 보안 목표 별 위험도를 기반으로 차량 탑승객의 사이버 보안을 보장하기 위해 필수적으로 적용되어야 하는 필수 보안 요구사항을 도출하였다.

1. 보안 요구사항(Security requirement)

ECU 소프트웨어, 통신 데이터, 유저 정보에 관한 14개의 보안 요구사항을 도출하였다. ECU소프트웨어에 대한 기밀성, 무결성, 가용성, 인증을 보장하기 위한 보안 요구사항은 SR-1부터 SR-6 까지 이며, 통신 데이터에 대한 기밀성, 무결성, 가용성, 인증, 최신성(freshness)을 보장하기 위한 보안 요구사항은 SR-7부터 SR-12까지이다. 유저데이터의 기밀성을 보장하기 위한 보안 요구사항은 SR-13, SR-14이다.

[SR-1] ECU소프트웨어에 대한 인가되지 않은 접근은 차단되어야 한다.

[SR-2] ECU소프트웨어에 대한 분석을 어렵게 하기 위한 기술이 적용되어야 한다.

[SR-3] ECU기동 시 ECU소프트웨어의 변조 여부를 확인 하여야 한다.

[SR-4] ECU소프트웨어는 삭제되지 않아야 한다.

[SR-5] ECU소프트웨어가 멀웨어 프로텍션 기능이 적용되어야 한다.

[SR-6] ECU소프트웨어의 업데이트는 인증/인가된 개체에 의해서만 수행되어야 한다.

[SR-7] 차량 내부 네트워크의 통신 데이터는 프로토콜의 제약이 없을 경우 암호화되어야 한다.
[SR-8] 통신 데이터는 메시지 변조를 방지해야 한다.
[SR-9] 내부 네트워크 상 비정상적인 메시지 또는 비정상트래픽을 탐지하고, 대응해야 한다.
[SR-10] 외부 인터페이스를 통해 차량 내부 네트워크로 유입되는 데이터에 대한 인증을 수행해야 한다.
[SR-11] 스마트 키를 사용하는 경우, 차량은 통신 데이터의 재전달(Relay) 여부를 판단하고, 차단해야 한다.
[SR-12] 재전송된 메시지는 탐지 및 차단되어야 한다.
[SR-13] 차량에 존재하는 모든 유저 데이터는 인가된 유저에 의해 삭제될 수 있어야 한다.
[SR-14] 유저 데이터는 암호화하여 저장되어야 한다.

2. 필수 보안 요구사항 도출

전체 16개의 보안 요구 사항 중 차량 내부보안 네트워크를 위해 필수적으로 적용해야 하는 보안요구사항은 10개가 도출되었다. 통신 데이터의 암호화는 프로토콜의 특성 상 적용의 어려움도 있겠지만, 무엇보다도 통신 데이터의 무결성과 통신 주체에 대한 인증을 필수로 적용한다면, 통신 데이터의 기밀성이 손상되더라도 차량 전체적으로는 안전을 보장 할 수 있을 것이다. 또한 개인정보의 무결성의 경우에는 변화하는 개인정보보호법과 EU의 GDPR(General Data Protection Regulation)의 변화에 따라 필수적으로 적용해야 할 요구사항이 될 수도 있다.

<Table 7>은 자산 별 보안목적, 공격 사례, 위험도, 필수 보안 요구사항을 매핑 하여 보여주고 있다. 필수 보안 요구사항은 <Table 6>의 위험 분석 결과를 기반으로 판단하게 된다. 위험 분석 결과가 허용할 수 없는 수준(Inacceptable)일 경우 해당 보안 요구사항은 필수 보안 요구 사항이 된다.

<Table 7> Essential Security Requirement

Assets	Security Objectives	Vulnerabilities and cyber attacks	Risk rating	Security Requirement	Essential Security Requirement
ECU Software	Confidentiality	AT.03, AT.06	Undesirable	SR-1, SR-2	-
	Integrity	AT.03, AT.06	Inacceptable	SR-3	O
	Availability	AT.02	Inacceptable	SR-4, SR-5	O
	Authenticity	AT.03, AT.04, AT.06, VUL.02, VUL.05	Inacceptable	SR-6	O
Communication Data	Confidentiality	AT.01, VUL.03	Undesirable	SR-7	-
	Integrity	AT.01, AT.03, VUL.01	Inacceptable	SR-8	O
	Availability	AT.02	Undesirable	SR-9	-
	Authenticity	AT.01, AT.02, AT.05, VUL.01	Inacceptable	SR-10, SR-11	O
	Freshness	AT.01, VUL.01	Inacceptable	SR-12	O
User Data	Confidentiality	VUL.03	Undesirable	SR-13, SR-14	-

Ⅴ. 관련 연구

Alexander. K et al.은 안전한 V2X 통신을 위한 연구에서 통신 상대방의 신뢰 수준에 따라 V2X통신 데이터가 영향 범위를 제한하는 방법론을 제시하였고, 사이버 공격으로 인해 받을 수 있는 안전, 금전, 개인정보

와 같은 잠재적 피해를 기반으로 신뢰보장 수준(trust assurance levels)을 제시하였다. (Alexander et al., 2013)

Marko. w와 Michael. S는 차량IT시스템을 위한 정량화된 보안 위험 분석에 대한 접근법에 대해 연구를 진행했으며, 차량 제조사가 보안 위험을 정량화 할 수 있도록 위험 분석 방법론을 제시하고 있다. 이 위험 분석 방법론은 공통 평가기준(CC, Common Criteria)과 철도 안전 엔지니어링 방법론을 기반으로 하고 있다. (Marko and Michael, 2012)

ISO에서는 자율주행차량 사이버 보안 연구가 진행 중에 있으며, 사이버 보안을 위해 조직 차원에서 수행해야 하는 항목과 디자인 단계부터 생산 후 단계에 이르기 까지 차량의 사이버 보안을 위해 필요한 항목과 절차를 포함한다. 특히 사이버 보안 수준을 객관적으로 평가 할 수 있는 사이버 보안 보증 수준(CAL, Cybersecurity Assurance Levels)을 제시하고 있다. (ISO, 2019)

Ⅵ. 결 론

오늘날의 차량은 탑승객의 편의를 위해 무선 업데이트, V2X와 같은 새로운 연결형 서비스를 탑재하고 있다. 하지만 차량의 기능이 늘어남에 따라 더 많은 취약점을 내포할 수 있으며, 공격에 사용될 수 있는 외부 인터페이스가 늘어난 것이기도 하다. 차량의 사이버 보안은 사람의 생명과 밀접한 연관이 있는 만큼 매우 중요한 사항이지만, 아직까지 차량 사이버 보안에 관해서 공표된 표준이나 법이 없는 것이 현실이다.

본 논문에서는 현재까지 차량에 발생한 공격 사례와 취약점을 바탕으로 차량에 필요한 보안 요구사항과 탑승객의 안전을 보장하기 위해 필수적으로 적용되어야 하는 필수 보안 요구사항 제시하였다. 사이버 보안으로 인해 발생 할 수 있는 안전(safety)문제를 최소화하기 위해 필수 보안 요구사항 만큼은 차량에 적용되기를 기대한다. 다만 본 연구는 차량을 대상으로 하는 실제 공격 사례와 취약점을 통해 식별된 자산을 기반으로 진행된 것이기에, 아직 식별되지 않은 자산일 경우에는 추가적인 연구를 필요로 한다.

보안의 관점에서는 보안 요구사항의 적용뿐 만 아니라 해당 보안 요구사항이 차량에 올바르게 적용 되었는지에 대한 객관적인 검증방법이 요구된다. 하지만 현재까지는 해당 보안요구사항이 적용된 차량이 존재하지 않으며, 차량 제조사로부터 공개된 자료가 제한적인 상황이므로 이에 대해서는 향후 연구로 남겨둔다.

ACKNOWLEDGEMENTS

본 연구는 국토교통부 및 국토교통과학기술진흥원의 연구비지원(18TLRP-B117133-03)으로 수행된 연구임.

본 논문은 초기 아이디어는 2018년 6월 한국자동차공학회 춘계학술대회에서 발표하였으며, 송윤근(2019)의 석사학위 논문을 수정・보완하여 작성하였습니다.

REFERENCES

Alexander K., Daniel A., Herve S., Tyrone S. and Marko W.(2013), “Trust assurance levels of cybercars in v2x communication,” *2013 ACM workshop on Security, privacy & dependability for cyber vehicles*, pp.49-60.

Charlie M. and Chris V.(2015), *Remote exploitation of an unaltered passenger vehicle*, Black Hat USA 2015.

Common Vulnerabilities and Exposures, "CVE-2017-6054," https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-6054, accedded 2019.03.29.

Common Vulnerabilities and Exposures, "CVE-2018-1170," https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-1170, accessed 2019.03.29, 2019e

Common Vulnerabilities and Exposures, "CVE-2018-16806," https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-16806, accessed 2019.03.29, 2019d

Common Vulnerabilities and Exposures, "CVE-2018-18071," https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-18071, accessed 2019.03.29, 2019c

Common Vulnerabilities and Exposures, "CVE-2018-18203," https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-18203, accessed 2019.03.29, 2019b

Common Vulnerabilities and Exposures, "CVE-2018-9322," https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-9322, accessed 2019.03.29, 2019a

Condé Nast, https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/, 2019. 03. 29.

for Information Technology Security Evaluation – Evaluation methodology, https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf.

Hiro O.(2012), "Paradigm change of vehicle cyber security," *2012 4th International Conference on Cyber Conflict(CYCON 2012)*, pp.1-11.

ISO, *ISO/SAE CD 21434 Road Vehicles – Cybersecurity engineering*, https://www.iso.org/standard/70918.html", accessed 2019.04.26.

ISO/IEC 15408(2017), *Common Methodology*

Karl K., Alexei C., Franziska R., Shwetak P., Tadayos K., Stephen C., Damon M., Brian K., Danny A., Hovav S and Stefan S, (2010), "Experimental Security Analysis of a Modern Automobile," *2010 IEEE Symposium on Security and Privacy*, pp.447-462.

Marko W. and Michael S.(2009), *A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems*, Automotive-Safety Security 2012, pp.195-210.

Marko W.(2018), "Strategies against being taken hostage by ransomware," *ATZelektronik worldwide*, vol. 13, no. 2, pp.44-47.

Pen Test Partners LLP, https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv, 2019. 03. 29.

PricewaterhouseCoopers(PwC) GmbH(2017), *The 2017 Strategy & Digital Auto Report*, https://www.strategyand.pwc.com/media/file/2017-Strategyand-Digital-Auto-Report.pdf.

PricewaterhouseCoopers(PwC) GmbH(2018), *Five trends transforming the Automotive Industry*, https://www.pwc.at/de/publikationen/branchen-und-wirtschaftsstudien/eascy-five-trends-transforming-the-automotive-industry_2018.pdf.

SAE International(2018), *J3016™ Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, https://saemobilus.sae.org/content/J3016_201806.

Sen N., Ling L. and Yuefeng D.(2017), Free-Fall: Hacking Tesla From Wireless to Can Bus, Black Hat USA 2017.

Tencent Keen Security Lab,
https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/, 2019.03.31.

US DoT(2017), *An Introduction to Connected Automated Vehicles*,
https://www.its.dot.gov/presentations/2017/CAV2017_AdvTechTransport.pdf.

Yousik L., Samuel W., Jungho L., Yunkeun S., Heeseok M. and Donghoon L.(2019), "Enhanced Android App-Repackaging Attack on In-Vehicle Network," *Wireless Communications and Mobile Computing*, vol. 2019, no. 5650245, p.13.