http://dx.doi.org/10.14400/JDC.2014.12.2.549

안전한 지능형 자동차를 위한 개인키 기반의 인증 기법에 관한 연구

이근호
백석대학교 정보통신학부

A Study of Authentication Scheme based on Personal Key for Safety Intelligent Vehicle

Keun-Ho Lee
Division of Information Communication, Baekseok University

요 약 IT와 융합한 지능형 자동차에 대한 연구가 현재 활발히 진행중이다. 안전한 지능형 자동차 서비스를 위해 다양한 통신 기술이 제공이 되고 있다. 지능형 자동차가 통신기술을 이용한 서비스가 제공되면서 다양한 보안위협 요소가 도출되고 있다. 지능형 자동차에서 보안 인증 솔루션을 위해서는 소유권, 지식, 생체정보를 포함하고 있어야 한다[6,7]. 본 논문에서는 지능형 자동차의 보안위협 요소를 분석하고 지능형 자동차의 보안 솔루션인 생체정보를 이용한 인증 기법을 제공한다. 기존의 지능형 자동차 인증보안 솔루션보다 높은 보안성을 갖는 구현의 문제점이 해결되도록 사용자 생체인증기법을 제안한다.

주제어 : 인증, 신체정보, 보안, 지능형 자동차, 개인키

Abstract Studies on the intelligent vehicles that are converged with IT and vehicular technologies are currently under active discussion. A variety of communication technologies for safety intelligent vehicle services are support. As such intelligent vehicles use communication technologies, they are exposed to the diverse factors of security threats. To conduct intelligent vehicle security authentication solutions, there are some factors that can be adopted ownership, knowledge and biometrics[6,7]. This paper proposes to analyze the factors to threaten intelligent vehicle, which are usually intruded through communication network system and the security solution using biometric authentication scheme. This study proposed above user's biometrics information-based authentication scheme that can solve the anticipated problems with an intelligent vehicle, which requires a higher level of security than existing authentication solution.

Key Words : Authentication, Biometric, Security, Intelligent Vehicle, Personal Key

1. Introduction

Rapid growth of IT technologies is encouraging a variety of service models to come out. In an effort to help their vehicles compete in the marketplace, vehicle

Received 15 January 2014, Revised 16 February 2014
Accepted 20 February 2014
Corresponding Author: Keun-Ho Lee(Baekseok University)
Email: root1004@bu.ac.kr

ISSN: 1738-1916

and truck manufacturers are offering increasingly more potent onboard devices, including powerful computers, a large array of sensors, radar devices, cameras, and wireless transceivers. These devices cater to a set of customers that expect their vehicles to provide seamless extension of their home environment populated by sophisticated entertainment centers, access to Internet, and other similar wants and needs. Powerful onboard devices support new applications, including location-specific services, online gaming, and various forms of mobile infotainment [8].

Among them, intelligent vehicle, which combines with the convenience of IT technology, is being actively studied. Intelligent vehicle requires a massive technological researches for security. The devices of intelligent vehicle, ECU (Electronic Control Unit) is electronic control system that controls the engine, transmission, steering, and brake. It was originally designed to control core engine functions such as fuel injection in engine cylinder and idling. However, as vehicle has been ever developed with more functions to follow, ECU comes to control more functions for today's vehicle. ECU is a kind of a compact computer that regulates and controls almost all the motions of vehicle. It is as important as it can be analogized with human brain. Therefore it is naturally important to detect threats to the security of ECU in an effort to prevent possible risks in advance.

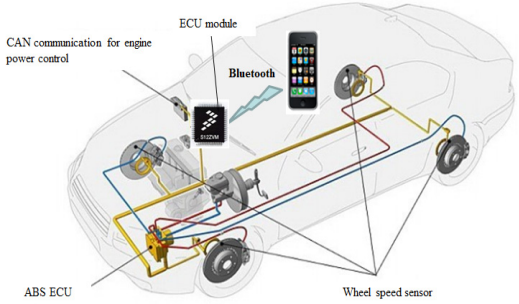
It is foreseeable that security issues will emerge in vehicle industry as development sincerely starts landing on interface of intelligent vehicle. At present, some technologies have been developed that a vehicle is connected to Smartphone-ECU interlinked mobile network and Bluetooth (wireless short-distance communication network). And information of a vehicle can be read by applications which are connected to a vehicle. However, the access to those services only requires simple user-authentication process, so they are vulnerable to computer virus attack or hacking.

Intelligent Vehicle system errors by hacking into ECU threatens driver's life and the disclosure of personal information and tapping of telephone and location can lead to the breach of privacy. Therefore a solid security solution is required. The security solution is to prevent, using user's biometric authentication scheme, the leak of personal and vehicle information and to limit the indiscreet access from outside.

One favorable way to protect vehicle is to establish access control system to limit access from outside. Biometric access control means to control the outer access to vehicle system not to read vehicle information and alter vehicle functions unless approved, and approve user to have access to ECU for service by distinguishing user's physical information. The current services that are linked to intelligent vehicle system use a security model that simply requires password-based authentication. This study aims to examine the factors that threaten vehicle security and propose a security solution using biometric authentication scheme that can solve the possible problem caused by hacking of security password.

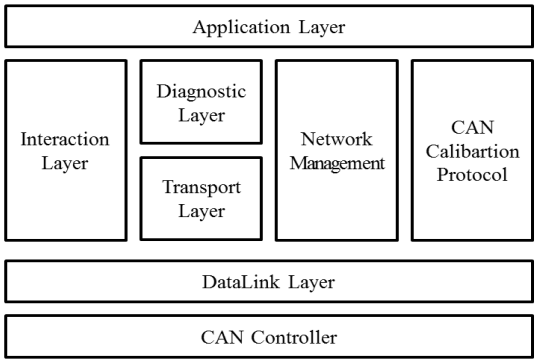
2. Related Work

As seen in Fig. 1, ECU, when intelligent vehicle are linked to external devices, controls the devices of a vehicle in the central system. ECUs are installed at every part of a vehicle that senses and controls vehicle motions. Different by vehicle type, there are 10 to 100 ECUs in a vehicle. They electronically control safety devices (e.g. airbag) and convenience devices (e.g. audio and air conditioner), not to mention the integral parts of a vehicle such as engine dynamometer, brakes, and steering[6]. ECU is composed of a single motherboard. The motherboard used have ROM inside but nowadays FlashROM is installed in it so that it is possible to write firmware easily.



[Fig. 1] ECU architecture and Communication

Therefore, when a certain abnormal signal is received to ECU, the firmware data of FlashROM can be corrupted, resulting in the malfunctions of a vehicle. FlashROM has the merit of writing and erasing data anytime to manage the functions of vehicle more efficiently. However, risks also come along with efficiency as much. As seen in Fig.2, which shows ECU firmware structure, Interaction Layer, Network Management, and Transport Protocol are defined in OSEK while Diagnostic Layer and Transport Protocol are defined in ISO.



[Fig. 2] OSEK/VXD firmware Architecture

CAN(Controller Area Network) is a sort of the standard protocol of a concerned software. CAN Calibration Protocol controls access to ECU FlashROM for reading and writing.

The main purpose of Network Management is to increase the use efficiency of vehicle power source. Transport Protocol is designed to transmit bulky data. It has such functions as data partitioning, synchronization and error sensing. Diagnostic Layer provides the interface of various diagnostic functions installed in a vehicle. In addition, it handles exceptions and requests related to CAN. Interaction Layer handles transmission mode, which is defined when software is configured. It also provides API for data exchange and sets the various default values[5].

3. Intelligent Vehicle Threats

The threats in the VC(Vehicular Cloud) can be classified using STRIDE[9], a system developed by Microsoft for classifying computer security threats. The threat categories are given here.

- **Spoofing user identity**

The attackers pretend to be another user to obtain data and illegitimate advantages.

- **Tampering**

The attackers alter data and modify and forge information.

- **Repudiation**

The attackers manipulate or forge the identification of new data, actions, and operations.

- **Information disclosure**

The attackers uncover personally identifiable information such as identities, medical, legality, finance, political, residence and geographic records, biological traits, and ethnicity.

- **Denial of Service**

The attackers mount attacks that consume system resources and make the resources unavailable to the intended users.

- **Elevation of privilege**

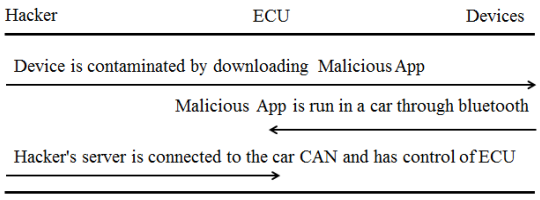
The attackers exploit a bug, system leakage, design flaw, or configuration mistake in an operating system

or software application to obtain elevated access privilege to protected resources or data that are normally protected from normal users[6,9,10,11].

Existing vehicle security solution requires a simple password authentication to approve user to start engine and track location. And ECU of a vehicle and device are automatically communicated on M2M (Machine To Machine) base. Because engine and location-tracking are approved controlled by simple password authentication, it reduces vehicle theft[1.4].

However, the security solution based on password authentication has limits. The password can be stolen and exposed. When it happens, vehicle information is disclosed, which causes another threat to vehicle security. Therefore it is not safe to say that users can blindly dependent on the solution[2].

As seen in Fig. 3, therefore, more efficient security measure should be prepared to tackle the issues related to vehicle security system, as mentioned above, before intelligent vehicles are developed and commercialized in computing vehicle service environment where ECU is connected to diverse communication devices. Virus can break in ECU of a vehicle through device contaminated with malicious code in CAN, of which security is vulnerable. Once a hacker has a grip on ECU, he or she can control a hacked vehicle in distance and wirelessly.

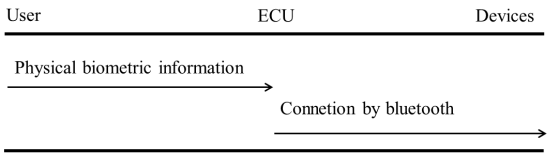


[Fig. 3] Hacking scenario

4. Authentication Scheme

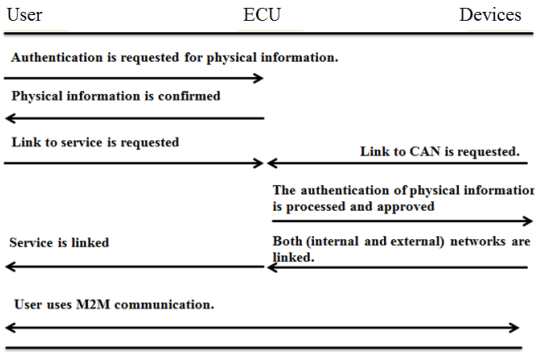
As seen in Fig.4, controlling ECU requires the communication between intelligent vehicle and external devices. This paper suggests that all the motions from the outside to ECU be verified for access by biometric authentication technique.

Access to the internal network of a vehicle must be authenticated by the physical information of user. The biometric information is coded in the terminal equipped with a sensor and added with other input before transmitted to ECU in a vehicle. Since such information is transmitted through M2M communication, the data traffic should be light. Therefore, such information should be hidden in the data to secure confidentiality and traffic efficiency.



[Fig. 4] Device connection by physical biometric information

As seen Fig.5 which shows the authentication process after the input of user bio-information, the authentication proceeds on user and external devices. Fingerprints, pupil or face can be used for physical information.



[Fig. 5] authentication scheme

To use an intelligent vehicle, user requests ECU to conform his/her physical information and ECU

confirms it. After confirmation between user and ECU, user requests ECU to link to a service he wants to use. At the time, external devices are also requested to be linked to use CAN.

The request for external devices is approved through biometric authentication procedure. Session starts to verify the request for external devices. ECU authenticates the link of user to the requested service. Then authentication is confirmed for the use of both networks in vehicle and external network.

5. Conclusion

This study proposed above user's physical information-based authentication technique that can solve the anticipated problems with an intelligent vehicle, which requires a higher level of security than existing one. The technique uses data collection module of a new vehicle to increase security for CAN through the procedures of biometric authentication in an effort to prevent intelligent vehicle from hacking. This paper proposes to analyze the factors to threaten intelligent vehicle, which are usually intruded through communication network system and the security solution using biometric authentication scheme.

We have successfully included the establishment of secure channels, the detection of spoofing user identity, tampering, information disclosure, elevation of privilege, mutual inner vehicle devices authentication and secure distribution of provisional biometric information authentication scheme.

REFERENCES

[1] Sun Hyung Baek, Jung-Guk Kim, Sang Hyun Park, HyunTae Ju, "A Development of Trip computer based on Android", Korean Institute of Information Scientists and Engineers, Autumn Conference, Vol.37, No2, pp.397~400, 2010

[2] http://maj3sty.tistory.com/1015

[3] Byung-Seok Yu, Sung-Hyun Yun, "The Design and Implementation of Messenger Authentication Protocol to Prevent Smartphone Phishing", Journal of the Korea Convergence Society, Vol.1, No.1, pp. 9~14, 2010

[4] Won-Jun Jang, Hyung-Woo Lee, "Biometric One-Time Password Generation Mechanism and its Application on SIP Authentication", Journal of the Korea Convergence Society, Vol.1, No.1, pp. 93~100, 2010

[5] Seung-Soo Shin, Kun-Hee Han, "Design of the Mail Protocol with Perfect Forward Security", Journal of the Korea Convergence Society, Vol.2, No.2, pp. 13~19, 2011

[6] Gongjun Yan ; Ding Wen ; Olariu, S. ; Weigle, M.C, "Security challenges in vehicular cloud computing", IEEE Transactions on Intelligent Transportation Systems, Vol.14, No.1, pp. 284~294, 2013

[7] Fed. Fin. Inst. Examination Council, Authentication in an Internet banking environment 2009. [Online]. Available: http://www.ffiec.gov/pdf/authentication_guidance.pdf

[8] L. Li, J. Song, F.-Y. Wang, W. Niehsen, and N. Zheng, "IVS 05: New developments and research trends for intelligent vehicles," IEEE Intell. Syst., Vol.20, No.4, pp. 10~14, 2005

[9] Keun-Ho Lee, "Analysis of Threats Factor in IT Convergence Security", Journal of the Korea Convergence Society, Vol.1, No.1, pp. 49~55, 2010

[10] Seung-Hwan Kim, Keun-Ho Lee, "User Authentication Risk and Countermeasure in Intelligent Vehicles", Journal of the Korea Convergence Society, Vol.3, No.1, pp. 7~11, 2012

[11] Keun-Ho Lee, "A Security Threats in Wireless Charger Systems in M2M", Journal of the Korea Convergence Society, Vol.4, No.1, pp. 1~5, 2013

이 근 호(Lee, Keun Ho)

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수
- 관심분야 : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호, ISMS(정보보호관리체계), 정보보호사전점검
- E-Mail : root1004@bu.ac.kr