스마트 자동차 원격접속 보안성 강화 방안

김충배O, 이영준*
O한국교원대학교 컴퓨터교육과,
*한국교원대학교 컴퓨터교육과
e-mail: cbkim@knue.ac.krO, yjlee@knue.ac.kr*

A Strategy to Strengthen Security for Remote Access of Smart Cars

Choungbae KimO, Youngjun Lee*
ODept. of Computer Education, Korea National University of Education,
*Dept. of Computer Education, Korea National University of Education

● 요 약 ●

본 논문에서는 스마트 자동차를 외부에서 제어할 수 있는 원격접속의 보안성을 강화할 수 있는 방안을 제안한다. 다양한 자동차 제조사들이 물리적인 자동차 구동에서 나아가 정보통신기술을 접목하여 운전자에게 다양한 편의성을 제공하고 있다. 정보통신기술을 이용해 자동차의 기능이 증가하는 만큼 정보시스템의 취약성을 이용해 외부의 비인가자에 의한 침입이 이루어질 수 있는 취약성 또한 증대하며, 자동차의 경우 이러한 위협이 주행 중 발생 시 운전자의 생명까지 위협할 수 있는 매우 위험한 상황이 발생할 수 있다. 이에 외부로부터 비인가자의 접근을 차단할 수 있는 방안을 기존 정보통신시스템 보안 기법을 접목하여 스마트 자동차의 안전한 운행이 가능할 수 있도록 한다. 본 논문에서는 기존 정보통신시스템에서 활용 중인 보안 방안을 통하여 제안하는 스마트 자동차 원격접근 제어 정책이 기존의 스마트 자동차 정보보안 정책에 비해 보안성 향상 면에서 더 우수함을 보인다.

키워드: 스마트카(smart car), 접근제어(access control)

I. Introduction

인류의 편리함을 추구하는 방향성이 단순히 바퀴를 사람의 힘으로 굴리는 인력거에서부터 시작하여, 내연기관을 이용해 동력장치를 통한 자동차를 만들어내었으며, 정보통신기술이 3차 산업혁명 시대를 거쳐 급속도로 발전하여 현재 진행 중인 4차 산업혁명 시대를 맞이하며 각 분야의 장점만을 접목하여 자동차의 각 분야를 정보통신기술로 제어할 수 있는 스마트 자동차까지 발전하였다. 자동차의 다양한 부문을 차량 내·외부에서 제어할 수 있도록 정보기술을 접목시켜 운전자에게 편의성을 대폭 향상시키며 차량 구매 시 이러한 편의성을 지닌 스마트 자동차를 자동차 구매자들이 선호하는 경향을 보인다. 하지만 정보통신기술 분야에서 간과하면 안 될 부문이 바로 정보보안이다. 정보기술개발 시 중점추진사항을 살펴보면 대부분 사용자의 편의성을 주요 목적으로 두고 있다. 하지만 정보통신기술은 기본적으로 다양한 취약성을 지니고 있기 때문에 정보보안을 고려하지 않고 개발 시 애기치 못한 취약성이 나타날 수 있고, 이로 인해 사용자의 중요한 정보자산이 유출되거나 변조·파괴될 수 있으며, 스마트 자동차와 같이 자동차의 물리적인 제어 부문을 외부에서 변조할 시 사람의 생명까지 위협할 수 있는 매우 위험한 상황이 발생할 수 있다. 본 논문에서는 이러한 취약성을 예방할 수 있는 보안성 강화 방안을 기존 정보통신기술 보안 강화의 시각에서 접근하여 제안하고 있다.

II. Preliminaries

1. Related works

1.1 스마트 자동차 구성

Fig.1은 스마트 자동차의 일반적인 구성이다. 기존 자동차의 구성에 다양한 센서가 탑재되었으며, 무선 네트워크 ethernet 통신으로 차량 외부와 연결되어 운전자가 차량 내부에 없어도 차량을 관제, 제어할 수 있다.

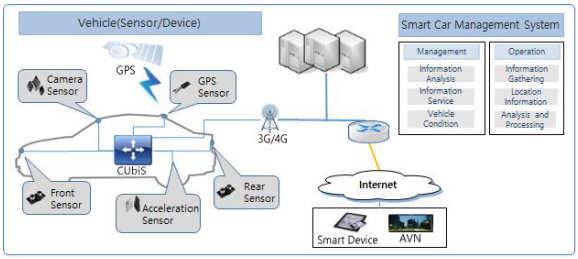

Fig. 1. Smart Car service[1]

기존의 CAN 통신 방식의 차량 내부에서만 이루어지던 통신이 물리적인 접근 시도가 제한 없는 무선 방식의 통신이 구현되며 다양한 보안 취약성을 지니게 되었다.

III. The Proposed Scheme

정보기술 분야에서의 전통적인 정보보안 방안은 기본적으로 인가된 사용자만 정보시스템에 접근할 수 있는 접근제어 기술이 있다. 시스템에 등록된 사용자 계정 정보를 확인하여 인가된 사용자만 접근할 수 있도록 하는 사용자 인증 방식에 네트워크 관점에서 보는 MAC(Media Access Control) 주소와 IP 주소를 통해 등록된 주소만 인증하는 방법, 나아가 OTP(One Time Password), 생체인식 방식까지 결합하여 Multi-Factor 방식의 인증을 통해 사용자의 원격접속기기 MAC, IP 주소가 Spoofing되어 공격받는 시나리오를 대비해 Cellular 방식의 인증, 등록된 홍채 및 지문 인증까지 다양한 인증방식을 결합하여 외부에서의 접근을 보다 다각화된 방향으로 제어하고 보안성을 강화할 수 있다.

이러한 Multi-Factor 인증 방식이 기존 정보통신기술 보안 방식에서도 통합 위협관리(UTM; Unified Threat Management)시스템을 통해 다양한 보안 기능을 하나의 물리적 장비로 구현되어 있다. 방화벽, 침입방지시스템(IPS; Intrusion Prevention System), 가상사설망(VPN; Virtual Private Network) 등 하나로 통합되어있듯이, 차량 내·외부 네트워크 접점에 Multi-Factor 인증 시스템을 차량에 맞게 소형 장비로 구현하여 장착한다면, 특정 소수의 차량 소유자만 접속하는 특성 상 고성능을 요구하지 않아 해당 제안이 적용 가능할 것이다.

IV. Conclusions

본 연구를 통해 제안한 접근제어 보안 강화 방안으로 기존의 계정 접근 방식보다 더 강화된 접근 단계를 통해 취약성을 예방할 것으로 예상한다. 새로운 물리적인 장비와 인증기술이 추가되어 비용이 증가하고, 인증단계의 다단화로 초기 접속에 다소 불편함이 증가할지라도, 운전자의 생명을 위협하는 매우 위험한 취약성은 편의성 및 비용과 맞바꿀 수 없는 매우 중요한 사항임을 다시 한 번 강조한다. 또한 이러한 강화 방안이 향후 자동차 제조업에서 초기 개발 단계에 적용되어 운전자의 안전을 보다 강화할 수 있기를 기대한다.

REFERENCES

[1] Myong-Yeal Lee, Jae-Pyo Park, “An analysis on invasion threat and a study on countermeasures for Smart Car” Journal of the Korea Academia-Industrial cooperation Society, Vol. 18, No. 3 pp. 374-380, 2017