Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 3 pp. 374-380, 2017

https://doi.org/10.5762/KAIS.2017.18.3.374
ISSN 1975-4701 / eISSN 2288-4688

스마트카 정보보안 침해위협 분석 및 대응방안 연구

이명렬[1*], 박재표[2]
[1]숭실대학교 대학원 컴퓨터학과, [2]숭실대학교 정보과학대학원

An analysis on invasion threat and a study on countermeasures for Smart Car

Myong-Yeal Lee[1*], Jae-Pyo Park[2]
[1]**Dept Computer of Graduate School, Soongsil University**
[2]**Information Science Graduate School, Soongsil University**

요 약 IoT(Internet of Things)는 인터넷을 기반으로 모든 사물을 연결하여 사람과 사물, 사물과 사물, 사물과 시스템 간의 정보를 상호 소통하는 지능형 기술 및 서비스 등을 지칭 한다. 사물인터넷환경의 발전은 더욱 경량화되고 지능적인 센서, 가볍고 다양한 환경에 적용 가능한 네트워크 프로토콜의 발전을 수반하고 있다. 이러한 요소기술의 발전은 안전기능과 사용자 편의성 등을 적용한 스마트카 환경의 빠른 발전을 도모하고 있다. 이러한 발전은 긍정적인 효과를 발휘하기도 하지만 보안 문제가 해결되지 않는다면 스마트카 서비스는 개인 생활의 큰 재앙을 유발 할 수 있다. 스마트카는 기존 차량에 여러 형태의 통신기능이 적용되고 차량을 제어 할 수 있는 다양한 기능이 제공되며 이에 대한 인증우회, 데이터 위변조를 통한 차량의 불법 제어를 통한 오동작 유발, 차량 운행 정보 탈취를 통한 개인 행태 정보 유출 등 다양한 보안 위협을 유발할 수 있다. 이에 본 논문에서는 사물인터넷 환경에서의 스마트카 서비스의 형태를 알아보고 스마트카 서비스가 가지는 보안 위협을 시나리오 기반으로 도출하고 이에 대한 대응 방안을 제시함으로서 안전한 스마트카 활용 방안을 제시하고자 한다.

Abstract The Internet of Things (IoT) refers to intelligent technologies and services that connect all things to the internet so they can interactively communicate with people, other things, and other systems. The development of the IoT environment accompanies advances in network protocols applicable to more lightweight and intelligent sensors, and lightweight and diverse environments. The development of those elemental technologies is promoting the rapid progress in smart car environments that provide safety features and user convenience. These developments in smart car services will bring a positive effect, but can also lead to a catastrophe for a person's life if security issues with the services are not resolved. Although smart cars have various features with different types of communications functions to control the vehicles under the existing platforms, insecure features and functions may bring various security threats, such as bypassing authentication, malfunctions through illegitimate control of the vehicle via data forgery, and leaking of private information. In this paper, we look at types of smart car services in the IoT, deriving the security threats from smart car services based on various scenarios, suggesting countermeasures against them, and we finally propose a safe smart car application plan.

Keywords : IoT, New convergence service, Privacy, Smart Car, Security, Sensor Network

1. 서론

스마트카는 운전자와 자동차, 자동차와 주변 환경 및 교통인프라, 그리고 일상생활의 모든 요소들을 유기적으로 연결하는 연결성(connectivity)을 기반으로 교통안전, 혼잡해소뿐만 아니라 다양한 사용자 맞춤형 이동서비스

*Corresponding Author : Myong-Yeal Lee(Soongsil University)
Tel: +82-10-3582-1706 email: biggale@gmail.com
Received January 19, 2017 Revised (1st February 22, 2017, 2nd March 8, 2017)
Accepted March 10, 2017 Published March 31, 2017

산업을 창출할 수 있는 미래 성장동력이다[1, 2]. 스마트카는 자동차 기술에 차세대 정보통신 기술을 접목시킨 지능형 자동차이다. 자동차 내·외부의 무선 통신을 이용하여 일반적으로 디바이스와 자동차, 자동차와 사용자 기기들과 연결되어 차량의 상태를 실시간 인식하여 무선 통신을 통한 제어 및 운행 효율성 등의 기능을 제공하는 형태로 구성되어 있다. 스마트카는 기존 자동차 내의 각종 디바이스 및 센서간에 데이터를 주고받을 수 있는 TMU(Telematrics Unit)을 이용하며, 무선 통신(3G/LTE, Bluetooth)을 이용하여 차량과 접속을 제공함으로써 지능화된 자동차 서비스가 가능하도록 하는 방식을 의미한다[3]. 궁극적으로 이러한 스마트카 서비스는 무선통신 기술을 통해 차량 내 정보제공 및 원격 제어 등을 통해 안정성 및 편의성의 극대화를 추구하는데 목적이 있다. 스마트카의 발전은 안전하고 편리한 차량 운행 환경을 제공하는 긍정적인 효과가 존재하나 정보보안 측면의 보호대책이 수립되지 않는다면 인간의 생명과 안전에 막대한 영향을 줄 수 있다. 이에 최근 ITU-T(International Telecommunication Union Telecommunication Standardization), ISO(International Organization for Standardization), ETSI(European Telecommunications Standards Institute) 등 다양한 기구에서 보안통신 기술, 각 개체 간 상호인증 기술, 해킹 방지 기술 등에 대한 표준화가 지속적으로 이루어지고 있다[4]. 그림1은 스마트카 서비스 환경의 일반적인 구성이다. 위와 같이 다양한 요소 기술의 구현을 통해 구축되는 스마트카 환경은 다양한 보안 위협을 가지고 있으며, 이에 대한 해결 방안을 요구하고 있다.

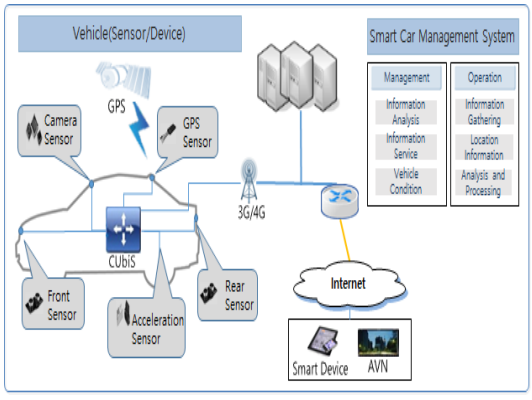

Fig. 1. Smart Car Service

2. 관련 연구

2.1 스마트카 시장 동향

스마트 자동차 시장은 2016년까지 연평균 36%이상 성장하고 있으며 2019년 3,011억 달러 규모로 성장할 것으로 ABI Research 등 국내외 다양한 연구조사 기관은 예측하고 있다[5]. 스마트 자동차를 구현하기 위한 기술은 대부분 IT기술과의 융합을 통해 일어나고 있으며, 안전기능을 높일수록 기술적 복합도가 상승하고, 차량의 더욱 많은 정보를 수집 할수록 이를 분석/처리 할 수 있는 능력도 이에 비례하여 요구되기 때문에, 차량의 제조원가 중에 전자장비의 비중은 점차 높아지고 있다. 차량 대당 70여개의 ECU와 1억 라인 이상의 SW가 탑재되는 등 전자 장치의 비중은 2020년 50% 이상 확대될 것으로 전망된다[6].

2.2 주요국 스마트카 육성 정책

기존 자동차 산업의 발전과 함께 정보통신 환경의 복합적인 발전을 가져올 스마트카 시장 환경의 변화는 각국의 스마트카 육성 정책에서 살펴볼 수 있다[7]. 표 1은 주요국 스마트카 육성 정책 현황이며, 차세대 전략산업으로서의 스마트카의 중요성이 증대되고 있음을 확인 할 수 있다.

Table 1. Status of smart car promotion policies in major countries

Country	Description
US	- Establishment of strategies for R&D of future information-centric vehicles and the industry's support for technology development particularly for key automotive companies - Demonstration projects of freedom cars & fuel and investment of 271 million dollars
Europe	- As part of EU2020's smart sustainable growth (EU's vision for economic growth), push forward with EPoSS, a policy of technology development for smart systems, including smart cars
Japan	- Establishment of an industry/government /academia-collaborated smart car realization roadmap and R&D since early 2000
China	- Inclusion of next-generation cars in the 7 major strategic newly-rising industries in the 12th round 5-year plan (2011-2015) - Fund support given when any of the country's domestic car companies take over an overseas company with advanced technology
South Korea	- The Ministry of Science, ICT and Future Planning has chosen the smart car industry as one of the 7 major strategic industries for achieving 40,000 dollars in per capita income

2.3 국내 주요 스마트카 사업 추진 현황

국내 스마트카 시장은 해외 업계 대비 사업 추진이 다소 늦은 감은 있으나 업계 경쟁력을 보유한 인포테이먼트 분야를 기점으로 사업 확대를 도모하고 있는 양상을 보이고 있다[8]. 또한 현대, 기아자동차 등 상용차 업체와 삼성전자, LG 전자 등 ICT 업체가 스마트카 사업에 대한 전략 및 투자계획을 수립하고 연구 개발을 수행하고 있다. 표2는 국내 주요 기업의 최근 스마트카 관련 사업추진 현황을 보여주고 있다[9]. 국내의 경우 특히 ICT 업체 기반 다양한 스마트카 상용 기술에 대한 표준화 및 연구가 이루어지고 있다.

Table 2. Domestic enterprise business promotion status

company		Description
Cars	Hyundai/Kia Motors	- Release of Blue Link, an in-vehicle infotainment system for smart cars (2011) - Hyundai Autron established, with the aim of independently developing semiconductors for cars (Apr 2012)
	Hyundai Mobis	- Performance improvement of electronic sub assemblies and research for domestic production; development of vehicle communications systems
	Mando Corporation	- Efforts to develop electronic sub assemblies for chassis, such as smart cruise and automatic parking - Took over DSP-Weuffen GmbH, a German driver assistant system maker, acquiring the related technology (Nov 2013)
ICT	Samsung Electronics	- Temporarily focused on the infotainment solution area rather than on smart car parts - Entered an agreement with BMW and Tata Motors (India) to use its smart device connectivity solution - Took over Harman to strengthen its position in the area of infotainment (Nov 2016)
	LG Electronics	- Gave the most aggressive response among the key domestic companies, such as newly establishing a VC (Vehicle Components) operations division - Sought synergy with its vehicle-related divisions (Chem, Hausys, Innotek, CNS)
	LG Display	- Focused on regular displays and vehicle displays as new enterprises
	SK hynix	- Focused on the infotainment area, in collaboration with nVidia
	SKT	- Released T Car, a smart car service for aftermarket through auto repair shops, etc. (Jan 2014)
	Hancom	- Took over MDS Technologies, a leading domestic company in vehicle software (Mar 2014)

3. 스마트카 정보보안 예상위협 분석

3.1 스마트 교통서비스 정보보안 예상위협 분석

사물인터넷 환경의 교통서비스의 고도화는 사용자 편의성 및 안전에 대한 다양한 서비스를 통한 삶의 질을 향상 시킬 수 있다. 다만 스마트 교통서비스의 정보보안 침해사고는 인간의 목숨 및 금전적인 문제들이 연계될 수 있기 때문에 정보보안에 대한 중요성이 강조되고 있다. 스마트카는 기존 차량에 여러 형태의 통신기능이 적용되고 차량을 제어 할 수 있는 다양한 기능이 제공되며 이에 대한 인증우회, 데이터 위·변조를 통한 차량의 불법 제어를 통한 오동작 유발, 차량 운행 정보 탈취를 통한 개인 행태 정보 유출 등 다양한 보안 위협이 존재한다. 스마트카 교통 환경에서 발생할 수 있는 예상 위협 및 위험은 표 3과 같이 분석할 수 있다.

Table 3. Smart Traffic Security Threats

Category	Description
Wire tapping and information leak	- Attacker acquires sensor information by illegally gaining access to the center - Data leak by sniffing Bluetooth and wireless communications - Leak of information by connected devices in the vehicle
Personal information infringement	- Analysis of personal information such as the state of vehicle and owner information, after leak of vehicle information and stored information - Analysis of individuals' behavior information after leak of vehicle drive history information, etc.
Data forgery/alteration	- Attacker sends forged/altered control data over wireless communications, including Bluetooth - Illegal behavior is induced in automatic control devices such as vehicle startup and door lock
Impersonation attack	- The attacker illegally gains access to a device containing authentication information for identifying personnel, copies the information, and impersonates as a legitimate user of the system
Denial of service attack	- Attacker repeatedly sends meaningless data to interfere with Bluetooth/wireless communications, preventing normal service
Physical attack	- Attacker infers vehicle information with a physical type of attack, such as analyzing the internal memory voltages
Location tracking	- Attacker uses the unique identity information of a user to find out their location and route history
Fuzzing attack	- The valid physical range of a smart car or system is either scaled up or scaled down to cause errors - Data that shouldn't be sent to a smart car or system are sent to cause errors

3.2 스마트 교통서비스 위협 예상 시나리오

스마트 교통서비스 환경에서 발생 할 수 있는 보안 위협에 대한 예상 시나리오는 표 4와 같이 분석할 수 있다.

Table 4. Smart Traffic Security Threats Scenario

Scenario	Description
Vehicles are controlled and manipulated using apps infected with malicious codes	- Gets users to install an app infected with malicious codes to maliciously control and manipulate their vehicles without authorization
Data are altered and vulnerabilities in the wireless communication are exploited to control vehicles and cause malfunctions	- Devices such as smartphones connected to vehicles and the communication interface are maliciously misused and data are altered to control the vehicles or cause malfuncitons
Denial of service attack to cause malfunction in the vehicle sensors	- A large number of packets are sent to the smart car controller to cause malfunction in the vehicle's control sensor
Telematics server is attacked to obtain power to control vehicles	- Telematics server, one of the smart car services, is attacked to try to obtain server privileges, in which case the attacker would be able to control the vehicles of all users subscribed to the service

3.2.1 악성코드가 감염된 앱을 이용한 차량 제어 및 조작

스마트카의 경우 차량과 연결된 센서를 스마트폰 및 AVN 등을 통해 컨트롤하고 스마트카 관리시스템과 연동하여, 해당 차량의 다양한 정보를 수집, 활용한다. 스마트카를 제어하는 스마트폰에 악성코드가 설치 될 경우 그림 2와 같이 공격자에게 차량 제어권을 탈취 당할 수 있다.

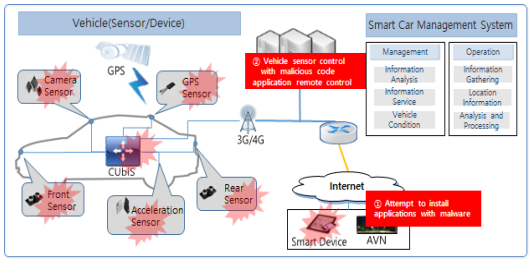

Fig. 2. Threats Scenario #1

악성코드가 감염된 앱을 이용한 차량 제어 및 조작에 대한 예상 위협 프로세스는 다음과 같다.

① 공격자는 악성코드에 감염된 차량 진단 앱을 다운로드 및 설치하게 유도한다.

② 공격자는 설치 된 앱을 원격 조정하여 차량 제어 및 오동작 하도록 조작할 수 있다.

3.2.2 무선통신 취약점 및 데이터 위변조를 통한 차량의 제어 및 오동작 유발

스마트 자동차 시스템의 센서 통신이 블루투스 및 무선 등으로 송수신 될 경우 무선으로 인한 도청, 패킷 위변조 취약점에 노출 될 수 있으며 그로인해 그림 3과 같이 차량 불법 제어 및 오동작을 유발시킬 수 있다.

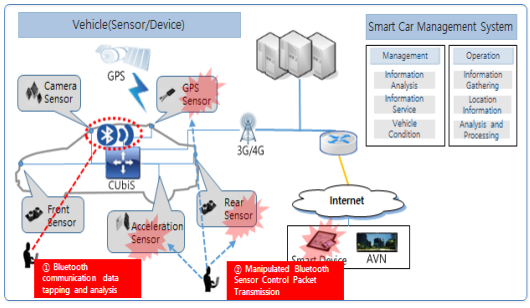

Fig. 3. Threats Scenario #2

무선통신 취약점 및 데이터 위·변조를 통한 차량의 제어 및 오동작 유발에 대한 예상 위협 프로세스는 다음과 같다.

① 공격자는 자동차에 연결된 스마트폰 블루투스 통신 데이터를 도청하여 분석한다.

② 공격자는 분석된 도청 데이터를 바탕으로 통신 패킷을 위변조하여 차량 제어 및 오동작을 유발할 수 있다. 이를 통해 공격자는 달리는 자동차의 속력을 높인다거나 시동을 제어하여 대형 사고를 유도할 수 있다.

블루투스 통신 공격에 이용되는 취약점은 표5와 같다.

Table 5. BlueTooth Security Threats

Category	Description
Bluejacking	- Messages or files that attempt spam or phishing attacks are sent to a mobile unit with Bluetooth support
Bluesnarfing	- Firmware vulnerabilities of a Bluetooth device are exploited to attack the vulnerability that allows access to data stored in the device
Bluebugging	- Firmware vulnerabilities of a Bluetooth device are exploited to obtain access privileges to the device
Car Whisperer	- Attacks vehicles with vehicle kit support, where vulnerabilities that allow listening in on audio signals and sending altered data are exploited

3.2.3 서비스 거부 공격을 통한 자동차 기기 오동작

스마트 자동차 서비스의 구성은 자동차(센서/디바이스)와 스마트카 관리시스템(텔레메틱스)와 자동차 제어를 위한 사용자 스마트기기 및 AVN 등으로 구성되어 있다. 이때 서비스거부공격에 대한 설계가 이루어지지 않을 경우 서비스거부공격에 의한 센서 오동작이 발생할 수 있다.

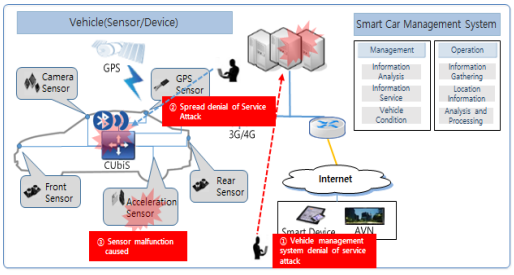

Fig. 4. Threats Scenario #3

서비스 거부 공격을 통한 자동차 기기 오동작에 대한 예상 위협 프로세스는 다음과 같다.

① 공격자는 스마트카 관리시스템에 대한 서비스거부 공격을 수행한다.

② 공격자는 블루투스 및 무선에 대한 서비스 거부 공격을 수행한다.

③ 예상치 않은 서비스 불가 상태로 인하여, 운행 중인 자동차의 센서가 오동작하여 사고를 유발 할 수 있다.

3.2.4 텔레메틱스 서버 공격을 통한 자동차 제어권 획득

텔레메틱스 서버가 공격자에 의해 탈취될 경우 가입된 모든 자동차에 대한 제어권을 공격자가 획득하게 되며, 이를 통하여 공격을 수행할 수 있다.

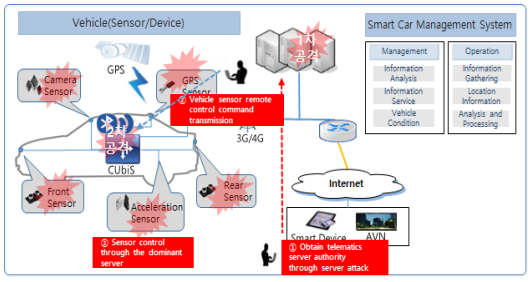

Fig. 5. Threats Scenario #4

텔레메틱스 서버 공격을 통한 자동차 제어권 획득에 대한 예상 위협 프로세스는 다음과 같다.

① 공격자는 텔레메틱스 스마트카 관리 시스템의 취약점을 통해 1차로 서버 제어권을 획득한다..

② 공격자는 텔레메틱스 서비스 장악을 통해 모든 가입자에게 원격 명령을 수행할 수 있다.

③ 악의적인 공격자는 이를 통해 원격 서버에서 센서를 조작하여, 교통사고 유발 등의 범죄에 악용할 수 있다.

4. 스마트카 환경의 예상 보안위협별 대응방안

위에서 분석한 스마트카 환경에서의 보안 위협에 대해 차량, 네트워크 구간, 관리시스템, 스마트기기 등 4개 부문에 대한 보호대책을 수립하여야 하며, 이와 이를 위한 대응방안을 제안한다. 스마트 카의 불법적인 접근 및 위장공격에 대응 할 수 있은 기기인증의 방법과 사용자 인증, 네트워크 구간의 도청 및 정보유출에 대응하기 위한 데이터 암호화 및 통신구간 암호화 등을 통하여 안전한 스마트카 환경을 구현할 수 있다. 이에 따라 표 6과 같이 스마트카 환경의 보안 위협별로 대응할 수 있는 대응방안과 적용기술을 도출하였다.

분석된 예상 위협별 대응방안에 대한 적용기술은 다음과 같다.

스마트카 하드웨어 해킹을 통한 정보 유출에 대한 위협은 데이터암호화(공개키 기반 암호화)를 통한 메모리 추출에 의해 데이터 노출을 방지할 수 있으며, 하드웨어에 존재하는 UART, LIN 등의 인터페이스 즉, 기능 제거에 의해 대응이 가능하다.

차량에 저장된 정보 유출을 통한 소유자 정보 노출 위협은 공개키 기반의 사용자 정보 데이터 암호화와 스마트카 관리 시스템과 차량간의 차대번호 및 생체인증을 통해 대응이 가능하다.

블루투스 및 무선 통신간 제어 데이터 위변조 공격을 통한 제어권 획득 위협은 AES 및 MD5를 통한 스마트기기 및 텔레매틱스 구간 통신 시 무결성 제공을 통해 대응이 가능하고 위조된 사용자 식별 정보를 통한 인증 위협은 사용자 식별 시 기기인증 및 사용자 인증을 통해 위조 확인 및 무결성 검증 절차 제공으로 대응이 가능하며, 차량 센서와 관리 시스템간 통신 방해 유·무선 데이

터 전송 위협은 차량과 관리 시스템간 통신 시 인증된 기기 및 사용자만이 사용할 수 있는 인증기법을 통해 대응이 가능하다.

Table 6. Security Threats and Countermeasures

Threat	Attack	Countermeasure		Relative Techniques
Physical threats	Information leak by hacking the hardware of a smart car	Encryption	Using data encryption to prevent data leak by memory extraction	Public key-based encryption
Functionality removal		Functionality removal	Removal of interfaces that exist in hardware such as UART and LIN	Hacking of UART and firmware
Personal information infringement	Leak of owner information by leak of data stored in the vehicle	Encryption	Data encryption for user data	Public key-based encryption
	Leak of behavior information by leak of data such as vehicle driving history	Authentication	Smart car management system and vehicle-to-vehicle authentication	Chassis no. , biometric authentication
		Encryption	Zone encryption for management system and vehicles	AES, DES, IDEA
Data forgery/alteration	Obtaining control privileges by forgery/alteration of control data sent via Bluetooth/wireless communications	Integrity	Integrity for zone communication for smart devices and telematrics	AES, MD5
Impersonation attack	Authentication by identity information of a fake user	Integrity	Check user identity forgery and veirfy integrity during user authentication	Device authentication, user authentication
Denial of service	Wired/wireless data sent to interfere with the communication between vehicle sensors and the management system	Authentication	Authentication allowing only authorized devices and users during communication between vehicles and the management system	Device authentication, user authentication

5. 결론

스마트카는 다양한 정보통신 요소기술이 적용 되어 있으며, 특히 네트워크, 센서 그리고 텔레메틱스 부문에 대한 적용이 증가하고 있다. 이러한 요소 기술 적용은 사용자의 개입 없는 주행과 주차, 차선이탈 방지 등의 사용자 편의성 및 안전기능의 강화를 통하여 더욱 안전하고 편리한 운영 환경을 제공하는 장점을 가지고 있다. 다만 이로 인해 다양한 정보보호 관점의 문제가 유발될 가능성이 존재하며 본 연구는 스마트카의 구성요소를 정의하고, 발생 가능한 위협을 시나리오 기반으로 살펴보고 이에 대한 대응 방안을 분석하였다.

스마트카는 카메라, GPS, 전후방, 가속도 센서 등 다양한 센서와 블루투스, 3G/4G 모듈 등의 통신 모듈, 무선통신과 GPS 기술이 결합되어 차량의 위치 정보, 안전운전, 엔터테이먼트 등 다양한 서비스를 제공하는 텔레메틱스 등과 같은 차량에 설치되는 구성요소와 차량 정보분석, 안내서비스, 상태관리, 정보수집 분석 처리를 수행하는 통합관리 및 운영서버로 구성된 스마트카 관리 시스템 환경으로 구성된다. 이러한 구성 환경에서 발생 가능한 보안 부문의 위협은 스마트카 하드웨어 해킹을 통한 정보 유출, 차량에 저장된 운행 정보 등의 유출을 통한 개인정보 침해, 통신 구간 데이터 위변조 공격을 통한 제어권 획득 및 위조된 사용자 식별 정보를 통한 부정 인증을 유발 할 수 있는 위장 공격, 무선 통신 방해를 통한 서비스 거부 공격 등을 유발 할 수 있다. 이를 통해 공격자는 차량 소유자의 개인정보를 활용한 행태정보 분석, 차량 제어권 획득을 통한 운행 개입 등을 수행할 수 있다.

본 연구를 통해 데이터 암호화, 하드웨어에 존재하는 URAT, LIN등의 인터페이스 제거를 통한 물리적 공격에 대한 대응, 차량과 관리시스템 간 인증 및 사용자 정보 암호화를 통한 개인침해 공격 대응 기기인증 및 무결성 검증을 통한 데이터 위변조, 위장 공격 대응 등 구간, 구성별 보안 대응 방안을 도출 할 수 있었다.

본 논문에서 수행한 스마트카 환경의 보안 위협과 대응방안이 스마트카 산업 발전과 더불어 함께 발전하여야 하는 정보보안에 대해 상기 할 수 있는 기회가 될 것으로 기대한다.

References

[1] Jae-Kwan Lee, "Smart Car Trends and Industrial Challenges," *International Computer Symposium 2016*, *The Institute of Electronics Engineers of Korea*, pp. 19, Apr. 2016.

[2] Jeong-Ho Kim, Jyung-Hwan Song, Moon-Seog Jun, “Multiple authentication protocol for secure communications in Internet of Things,” *Korea Academia-Industrial Cooperation Society Conference Fall*, pp. 382-384, 2014.

[3] Cheol-Hui Kim, "IT industry major mega Trends,"

Report of Policy, The Federation of Korea Information Industries, pp. 111, 2014.

[4] Su-Min Park, Jin Kwak, "Next Generation Intelligent Transportation System(C-ITS) Status of domestic and foreign countries and major security standardization trends," *Korea Institute of Information Security And Cryptology*, pp. 53-59, Oct. 2015.

[5] Jong-Seon Park,Hyeok-Jin Yoon, "Smart Car Industry," *Eugene Investment Research Report*, pp. 30, Jan. 2014.

[6] Jeong-A Jang, Dong-Young Kwak, "Car-IT Technology and service development strategy," *Korea Institute of Information Technology Magazine 9*, pp. 11-18, Apr. 2011.

[7] Jong-Won Park, Chang-Ho Yun, Chel-Sang Yoon, Xingchen Jiang, Hae-Sun Jung, Yong-Woo Lee, "An IoT Platform for Smart City," *Spring Conference*, *Korean Society For Internet Information*, pp. 53-54, Apr. 2016.

[8] Eun-Ji Jang, Tai-Keong Jeong, Woong-Jae Lee, "Landing on Smart Vehicle and Autonomous Technology with IoT Data Transferring Methodology," *Spring Conference, Korean Society For Internet Information*, vol. 17, no. 1, pp. 211-212, Apr. 2016.

[9] Yun-Jeong Jo, "Smart car market expansion Domestic ICT industry Corresponding task," *KDB Industry Bank*, 2016.

이 명 렬(Myong-Yeal Lee) **[정회원]**

- 2011년 2월 : 숭실대학교 정보과학대학원 정보보안학과 (공학석사)
- 2012년 3월 ~ 현재 : 숭실대학교 대학원 컴퓨터학과 박사과정

<관심분야>
정보보안, 사물인터넷, 개인정보보호, 디지털포렌식

박 재 표(Jae-Pyo Park) **[종신회원]**

- 1998년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학석사)
- 2004년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학박사)
- 2010년 3월 ~현재 : 숭실대학교 정보과학대학원 교수

<관심분야>
네트워크 보안, 디지털포렌식, 금융IT