Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.6, Dec. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.6.1151

안전한 자동차용 SUMS 구축을 위한 보안성 평가기준 도출*

서 재 완,[1†] 곽 지 원,[1] 홍 바 울,[1] 조 광 수,[1] 김 승 주[2‡]
[1,2]고려대학교 정보보호대학원 (대학원생, 교수)

A Study on Security Evaluation for Secure Software Update Management System in Automotive*

Jaewan Seo,[1†] Jiwon Kwak,[1] Paul Hong,[1] Kwangsoo Cho,[1] Seungjoo Kim[2‡]
[1,2]ICSP(Institute of Cyber Security & Privacy), School of Cybersecurity,
Korea University (Graduate student, Professor)

요 약

차량에 무선 통신 기능이 탑재되기 시작하면서 무선 통신 기능의 취약점을 악용한 차량의 사이버 공격이 증가하고 있다. 이에 대응하기 위해 UNECE는 차량 제조사가 무선 통신 기능을 활용하여 차량에 탑재되는 소프트웨어를 안전하게 배포할 수 있도록 UN R156 규정을 제정하였다. 해당 규정은 차량의 소프트웨어를 안전하게 배포하는데 필요한 보안 요구사항을 명시하고 있으나 해당 요구사항을 개발 및 구현하는데 필요한 구성요소와 세부 기능에 대한 정보가 생략된 채 추상적인 요구사항만이 제시되어 있다. 따라서 본 논문에서는 체계적으로 보안 위협을 분석하는 방법인 위협모델링을 활용하여 안전한 SUMS를 구축하는데 필요한 상세 보안 요구사항을 도출한다. 이후 해당 요구사항을 바탕으로 SUMS에 대한 보안성 평가기준을 제안한다.

ABSTRACT

As wireless communication functions begin to be installed in vehicles, cyberattacks that exploit vulnerabilities in wireless communication functions are increasing. To respond to this, UNECE enacted the UN R156 regulation to safely distribute the software installed in the vehicle by using the wireless communication function. The regulations specify the requirements necessary to safely distribute the software for vehicles, but only the abstract requirements are presented without information on the components and detailed functions necessary to develop and implement the requirements. Therefore, in this paper, we propose a security evaluation standard that can evaluate whether a safe SUMS is built using threat modeling, a method for systematically analyzing security threats.

Keywords: SUMS, Software Update, Threat Modeling, Security Requirement, Security Evaluation.

I. 서 론

차량에는 탑승자들에게 편리함을 제공하기 위한 목적으로 무선 통신 기술이 적용되고 있다. 해당 기술을 바탕으로 차량은 인포테인먼트와 같은 서비스뿐만 아니라 무선 업데이트와 같은 기능을 제공한다.

Received(10. 26. 2022), Modified(11. 25. 2022), Accepted(12. 05. 2022)
* 본 연구는 국토교통부/국토교통과학기술진흥원의 지원으로 수행되었음(22AMDP-C162334-02: 자동차 통합보안 안전성 평가기술 개발)
† 주저자, bace@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

하지만 무선 통신 기술과 관련된 기능들이 추가됨에 따라 차량의 무선 통신 기능 및 차량과 통신하는 외부 시스템의 취약점을 악용한 사이버 공격 사례가 증가하고 있다. 실제로 2015년 Charlie Miller와 Chris Valasek은 차량 해킹을 통해 운전자의 생명을 위협할 수 있다는 결과를 Black Hat에서 발표하였다[1]. 2017년 Keen Security Lab 소속의 중국 연구원들은 위·변조된 Tesla 펌웨어를 통해 차량의 제어권을 탈취할 수 있다는 결과를 발표하였다[2]. 또한, 2021년 CanSecWest 컨퍼런스에서는 차량의 무선 통신 취약점을 통해 해커가 임의로 차량을 조작할 수 있다는 결과가 발표되었다[3].

이처럼 차량에 대한 사이버 공격이 가능해지면서 UNECE(United Nations Economic Commission for Europe)는 2021년 차량의 사이버보안을 확보하기 위한 규정을 발표하였으며 이러한 규정을 준수하여 자동차를 개발하는 OEM에 대해서만 유럽 국가에 자동차를 수출할 수 있도록 명시하였다. 이에 국내에서도 차량을 유럽 국가에 수출하기 위해서는 해당 규정을 준수해야 한다. 해당 규정 중 UN R156(UN Regulation No.156)[4]은 사이버 공격으로부터 안전하게 차량의 소프트웨어를 업데이트하기 위한 보안 요구사항이 포함되어 있다. 하지만 UN R156에 명시된 보안 요구사항은 SUMS 구축 시 어떤 보안기능이 필요한지에 대한 상세 정보를 제공하지 않기 때문에 OEM이 해당 규정만을 참고하여 소프트웨어 업데이트 관리 시스템(SUMS, Software Update Management System)을 구축하는 것이 제한된다.

기존에는 UN R156의 보안 요구사항을 다루는 연구들이 존재하지 않았으며, SUMS와 관련된 보안 요구사항에 관한 연구들에서도 모든 위협들을 기반으로 도출하는 것이 아닌 일부 위협들만을 대상으로 하는 단편적인 보안 요구사항을 제시하고 있다. 따라서 OEM에서 SUMS 구축 시 참고 가능한 상세 요구사항이 필요하다.

이에 본 논문에서는 체계적으로 위협을 분석하는 방법인 위협모델링[5]을 이용하여 SUMS에서 발생 가능한 위협들을 식별한다. 그리고 해당 위협들을 완화하기 위한 항목들을 기반으로 SUMS 구축 시 준수해야 하는 상세 보안 요구사항을 제시하며 해당 내용은 다음 링크[1]를 통해 확인할 수 있다. 이후 본 논문에서 제시한 보안 요구사항과 관련된 UN R156의 요구사항을 매핑한다. 따라서 OEM에서 본 논문에서 제시한 보안 요구사항을 활용하는 경우 UN R156의 요구사항 중 보안과 관련된 요구사항을 만족할 수 있을 뿐만 아니라, 상세 보안 요구사항을 기반으로 안전한 SUMS를 구축할 수 있을 것으로 기대된다.

본 논문은 총 5장으로 구성된다. 2장에서는 체계적인 문헌 수집 전략을 바탕으로 선별된 SUMS 관련 연구에 대해 설명한다. 3장에서는 SUMS에 대한 위협모델링을 수행한다. 4장에서는 위협모델링 결과 도출된 보안성 평가기준을 제시한다. 마지막으로 5장에서는 연구 결과를 요약·제시한다.

II. 관련 연구

본 장에서는 차량용 SUMS와 관련된 최근 연구 동향을 기술한다. 본 논문에서는 SUMS와 관련된 연구를 식별하고 분석하기 위해 먼저 SUMS, OTA(Over-The-Air) 업데이트 등의 키워드를 기반으로 관련된 문헌들을 모두 수집하였다. 이후 해당 문헌들에 대한 요약, 서론, 결론, 본론 분석을 통해 관련 연구를 식별하는 3단계의 프로세스를 기반으로 연구 동향을 조사하였다.

2.1 문헌 수집 전략

관련 연구 조사 프로세스는 3단계로 진행되며 각 단계별 수행 내용은 아래와 같다.

1) 키워드 기반의 문헌 수집 및 문헌 제목을 통한 분류: IEEE, ACM, Springer 등의 학술 데이터베이스에서 SUMS, OTA Update, Security Requirement의 키워드를 조합하여 최근 5년간 출판된 문헌들을 수집하였다. 이후 중복된 문헌 및 연구 방향과 관련성이 적은 문헌을 제거하였다.

2) 문헌 요약, 서론, 결론 분석을 통한 분류: 1단계에서 식별된 문헌의 요약과 서론, 결론 내용을 기반으로 본 논문의 연구 방향과 관련성이 적은 문헌을 제거하였다.

3) 문헌 본론 분석을 통한 분류: 2단계에서 식별된 문헌들의 본론을 분석하여 본 논문의 연구 방향과 관련된 문헌들을 관련 연구로 식별하였다.

1) https://1drv.ms/x/s!Au-PtGLSDXMcgdtORQFvm24k2yjTSQ?e=sw2PQH

2.1의 전략을 활용하여 관련 연구 문헌을 수집 및 분류한 결과 1단계에서 109건의 문헌이 선정되었다. 이후 2단계에서는 28건, 최종적으로 3단계에서는 총 9건의 관련 연구가 식별되었다.

2.2 연구 동향

본 절에서는 2.1절을 통해 식별된 9건의 연구에 관해 기술한다. 해당 연구들은 모두 SUMS와 관련된 보안 요구사항을 나타내고 있으며, 보안 요구사항의 적용 범위에 따라 Fig. 1.과 같이 ▲OTA 업데이트 시스템 관련 보안 요구사항, ▲차량 구성요소 관련 보안 요구사항으로 분류된다.

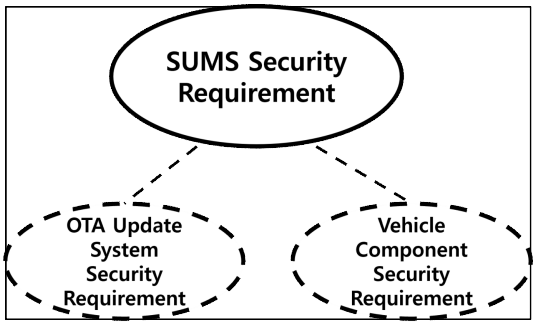

Fig. 1. Categorization of Related Work

2.2.1 OTA 업데이트 시스템 관련 보안 요구사항

2018년 Lee 등은 OTA 업데이트 시스템과 관련된 위협들을 나열하고 해당 위협들을 완화하기 위해 무단 트래픽 방지, 인증 및 권한 부여 메커니즘, 데이터 변조 방지, 보안 통신 채널 등을 사용할 수 있다고 제시한다[6].

2020년 T. Placho 등은 차량 소프트웨어 업데이트 시 무결성, 가용성 등과 관련된 요구사항을 제시하며, 해당 요구사항들을 충족해야 한다고 명시한다[7]. 이후 해당 요구사항들을 적용할 수 있는 Mender, Hawkbit, Uptane에 대해 설명한다.

2021년 A. Mukherjee 등은 OTA 업데이트 시스템에 대한 아키텍처를 제안하였다. 이후 해당 아키텍처에서 발생할 수 있는 관련 위협들을 나열하고 해당 위협들을 완화하기 위해 TrustZone, TEE, 보안 통신 채널을 사용할 수 있다고 제시한다[8]. C. Ponsard 등은 업데이트 시스템에서 발생할 수 있는 위협들을 나열하고 해당 위협들을 완화하기 위해 디지털 서명, 최신 버전의 업데이트 파일 설치, 보안 통신 채널 등을 사용할 수 있다고 제시한다[9]. Zhi Wu 등은 OTA 시스템을 통해 송/수신되는 업데이트 파일에 대한 무결성 관련 위협들을 나열하고 해당 위협들을 완화하기 위해 디지털 서명, 메시지 인증 코드, 보안 통신 채널 등을 사용할 수 있다고 제시한다[10].

2022년 R. Kirk 등은 OTA 업데이트 시스템을 공식으로 나타내고 도청, 스푸핑 등의 공격을 모델링하여 테스트한다[11]. 이후 해당 공격들 중 일부가 수행 가능하다는 결과를 도출하고 해당 공격들을 완화하기 위해 정기적인 업데이트, 암호화, 무결성 검사 등을 사용할 수 있다고 제시한다. A. Ghosal 등은 클라우드 서버를 통해 차량 소프트웨어 업데이트 시 발생 가능한 위협들을 나열하고 해당 위협들을 완화하기 위해 개체 인증, 타임스탬프, 접근통제, 변조된 데이터 감지 기능 등을 사용할 수 있다고 제시한다[12].

2.2.2 차량 구성요소 관련 보안 요구사항

2020년 Jinghua Yu 등은 차량 내 통신 시스템에서 발생할 수 있는 무결성 관련 위협들을 나열하고 해당 위협들을 완화하기 위해 무결성 검사 알고리즘, 변조된 데이터 감지 기능 등을 사용할 수 있다고 제시한다[13]. M. Hamad 등은 차량 내 하드웨어 및 소프트웨어 등에서 발생 가능한 위협들을 나열하고 해당 위협들을 완화하기 위해 인증, 권한 부여, 기밀성, 무결성, 가용성 등의 보안 속성을 고려할 수 있다고 제시한다[14].

2.3 연구 동향 요약

앞에서 기술하였듯이 기존 9개의 문헌에서는 OTA 업데이트 시스템 및 차량 구성요소와 관련된 보안 요구사항을 제시하고 있다. 하지만 기존 보안 요구사항과 관련된 연구들은 UN R156의 보안 요구사항을 다루고 있지 않으며, SUMS를 구성하는 요소들 중 일부 구성요소에 대한 요구사항만을 제시하고 있다. 또한 해당 요구사항들은 기밀성, 무결성 등의 보안 속성을 준수해야 한다는 추상적인 요구사항과 인증, 디지털 서명, 보안 통신 채널 등에 대한 요구사항에만 치중되어 있다. 즉, SUMS 구축을 위해 필요한 상세 보안 요구사항 관련 연구가 부족하

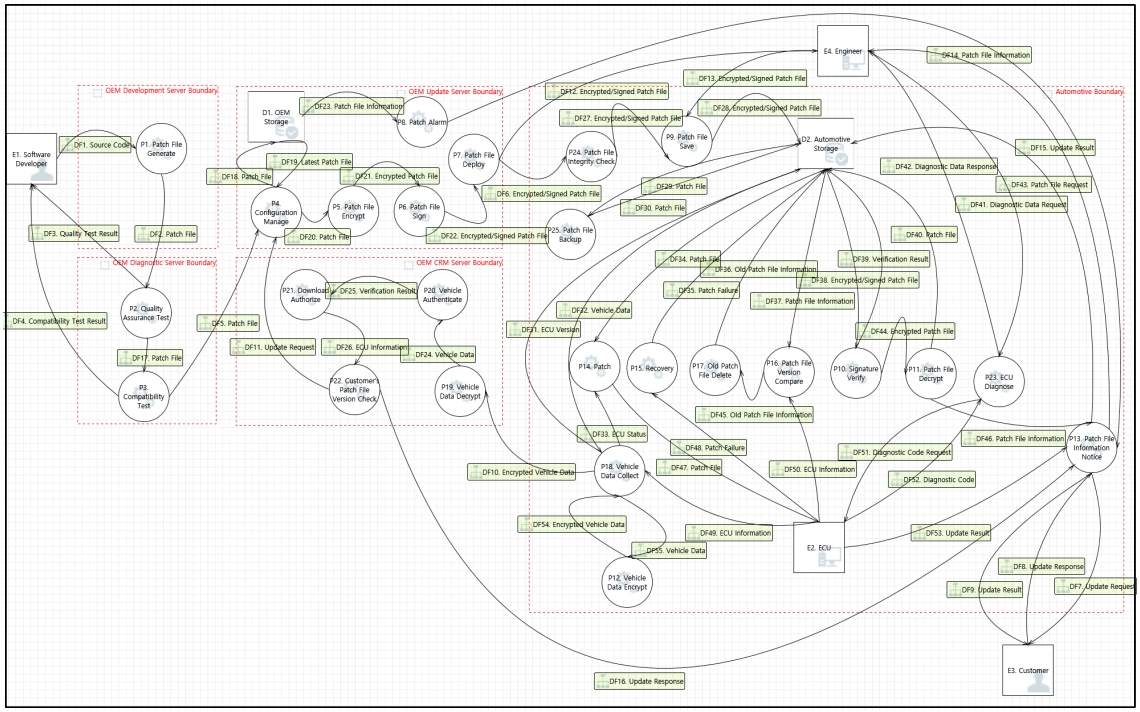

Fig. 2. DFD for SUMS

다. 따라서 본 논문에서는 UN R156의 보안 요구사항과 매핑될 뿐만 아니라, SUMS 구축 시 필요한 상세 보안 요구사항을 도출하는 연구를 수행하였다.

III. 보안성 평가기준 도출

본 장에서는 차량용 SUMS에 대한 보안성 평가기준을 도출하기 위해 수행한 위협모델링 과정에 대해 기술한다. 위협모델링을 수행하기 위해서는 먼저 분석 대상인 차량용 SUMS의 수행 기능 및 관련 데이터가 먼저 파악되어야 한다. 하지만 상기 정보가 포함된 차량용 SUMS에 대한 설계 또는 구현 결과물은 대부분 외부에 공개되지 않기 때문에 분석이 제한되었다. 이에 따라 본 논문에서는 차량 관련 조직의 문서와 프로젝트 결과물을 분석하여 SUMS 아키텍처의 구성요소와 기능을 식별한 후 해당 결과를 기반으로 위협모델링을 수행하였다.

본 논문에서 차량용 SUMS에 대한 위협모델링을 수행하기 위해 활용한 방법은 차량에 대한 위협과 위험 수준을 분석하기 위한 방법론 중 하나인 HEAVENS Security Model이다. 해당 방법은 Microsoft의 STRIDE를 기반으로 차량 내 위협을 식별하고 각 위협에 대한 TL(Threat Level), IL(Impact Level)을 산정하여 위험도를 평가한다. 이러한 HEAVENS Security Model은 차량에 대한 위협 식별 시 차량 내부에 대해서만 고려하는 것이 아닌 OEM, 차량, 운전자 등의 주변 요소들도 함께 고려한다[15]. 또한 BMW, DAIMLER, HONDA, HYUNDAI 등 전 세계의 다양한 차량 제조업체/공급업체로 구성된 GENIVI Alliance에서도 차량에 대한 공격 경로식별 및 위험도 평가를 수행하는 데 STRIDE를 활용하고 있다[16]. 따라서 본 논문에서는 해당 방법을 활용하여 차량용 SUMS를 분석하였으며, 세부 절차는 ▲DFD(Data Flow Diagram) 작성부터 ▲공격 라이브러리 수집, ▲위협 분석(STRIDE 적용), ▲공격 트리(공격 시나리오) 작성, ▲완화방안 도출, ▲보안성 평가기준 도출까지 총 6단계로 진행된다.

3.1 DFD 작성

DFD는 분석 대상 시스템을 데이터 흐름의 관점에서 추상화하여 표현한 것으로 시스템 구조 및 공격 지점을 식별할 수 있다. 이러한 DFD를 작성하는 경

우 해당 DFD가 실제 시스템에도 동일하게 적용되어야 한다는 성질인 건전성이 중요하다. 따라서 DFD는 분석 대상과 추상화한 모델 사이에 차이가 발생하지 않도록 가급적 함수 수준까지 표현되어야 한다. 이를 위해 DFD는 분석 대상 시스템을 추상화하여 나타내는 단계인 Context Level, 분석 대상 프로세스를 서브시스템 단위로 분해하여 표현하는 Level 0, 분석 대상 내 서브시스템을 모듈 단위로 분해하여 표현하는 Level 1, 모듈을 내부 기능 또는 함수 단위까지 상세히 분해하여 표현하는 Level 2 순서대로 상세화되어 작성된다[17-19]. 하지만 Level 2 DFD는 소스코드와 같은 자료를 기반으로 함수 수준까지 매우 상세하게 표현되기 때문에 하나의 제품에 특정된 DFD가 작성될 수 있다. 따라서 본 논문에서는 차량 관련 조직의 문서와 프로젝트 결과물을 기반으로 필수 모듈을 식별하여 Level 1 수준의 DFD를 작성하였다. 이러한 DFD는 ▲Entity, ▲Process, ▲Data Store, ▲Data Flow, ▲Trust Boundary의 5가지 구성요소를 통해 데이터의 흐름을 보여준다. 본 논문에서 도식화한 SUMS 아키텍처에 대한 DFD는 Fig. 2.와 같다.

3.2 공격 라이브러리 수집

DFD가 작성된 이후에는 분석 대상 시스템과 관련하여 현재까지 알려진 취약점을 모두 수집해야 하며, 이처럼 알려진 취약점이 모두 수집된 것을 공격 라이브러리라고 한다. 공격 라이브러리는 분석 대상 시스템과 밀접한 취약점 및 공격 기법이 수집될수록 발생 가능한 위협을 구체적으로 식별할 수 있도록 도와준다. 이러한 공격 라이브러리는 CVE(Common Vulnerabilities and Exposures), CWE(Common Weakness Enumeration), 논문 및 기술 문서 등을 바탕으로 수집된다. 공격 라이브러리 수집 시 사용되는 키워드는 분석 대상 시스템의 이름부터 DFD 내 존재하는 각 구성요소의 이름까지 최대한 다양하게 조합하여 수집한다. 본 논문에서는 SUMS와 관련된 CVE 35건, CWE 6건, 논문 27건, 표준 1건, 기술 보고서 1건으로 총 70건의 공격 라이브러리를 수집하였으며, 해당 내용은 Table 1.과 같다.

Table 1. Attack Library for SUMS

No.	Threat Type	Name	Ref
AL-V-1	Denial of Service	CVE-2010-2959	[20]
AL-V-2	Denial of Service	CVE-2010-3874	
…			[21]~[46]
AL-S-1	Spoofing	ITU-T X.1373	[47]
	Tampering		
	Denial of service		
	Information disclosure		
AL-TR-1	Spoofing	Automotive Industry Guidelines for Secure Over-the-Air Updates	[48]
	Information disclosure		
	Denial of service		
	Elevation of privilege		

3.3 위협 분석

위협 분석은 DFD의 각 구성요소에 존재할 수 있는 잠재적 위협을 모두 식별하는 과정이다. 본 논문에서 사용하는 STRIDE 기법은 보안 위협을 ▲위장(Spoofing), ▲변조(Tampering), ▲부인(Repudiation), ▲정보 유출(Information disclosure), ▲서비스 거부(Denial of service), ▲권한 상승(Elevation of privilege)의 6가지 범

Table 2. STRIDE for SUMS

Type	ID	Name	Threat	Attack library	No.
Entity	E1	Software Developer	S	AL-V-19	T1
			S	AL-W-5	T2
			S	AL-P-1	T3
			S	AL-TR-1	T4
…					
Data Flow	DF55	Vehicle Data	I	AL-P-17 AL-P-24 AL-P-27 AL-W-3 AL-S-1	T1002
			I	AL-V-33 AL-P-21	T1003
			I	AL-P-4	T1004
			I	AL-P-13	T1005
			I	AL-P-18	T1006
			D	AL-P-19	T1007

주로 나누어 식별한다. DFD 작성 시 식별된 구성요소 별로 발생할 수 있는 모든 위협은 이러한 6가지 범주에 기반하여 도출되어야 한다. 다음 Table 2.는 DFD의 구성요소 별로 도출될 수 있는 위협들을 나타낸다.

3.4 공격 트리 작성

공격 트리는 분석 대상 시스템에서 발생할 수 있는 잠재적 위협을 이용하여 공격 시나리오를 도출하는 기법이다[49]. 최상위 노드는 공격자의 최종 공격 목표를 나타내며, 최하위 노드는 각 공격 시나리오를 수행하기 위한 진입점으로 공격자가 해당 시나리오를 활용하여 공격을 수행하는 데 필요한 시스템 내 잠재적 위협을 나타낸다. 공격 트리에서 하위 노드는 AND, OR 조건을 통해 상위 노드의 공격 목표를 달성할 수 있다. AND 조건의 경우 상위 노드 공격 목표를 달성하기 위해 AND 조건으로 묶인 하위 노드들이 모두 달성되어야 함을 뜻하며, OR 조건의 경우 AND와 반대로 한 가지의 하위 노드만 달성되어도 상위 노드로 도달할 수 있음을 의미한다. 이러한 공격 트리는 수집된 보안 위협들이 실제 공격에서 어떻게 활용될 수 있는지를 시각적으로 파악하기 위해서 사용된다. 본 논문에서 작성한 공격 트리는 다음 Table 3. ~ Table 6.과 같다.

Table 3. Obstruction of automotive operation

Purpose of attack					Threat
1	Obstruction of automotive operation				-
OR	1.1	Obstruction of CAN network operation			-
	OR	1.1.1	Arbitrary code execution		-
		OR	1.1.1.1	Integer overflow	T167, T197, T225, T259, T297, T325, T353, T381, T409, T491, T555
...					
OR	1.2	Obstruction of wireless network operation			-
	OR	1.2.1	Arbitrary code execution		-
		OR	1.2.1.1	Stack overflow	T558
...					

Table 4. Automotive control

Purpose of attack					Threat
2	Automotive control				-
OR	2.1	CAN network data tampering			-
	AND	2.1	Fix malicious code		-
		OR	2.1.1.1	OBD port access	T249, T476, T500, T543, T905, T918
...					
OR	2.2	Wireless network data tampering			-
	OR	2.2.1	Replay attack		T162, T192, T221, T253, T293, T321, T349, T377, T405, T482, T541, T549
...					

Table 5. Obstruction of server operation

Purpose of attack					Threat
3	Obstruction of server operation				-
OR	3.1	Obstruction of system operation			-
	OR	3.1.1	System access		-
		OR	3.1.1.1	Inappropriate access control	T47, T69, T77, T100, T109, T117, T126, T133, T153, T170, T182, T200, T212, T228, T240, T264, T283, T300, T312, T328, T340, T356, T368, T384, T396, T412, T424, T445, T453, T460, T466, T501, T531, T565, T585, T608
...					
OR	3.2	Obstruction of wireless network operation			-
	OR	3.2.1	Arbitrary code execution		-
		OR	3.2.1.1	Stack overflow	T558
...					

Table 6. Server control

Purpose of attack					Threat
4	Server control				-
OR	4.1	Root shell access			-
	OR	4.1.1	Kernel access		-
		OR	4.1.1.1	Inappropriate access control	T170, T186, T200, T214, T228, T242, T264, T287, T300, T314, T328, T343, T356, T371, T384, T399, T412, T426, T501, T529, T534, T589
...					
OR	4.2	Arbitrary code execution			-
	OR	4.2.1	Use weak functions		-
		OR	4.2.1.1	Stack overflow	T86, T106, T114, T122, T558
...					

3.5 완화방안 도출

완화방안은 공격 트리를 기반으로 실제 시스템에서 발생할 수 있는 공격 시나리오를 완화하기 위해 점검해야 하는 항목이다. 완화방안 도출 시 주의해야 할 점은 공격 트리에서 식별된 공격 시나리오를 우선적으로 고려하되, 위협 분석(STRIDE) 단계에서 도출되었지만, 공격 트리에 연관되지 않은 위협 또한 추후 공격에 활용될 수 있기에 함께 고려해야 한다는 것이다. 이러한 완화방안은 ①공격 트리 내 각 공격 시나리오의 최하위 노드와 연관된 취약점과 ②공격 트리 하위노드로 지정되지 않은 잠재적 위협에 연관된 취약점들을 완화시킬 수 있는 항목들로 구성된다. 3.4절에서 위협모델링을 통해 식별한 위협을 기반으로 작성한 공격 트리에는 Table 7.의 Attack/Threat 열에 작성한 바와 같이 49개의 최하위 노드가 존재하며, 부적절한 접근통제와 연관된 취약점이 가장 많은 비중을 차지하고 있었다. 실제 시스템에서는 이러한 최하위 노드를 기반으로 발생할 수 있는 공격 시나리오를 완화해야 하며, 이를 위해 점검해야 하는 항목이 필요하다. 따라서 Checklist 열에 공격 시나리오를 완화하기 위해

Table 7. Checklist for SUMS

Checklist	Counter measure	Attack/ Threat	Attack tree
(C1) Check for Inappropriate Access Controls	Access control	Improper access control	AT1, AT2, AT3, AT4
...			
(C15) Check input length in string buffer	Secure Coding	Heap overflow	AT1, AT3, AT4
		OOB vulnerability	AT1, AT2, AT4
		Stack overflow	AT1, AT3, AT4
		Buffer overflow	AT1, AT2, AT3, AT4
		Execution of programs in unauthorized areas	AT2, AT4
(C16) Check input range of integer values		Integer overflow	AT1, AT2, AT4
(C17) Check whether special characters are filtered		Command injection	AT2
...			
(C20) Check the encryption algorithm used by the system	Use strong encryption algorithms	Weak Encryption	AT2
		Decryption	AT2
		Reversing	AT2
(C21) Check whether data is encrypted	Using encryption algorithm	Data lookup	AT2
...			
(C25) Check whether address verification is normal	Validation check	Bypass validation	AT4

점검해야 하는 항목들을 기술하였다. 본 논문에서는 총 25개의 점검항목을 도출하였으며, 해당 내용은 아래 Table 7.과 같다.

IV. 도출된 보안성 평가기준

본 장에서는 4,1절을 통해 완화방안에 따라 도출한 보안성 평가기준을 나타내며, 4.2절을 통해 UN R156과 보안성 평가기준이 어떻게 연관되는지 기술한다.

4.1 보안성 평가기준

본 장에서는 차량 SUMS에 대한 보안성 평가기준을 기술한다. 본 논문에서는 차량 SUMS에 대한 보안성 평가기준을 도출하기 위해 체계적으로 위협을 분석하는 방법인 위협모델링을 통해 총 1007개의 위협을 식별하였다. 이후 해당 위협들을 기반으로 실제 시스템에서 공격자의 목적을 달성하기 위한 세부 공격들을 모두 식별하여 공격 트리를 작성하였다. 공격 트리는 49개의 최하위 노드로 구성되어 있으며, 해당 최하위 노드들과 연관된 취약점들을 완화할 수 있는 항목들을 상세화하여 보안성 평가기준을 도출하였다.

Table 8. Security requirement for SUMS

No.	Security requirement	Checklist
SR1	SUMS security function shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and key lengths.	C20, C21
SR2	SUMS security function shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that remove all traces of a cryptographic key so that it cannot be recovered by either physical or electronic.	C20, C21
...		
SR 46	SUMS security function shall enforce the following rules when importing user data controlled under the security functional policy from outside the SUMS. special character filtering restrict string length	C15, C16, C17

따라서 본 논문에서 도출한 보안성 평가기준은 실제로 발생 가능하거나 잠재적으로 발생할 수 있는 위협을 모두 완화할 수 있다. 해당 보안성 평가기준은 아래 Table 8.과 같으며 총 46개로 구성되어 있다.

4.2 UN R156과 보안성 평가기준 비교

본 절에서는 UN R156의 보안 요구사항과 본 논문에서 제안하는 보안성 평가기준 간 관계를 나타낸다. 앞서 1장에서 설명하였듯이 기존의 UN R156의 보안 요구사항은 추상적인 정보만을 명시하고 있다. 따라서 Table 9.를 통해 본 논문에서 제안하는 상세 보안성 평가기준이 UN R156의 어떠한 보안 요구사항과 연관되는지 기술한다.

Table 9. Security requirement of UN R156

No.	UN R156	Security requirement
7.1.3.1	The process they will use to ensure that software updates will be protected to reasonably prevent manipulation before the update process is initiated.	SR1, SR2, SR3, SR4, SR5, SR6, SR7, SR8, SR9, SR10, SR11, SR12, SR13, SR14, SR15, SR16, SR17, SR18, SR19, SR20, SR21, SR22, SR23, SR24, SR25, SR26, SR27, SR28, SR29, SR30, SR31, SR32, SR33, SR34, SR36, SR37, SR38, SR39, SR40, SR41, SR42, SR43, SR44, SR45, SR46
7.1.3.2	The update processes used are protected to reasonably prevent them being compromised, including development of the update delivery system.	SR1, SR2, SR3, SR4, SR5, SR6, SR7, SR8, SR9, SR10, SR11, SR12, SR13, SR14, SR15, SR16, SR17, SR18, SR19, SR20, SR21, SR22, SR23, SR24, SR25, SR26, SR27, SR28, SR29, SR30, SR31, SR32, SR33, SR34, SR36, SR37, SR38, SR39, SR40, SR41, SR42, SR43, SR44, SR45, SR46

7.1.3.3	The processes used to verify and validate software functionality and code for the software used in the vehicle are appropriate.	SR9, SR10, SR12, SR13, SR14, SR15, SR16, SR17, SR18, SR19
7.2.1.1	The authenticity and integrity of software updates shall be protected to reasonably prevent their compromise and reasonably prevent invalid updates.	SR9, SR10, SR12, SR13, SR14, SR15, SR18, SR19
7.2.1.2.3	The vehicle manufacturer shall protect the RXSWINs and/or software version(s) on a vehicle against unauthorised modification. At the time of Type Approval, the means implemented to protect against unauthorized modification of the RXSWIN and/or software version(s) chosen by the vehicle manufacturer shall be confidentially provided.	SR1, SR2, SR3, SR4, SR5, SR6, SR7, SR8, SR9, SR10, SR11, SR12, SR13, SR14, SR15, SR16, SR17, SR18, SR19, SR20, SR21, SR22, SR23, SR24, SR25, SR26, SR27, SR28, SR29, SR30, SR31, SR32, SR33, SR34, SR36, SR37, SR38, SR39, SR40, SR41, SR42, SR43, SR44, SR45, SR46
7.2.2.5	The vehicle shall ensure that preconditions have to be met before the software update is executed.	SR1, SR2, SR3, SR4, SR5, SR6, SR7, SR8, SR9, SR10, SR11, SR12, SR13, SR14, SR15, SR16, SR17, SR18, SR19, SR20, SR21, SR22, SR23, SR24, SR25, SR26, SR27, SR28, SR29, SR30, SR31, SR32, SR33, SR34, SR35, SR36, SR37, SR38, SR39, SR40, SR41, SR42, SR43, SR44, SR45, SR46

V. 결 론

현재 차량은 OEM 서버를 비롯한 다양한 장치와 연결되며 SUMS에 의해 시스템이 업데이트된다. 하지만 이러한 서비스를 제공하기 위해 추가되는 소프트웨어 및 하드웨어가 새로운 공격 경로가 될 수 있기 때문에 차량을 취약하게 만든다. 따라서 차량용 SUMS에 대한 보안 수준을 평가하는 지표가 되는 보안성 평가기준이 필요한 실정이다. 하지만 기존 UN R156에 명시된 보안 요구사항은 SUMS 구축 시 어떤 보안기능이 필요한지에 대한 상세 정보 정보를 제공하지 않기 때문에, OEM에서 해당 항목들을 기반으로 SUMS에 대한 보안 수준을 평가하기에는 어려움이 존재한다. 이러한 문제점으로 인해 기존에도 SUMS와 관련된 보안 요구사항에 관한 연구들이 진행되고 있었다. 하지만 기존 연구들은 UN R156과 보안 요구사항 간의 연관성이 보이지 않기에 기존 보안 요구사항을 통해 UN R156의 보안 요구사항을 어떻게 만족시키는지 알기 어려울 뿐만 아니라, SUMS 내 일부 구성요소에 대한 단편적인 요구사항만을 다루고 있다. 이에 본 논문에서는 체계적인 방법인 위협모델링을 수행하여 SUMS에서 발생할 수 있는 위협들을 모두 식별하였고, 이러한 위협을 완화하기 위해 필수적으로 고려해야 하는 보안성 평가기준을 도출하였다. 이러한 보안성 평가기준은 SUMS 구축 시 어떤 보안기능이 필요한지에 대한 상세 정보가 포함된 보안 요구사항을 나타내며, UN R156의 보안 요구사항과 매핑된다. 따라서 본 논문에서 제시하는 보안성 평가기준은 SUMS의 보안 수준을 평가하는 지표로 사용될 수 있다. 뿐만 아니라 본 논문에서 제안하는 보안성 평가기준은 기존의 UN R156보다 상세한 정보를 제공하기 때문에 OEM이 이를 참고하는 경우 안전한 SUMS를 구축할 수 있을 것으로 기대된다.

References

[1] C. Miller and C. Valasek “Remote Exploitation of an Unaltered Passenger Vehicle,” Black Hat USA, Aug. 2015.

[2] S. Nie, L. Liu and Y. Du, “Free-Fall: Hacking Tesla from Wireless to CAN Bus,” Black Hat USA, Jul. 2017.

[3] R.P. Weinmann, B. Schmotzle, "T-BONE: Drone vs. Tesla," CanSecWest Conference, Apr. 2021.
[4] UNECE, "Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system," UN R156, Mar. 2021.
[5] A. Shostack, Threat modeling: Designing for security, 1st Ed., John Wiley & Sons, Feb. 2014.
[6] C.W. Lee and S. Madnick "A system theoretic approach to cybersecurity risks analysis of passenger autonomous vehicles," MIT Sloan Research Paper, no. 5724-18, pp. 1-34, Feb. 2018.
[7] T. Placho, C. Schmittner, A. Bonitz and O. Wana, "Management of automotive software updates," Microprocessors and Microsystems, Vol. 78, Oct. 2020.
[8] A. Mukherjee, R. Gerdes and T. Chantem, "Trusted Verification of Over-the-Air (OTA) Secure Software Updates on COTS Embedded Systems," In Proceedings of the Third International Workshop on Automotive Vehicle Security, Jan. 2021.
[9] C. Ponsard and D. Darquennes, "Towards Formal Security Verification of Over-the-Air Update Protocol: Requirements, Survey and UpKit Case Study," In Proceedings of the 7th International Conference on Information Systems Security and Privacy - Volume 1: ForSE, pp. 800-808, Jan. 2021.
[10] Z. Wu, T. Liu, X. Jia and S. Sun, "Security design of OTA upgrade for intelligent connected vehicle," In Proceedings of the 1st International Conference on Control and Intelligent Robotics, pp. 736-739, Jun. 2021.
[11] R. Kirk, H.N. Nguyen, J. Bryans, S. A. Shaikh and C. Wartnaby, "A formal framework for security testing of automotive over-the-air update systems," Journal of Logical and Algebraic Methods in Programming, Vol. 130, Jan. 2023.
[12] A. Ghosal, S. Halder and M. Conti, "Secure Over-the-Air Software Update for Connected Vehicles," Computer Networks, Vol. 218, Dec. 2022.
[13] J. Yu, S. Wagner and F. Luo, "An STPA-based Approach for Systematic Security Analysis of In-vehicle Diagnostic and Software Update Systems," Computer Science, Jun. 2020.
[14] M. Hamad, "A Multilayer Secure Framework for Vehicular Systems," Ph.D. Thesis, Carolo-Wilhelmina Technical University, Feb. 2020.
[15] A. Lautenbach and M. Islam, "Security models," D2, HEAVENS, Mar. 2016.
[16] GENIVI Alliance, "Security Threats& Mitigations," https://genivi.github.io/rvi_sota_server/sec/security-threats-mitigations.html, Oct 2021.
[17] University of Missouri - St. Louis, "Data Flow Diagrams Examples," http://www.umsl.edu/~sauterv/analysis/dfd/dfd_intro.html, Oct. 2021.
[18] Lucidchart. "What is a Data Flow Diagram," https://www.lucidchart.com/pages/data-flow-diagram, Oct. 2021.
[19] Carnegie Mellon University, "Checking Threat Modeling Data Flow Diagrams for Implementation Conformance and Security," http://reports-archive.adm.cs.cmu.edu/anon/isri2006/CMU-ISRI-06-124.pdf, Oct. 2021.
[20] MITRE, "CVE," https://cve.mitre.org/cgi-bin/cvename.cgi, Sep. 2021.
[21] MITRE, "CWE," https://cwe.mitre.org/data/definitions, Sep. 2021.
[22] Y. Ashibani and Q. H.Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," Computers & Security, Vol. 68, pp. 81-97, Jul.

2017.

[23] C. Riggs, C.E. Rigaud, R. Beard, T. Douglas and K. Elish, "A survey on connected vehicles vulnerabilities and countermeasures," Journal of Traffic and Logistics Engineering, Vol. 6, no. 1, pp. 11-16, Jun. 2018.

[24] M.L. Manna, L. Treccozzi, P. Perazzo, S. Saponara and G. Dini, "Performance Evaluation of Attribute-Based Encryption in Automotive Embedded Platform for Secure Software Over-The-Air Update," Sensors, Vol.21, no. 2, Jan. 2021.

[25] M. Zoppelt, R.T. Kolagari, "UnCle SAM: Modeling Cloud Attacks with the Automotive Security Abstraction Model," International Conference on Cloud Computing, GRIDs, and Virtualization, pp. 67-72, May. 2019.

[26] Myoungsu Kim, Junyoung Park, Euns eon Jeong, Insu Oh, Kangbin Yim, Junghoon Park, "OTA Vulnerability on User Equipment in Cloud Services," International Conference on Information Technology Systems and Innovation, pp. 425-428, Oct. 2018.

[27] A.M.K Nasser, and S. Lauzon, "Safety-Driven Cyber Security Engineering Approach Applied to OTA," Embedded Systems, Cyber-physical Systems, and Applications, pp. 8-13, Feb. 2018.

[28] N. Weiss, E. Pozzobon and S. Renner, "Extending Vehicle Attack Surface Through Smart Devices," International Conference on Emerging Security Information, Systems and Technologies, pp. 131-135, Sep. 2017.

[29] M. Levi, Y. Allouche and A. Kontorovich, "Advanced Analytics for Connected Car Cybersecurity," IEEE 87th Vehicular Technology Conference, Jun. 2018.

[30] T. Alladi, V. Chamola, B. Sikdar and Kim-Kwang R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," IEEE Consumer Electronics Magazine, Vol. 9, Issue. 2, pp. 17-25, Mar. 2020.

[31] P. Bajpai, R. Enbody and B.H.C. Cheng, "Ransomware Targeting Automobiles," ACM Workshop on Automotive and Aerial Vehicle Security, pp. 23-29, Mar. 2020.

[32] M.H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," IEEE Vehicular Technology Magazine, Vol. 12, Issue. 2, pp. 45-51, Jun. 2017.

[33] P. Carsten, T.R. Andel, M. Yampolskiy, J.T. McDonald and S. Russ, "A System to Recognize Intruders in Controller Area Network (CAN)," International Symposium for ICS & SCADA Cyber Security Research, pp. 111-114, Sep. 2015.

[34] T. Hoppe, S. Kiltz and J. Dittmann, "Security threats to automotive CAN networks-Practical examples and selected short-term countermeasures," Reliability Engineering & System Safety, Vol. 96, Issue. 1, pp. 11-25, Jan. 2010.

[35] S. Nie, L. Liu, Y. Du and W. Zhang, "Over-the-air: How we remotely compromised the gateway, BCM, and autopilot ECUs of Tesla cars," Black Hat USA, Aug. 2018.

[36] B.M. Luettmann and A.C. Bender, "Man in the middle attacks on auto updating software," Bell Labs Technical Journal, Vol. 12, Issue. 3, pp. 131-138, Sep. 2007.

[37] J.N. Brewer and G. Dimitoglou, "Evaluation of Attack Vectors and Risks in Automobiles and Road Infrastructure," International Conference on Computational Science and Computational Intel

ligence, pp. 84-89, Dec. 2019.
[38] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang and S. Yu, "Attacks and defences on intelligent connected vehicles: a survey," Digital Communications and Networks, Vol. 6, Issue. 4, pp. 399-421, Nov. 2020.
[39] P. Carsten, "In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions," Cyber and Information Security Research Conference, pp. 1-8, Apr. 2015.
[40] H. Wen, Q. Chen and Z. Lin, "Plug-N-pwned: Comprehensive vulnerability analysis of OBD-II dongles as a new over-the-air attack surface in automotive IoT," Proceedings of the 29th USENIX Security Symposium, pp. 949-965, Aug. 2020.
[41] Kyong Tak Cho, "From Attack to Defense: Toward Secure In-vehicle Networks," Ph.D. Thesis, University of Michigan, 2018.
[42] S. Checkoway, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," Proceedings of the 20th USENIX Security Symposium, Aug. 2011.
[43] L. Moukahal and M. Zulkernine, "Security vulnerability metrics for connected vehicles," IEEE International Conference on Software Quality, Reliability and Security Companion, pp. 17-23, Jul. 2019.
[44] M. Charlie, K. Harnett and A. Carter, "Characterization of potential security threats in modern automobiles: A composite modeling approach," DOT HS 812 074, National Highway Traffic Safety Administration, Oct. 2014.
[45] M. Salfer and C. Eckert, "Attack surface and vulnerability assessment of automotive Electronic Control Units," In Proceedings of the 12th International Conference on Security and Cryptography, pp. 317-326, Jul. 2015.
[46] V.LL. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," IEEE International conference on internet of things (ithings) and IEEE green computing and communications (greencom) and IEEE cyber, physical and social computing (cpscom) and IEEE smart data (smartdata), pp. 164-170, Dec. 2016.
[47] ITU-T, "Secure software update capability for intelligent transportation system communication devices," ITU-T X.1373, Dec. 2017.
[48] FASTR Connectivity and Cloud Work Group, "Automotive Industry Guidelines for Secure Over-the-Air Updates," Oct. 2018.
[49] V.K. Saini, Q. Duan, V. Paruchuri, "Threat Modeling Using Attack Trees," Journal of Computing Sciences in Colleges, Vol. 23, Issue. 4, pp. 124-131, Apr. 2008.

〈저자소개〉

서 재 완 (Jaewan Seo) 정회원
2013년 3월~2019년 2월: 한신대학교 정보통신학부 학사
2020년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 보안공학, 자동차 보안성 평가, 위협모델링

곽 지 원 (Jiwon Kwak) 학생회원
2010년 3월~2017년 2월: 중앙대학교 전자전기공학부 학사
2017년 3월~2019년 8월: 고려대학교 일반대학원 사이버국방학과 석사
2019년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 보안성 분석 평가, 정형기법, 고신뢰 시스템 개발

홍 바 울 (Paul Hong) 학생회원
2010년 3월~2015년 2월: 홍익대학교 학사
2015년 3월~2017년 2월: 고려대학교 정보보호대학원 석사
2017년 2월~2020년 3월: 한국전자인증 개발팀
2020년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 보안공학, 위협모델링, 시큐어코딩, 소프트웨어 개발

조 광 수(Kwangsoo Cho) 정회원
2015년 3월~2019년 2월: 호서대학교 컴퓨터공학과 학사
2019년 3월~2021년 8월: 고려대학교 정보보호대학원 석사
2021년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 보안공학, RMF A&A, 시큐어코딩, 소프트웨어 개발

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2004년~현재: 한국정보보호학회 이사
2007년~현재: 대검찰청 디지털수사 자문위원
2011년~현재: 고려대학교 정보보호대학원 정교수
2016년~2018년: 개인정보분쟁조정위원회 위원
2017년~현재: 고려대학교 국방RMF연구센터(AR²C) 센터장
2018년~2020년: 대통령직속 4차산업혁명위원회 위원
2018년~현재: 고려대학교 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2018년~2019년: 육군사관학교 초빙교수
2018년~2020년: 국방부 정보화책임관(CIO) 자문위원
2019년~현재: 중소벤처기업부 규제특례 심의위원
2020년~현재: 해군발전자문위원회 위원
2020년~현재: 서울특별시 스마트도시위원회 위원
2021년~현재: 사이버작전사령부 자문위원
2022년~현재: 고려대학교 스마트모빌리티학부 학부장
〈관심분야〉 보안공학 및 보안내재화 방법론, 자동차 및 무인이동체 보안성 평가 인증, RMF A&A, 암호학 및 블록체인