Journal of Convergence for Information Technology
Vol. 9. No. 9, pp. 13-19, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.9.013

Security Credential Management & Pilot Policy of U.S. Government in Intelligent Transport Environment

Jin-Keun Hong
Professor, Division of Information Communication Technology, Baekseok University

지능형 교통 환경에서 미국정부의 보안인증관리 & Pilot 정책

홍진근
백석대학교 ICT학부 교수

Abstract This paper analyzed the SCMS and pilot policy, which is pursued by the U.S. government in connected vehicles. SCMS ensures authentication, integrity, privacy and interoperability. The SCMS Support Committee of U.S. government has established the National Unit SCMS and is responsible for system-wide control. Of course, it introduces security policy, procedures and training programs making. In this paper, the need for SCMS to be applied to C-ITS was discussed. The structure of the SCMS was analyzed and the U.S. government's filot policy for connected vehicles was discussed. The discussion of the need for SCMS highlighted the importance of the role and responsibilities of SCMS between vehicles and vehicles. The security certificate management system looked at the structure and analyzed the type of certificate used in the vehicle or road side unit (RSU). The functions and characteristics of the certificates were reviewed. In addition, the functions of basic safety messages were analyzed with consideration of the detection and warning functions of abnormal behavior in SCMS. Finally, the status of the pilot project for connected vehicles currently being pursued by the U.S. government was analyzed. In addition to the environment used for the test, the relevant messages were also discussed. We also looked at some of the issues that arise in the course of the pilot project.

Key Words : SCMS, RSU, Vehicular, Connected, Security

요 약 본 논문은 미국 정부가 추진하고 있는 커넥티드 차량에서 SCMS와 파일롯 정책에 대해 분석하였다. SCMS는 인증, 무결성, 프라이버시, 그리고 상호운용성을 보장한다. 미국의 SCMS 지원위원회는 국가단위의 SCMS를 설립하고 시스템 전반에 대한 통제 역할을 수행하고 있다. 물론 보안 정책 수립 그리고 절차와 훈련 프로그램을 도입한다. 본 논문에서는 C-ITS에 적용하는 SCMS의 필요성에 대해 논의하였다. 그리고 SCMS의 구조에 대해 분석하였고 미국 정부의 커넥티드 차량의 파일롯 정책에 대해 고찰하였다. SCMS의 필요성에 대한 논의에서 차량과 차량 사이에 SCMS의 역할과 책임성이 중요하다는 사실을 강조하였다. 보안 인증 관리시스템에서는 구조를 살펴보았는데 차량이나 RSU에 사용되는 인증서의 유형에 대해 분석하였다. 인증서에 따른 기능과 특성을 분석하였다. 또한 SCMS가 가지는 비정상 행위에 대한 탐지와 경고 기능에 대한 고찰과 함께 기본 안전성 메시지의 기능에 대해서 분석하였다. 마지막으로 현재 미국 정부가 추진하고 있는 커넥티드 차량의 파일롯 프로젝트의 현황을 분석하였다. 테스트에 사용되는 환경과 함께 관련 메시지에 대해서도 분석하였다. 파일롯 프로젝트를 추진함에 있어서 발생하는 논의점에 대해서도 살펴보았다.

주제어 : 보안인증관리시스템, 로드사이드유니트, 차량, 커넥티드, 보안

*This paper is sponsored of project funding of NSR.
*Corresponding Author : Jin-Keun Hong(jkhong@bu.ac.kr)
Received August 7, 2019
Revised September 9, 2019
Accepted September 20, 2019
Published September 28, 2019

1. Introduction

Future societies will see universal expansion of connectivity and services for self-driving cars. The concept of connected self-driving cars is a combination of autonomous driving and connected vehicles. Of course, this connected self-driving vehicle will be used in smart cities. The smart city is a city where the Internet of Things, machine running, big data, and shared economy concepts and related technologies are combined to serve. In this type of smart city, connectivity and self-driving vehicle services will provide benefits such as improved safety, reduced congestion, reduced use and emissions of fossil fuels, reduced transportation costs and improved accessibility and mobility. The U.S. government's smart city projects include California, Oregon, Minnesota, Washington, Nebraska, Indiana, Iowa, Wisconsin, Michigan, Ohio, Pennsylvania, New York, Massachusetts, Kennedy, Rhode Island, New Jersey, Washington District of Columbia (D.C.), Maryland, North Carolina, South Carolina, Kentucky, Georgia, Florida, Alabama, and Texas. However, the U.S. government's smart city project centers on connected vehicle environment, smart road lights, pedestrian impact hedging system, integrated data exchange, joint payment system, multi-modal travel planning, smart mobility hub, mobility support, connected electric self-driving vehicle, delivery zone availability, improved parking, event parking management, vehicle routing, and truck parking availability. Currently, research on connected vehicles has been carried out actively. Connected vehicles transmit basic safety messages more than 10 times per second by wireless devices in the vehicle. This information is received by nearby vehicles and RSU. The driver will obtain a warning about a possible collision from this information. Therefore, connected vehicles will be able to escape unintended collisions with the help of this information. The connected vehicle will therefore warn the driver of the vehicle entering the intersection and of its unsafe hazards. It will also advise drivers to warn and slow down by providing information on traffic jams ahead.

2. Related Research

Ruijie Li et. al reviews about cooperative system in free space optical communication for simultaneous multiuser transmission [1]. It is analyzed the behavior of ergodic data rate and enhanced the performance of users in cooperative communication. Priyanka Karkhanis et. al presents about C-ITS reference architecture [2]. C-ITS is demonstrated by C-Mobile project from 2017 to 2020. In case of C-Mobile project is deployed and demonstrated in Europe sites. However C-Mobile based on C-ITS architecture is compatible with ISO/IEC/IEEE 42010 standard architecture. Pierpaolo Cincilla et. al presents about security of C-ITS messages [3]. In the C-ITS system, it is guaranteed communication security in heterogeneous environment. Safety of ITS is relevant to source authentication. Pierpaolo Cincilla et. al. is demonstrated of C-ITS security management infrastructure. Wei Tang et. al reviews about cooperative driving hardware simulation platform for cooperative ITS [4]. In the Micro IV platform, it is supported of improved positioning accuracy for V2V and V2I cooperation environment. Elena Cinque et. al presents about adaptive strategy to mitigate in the European Telecommunications Standard Institute (ETSI) Decentralized Congestion Control (DCC) [5].

In the ETSI, it is standardized for cooperative awareness messages and considered about decentralized congestion control method. Zhang Kailong et. al presents about simulator for service oriented cooperative ITS [6]. The designed C-ITS simulator is implemented for service oriented C-ITS which is included in adaptive enhancement and reconfigurable architecture. Robert D. Mushrall et. al presents about SCMS for vehicular communication [7]. SCMS is developed by US government as PKI and privacy protection of vehicular. SCMS is required of development planning about efficient distributed

certificate revocation lists and key expansion. In the EmuLab, it is demonstrated of how to work and test pseudonym certificates in SCMS. Also it is deployed of pilot program. Matthew D. et. al presents about threat analysis of SCMS in vehicular communication [8]. Matthew D. et. al are worked about six categories of STRIDE threat classification model as vehicular PKI in vehicular network. Malalatiana Randriamasy et. al reviews about formally validated of novel tolling service with the ITS G5 [9]. ITS-G5 technology is specified by ETSI. Malalatiana et. al are designed by efficient architecture for guarantee of security exchange by back office of tolling server. Safety and efficiency of this scheme is validated and verified from Automated Validation of Internet Security Protocols and Application (AVISPA) security protocol verifier tool. Marcos A. Simplicio et. al reviews about efficient security credential management system for vehicular communication [10]. SCMS support benefits of butterfly key expansion process. Chang Wu Chen et. al presents issue of protecting vehicular networks privacy in the presence of a single adversarial authority [11]. The SCMS is designed to assure privacy against a singer insider compromise and prevent privacy information leakage. Santos Jha et. al presents about pseudonym certificates validations and propose to trust framework which insures authenticity, integrity, unlinkability [12]. Santos et. al suggests SCMS with cross certification. Marcos Antonio Simplicio Junior et. al presents about privacy preserving method for temporarily linking/revoking pseudonym certificates and describes design to solve security degradation of computational overhead [13]. Raju Barskar et. al presents key management in vehicular ad hoc network [14]. For authentication in vehicular network and system, several group key management is suggested and developed. Hengyi Liang et. al presents about security vulnerabilities in connected vehicle applications and considers mechanism of network and system levels [15]. The topic of interest in this paper is the application of pilot projects (in many cities of U.S.) of connected vehicles being pursued by the U.S. government. For this paper, the U.S. government finished developing the first phase of concept (12 months) completed in September 2016 and proceeded with the second phase of design, build and test phase (20 months). The company is carrying out a three-stage pilot maintenance and operation phase (18 months). Finally, we will proceed with the post-pilot operation. In the C-ITS environment, security qualification is a messaging security measure, that applies to vehicles and vehicles, vehicles and infrastructure communications. PKI-based certificate management and cryptographic methods should be provided for this measure to provide safe effects. Certified participants have mechanisms to communicate and authenticate messages with the vehicle or infrastructure through digital certificates. Of course, it also has the ability to identify and remove non-legal devices or to protect. When SCMS is applied, SCMS has the advantages of authentication, integrity, privacy, and interoperability. The Commission that supports SCMS serves as a support for SCMS operations, technical management, and detecting misbehavior, implementing functions, and developing national-level SCMS. SCMS is paramount in ensuring message security and privacy. The device will interoperate and test local certificate management software for quality assurance. The SCMS Support Committee of the United States will establish national-level SCMS and play a role in controlling it. Policies, procedures and training programs will be introduced here. In this paper, we analyzed at the need for security qualification of C-ITS in Chapter 2. Chapter 3 and 4 are considered at the structure of security qualification management and analyzed the filot policy of connected vehicles of the U.S. government. It is concluded in Chapter 5.

3. Security Credential Necessity in C-ITS

It is issued that why, then, is it necessary to apply

SCMS to connected vehicles. In fact, SCMS is a very important system in the connected vehicle environment. Vehicles based on C-ITS shall be vehicle-friendly. The vehicle shall exchange and analyze data in real time. This work must be done in a very short time. The messages sent and received are those that are sent to warn of or warn of the driving situation. Therefore, the processing of this information is very important. Especially in safety. The vehicle collaboration system shall, in the case of the driver, transmit warning information between the vehicle and the vehicle with minimal control of the vehicle device.

Table 1. Characteristics of SCMS and V2V

Category	Characteristics
Vehicle to vehicle	-Exchange and analysis of data -Alert in driving condition -Control of message in vehicle equipment
SCMS	-Support of reliable and safety condition of vehicle -Exchange and enroll digital cert. -Generation and management of Cert of V2I and V2V.

On the security side, it is very important to generate warning messages from connected vehicle devices and to create a reliable environment for these warning messages. However, this role is played by the Security Credentials Management System (SCMS) in Table 1 and Fig. 1.

Devices can trust users and exchange information safely based on digital certificates through SCMS. SCMS is closely related to the U.S. Department of Transportation (USDOT). So it is that how can SCMS do this. SCMS is basically a security solution that issues and manages security certificates for V2V and V2I communication environments. Therefore, the certificate proves that the vehicle device is a trusted object in the system. It also provides privacy. Connected vehicle devices are registered with the SCMS. And get a security certificate from certification authority (CA). This value is attached to the message as part of the digital signature. Of course, the CA's role is to generate, distribute, and revoke certificates for vehicles.

4. Architecture of Security Credential Management

4.1 Security Architecture

However, the U.S. Department of Transportation's SCMS proof of concept supports the application of the selected number of connected vehicles until December 2020. The approved device is identified as a trusted object from the vehicle system. The connection chain follows the PKI basic structure. The certificate type will distinguish between vehicle and RSU. For vehicles, the onboard type is divided into on board equipment (OBE) registration certificates, pseudonym certificates, and identity certificates [16]. A certificate of registration is a certificate used to request an pseudonym certificate and an identity certificate. It has the function of the OBE passport. When the OBE is running, it connects to the SCMS and requires a certificate of registration. An pseudonym certificate is a short-term certificate. A certificate used for basic safety message authentication and reporting on abnormal behavior. Multiple certificates can be used for a single terminal considering privacy. The identification (ID) certificate is used by OBE to approve the vehicle to infra (V2I) application. This certificate uses one valid ID certificate for one application. The RSU has a certificate of registration and an application certificate. A certificate of registration is used when requesting an application certificate. Perform the passport function of the RSU. When the RSU is run, it is connected to the SCMS and requested a registration certificate. Application certificates are used to sign messages related to signalling, timing, passenger information, etc. Therefore there is also a detection of abnormal behavior, and when such a situation occurs, the system will be notified. If an abnormal actor is judged to be a malicious act, the system revokes this actor's message authority. The SCMS architecture has the ability to authenticate and verify basic safety messages in Fig. 1. Of course, it also has the ability

to detect and block abnormal behavior. This safety message provides a warning about safety and context- sensitive information for the receiving vehicle device. However, incorrect or false information could have a detrimental effect on the safety of the vehicle system in this situation. Thus, within the SCMS architecture, the relevant functions are implemented to control the authority of an abnormal actor to act, as well as to collect information about unusual threatening behaviors that can be addressed from these problems. The device reports threat information or related information to the SCMS. If the SCMS receives this information and finds any threat activity from it, it will block the vehicle device. In this case, the vehicle device is managed by an untrusted device. In the SCMS implementation organization includes PKI security services, authentication services, OEMs, USDOT, and telecommunications service providers. SCMS user organizations include vehicle owners and operators, dealers and installers, service and parts facilities, CV equipment and application suppliers, original equipment manufacturers (OEMs), state and local Department of Transportations (DOTs), and public infrastructure system integrators. SCMS Other organizations include USDOT, universities, standardization bodies and advocacy groups.

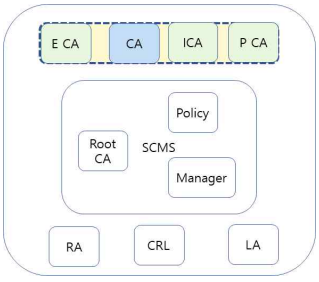

Fig. 1. Certification Architecture of SCMS

4.2 CV pilot policy of U. S.

In pilot test, messages applicable to connected vehicle technology include MAP messages, basic safety message (BSM) messages, signal phase and timing message (SPaT) messages and traveler information message (TIM) messages. The MAP message relates to the stop bar, lane and permitted movement in the intersection topography in which traffic light information is transmitted from the RSU to the vehicle. BSM messages are vehicle information that is transmitted between the vehicle and the vehicle, including location, speed and path history. Traffic sign control sends signal stage and timing information to the vehicle in the SPaT message. This information provides time information on whether green, yellow and red walking is allowed. It is primarily a service related to V2I safety. Pedestrian information is also communicated to the vehicle via a TIM message. This information includes speed limits and areas, construction areas and detours, curves and road conditions. It is primarily a service related to V2I safety. Of course, the U.S. government applies 802.11p technology to provide an application environment for transmitting this message, including the safety of connected vehicles. It also provides low-latency communication of less than 50 milliseconds and supports transfer speeds of 3-27 Mbps. The U.S. Department of Transportation designs security and privacy based on SCMS for connected vehicles. It is used to the authentication of messages signed by the authenticated source and applied to the message's password where necessary. 60 of security certificates are changed every week to respond to the trace, and the ID is changed every 5 minutes of 2Km (MAC address, Temp, ID, message counter value). It also detects abnormal actors and distributes certificate revocation lists (for malicious actors or compromised devices). For safety devices in after-market, the U.S. government is planning a pilot project consisting of security management systems, CV support systems, traffic control systems, smartphone or personal dedicated short range communication (DSRC) applications, ASD safety devices, bus or transit automatic synchronized discriminator (ASD) systems, commercial vehicle

warning devices ASD, CV RSU, and traffic call controllers. However, there are limitations to the implementation of these pilot projects. It is measured to increase the accuracy of location information, which should be presented and the issue of personal privacy exposure, which should also be resolved. Therefore, limited data collection policies for information without personal information should be required, and encryption and log destruction should be designed to occur automatically. In addition, obfuscation, normalization and aggregation procedures are required. In U.S. government, another problem is the threshold of the backhaul network. It is such that how do we address the cost of using all devices to connect and operate wirelessly. The concept of edge computing is being introduced as a way to solve this problem. This is the concept of converting data into information in the RSU. It is also the principle of collecting only limited data. And it's the use of operational management data to manage the state of operations. Also security is considered. Since the connected vehicle environment requires a trust-based environment, appropriate security solutions are required and reflected in the policy. This is to strengthen the communication security module between the RSU and the traffic communication module controller. It also strengthens security at the traffic control module control system, login and physical access level. Security is also enhanced for all external systems and links. It also upgrades security software to previous traffic controllers. It is also considered in terms of the availability of cell phones, a policy for PED applications. Blind people need applications that distribute PED navigation databases to provide SPaT messages and maps. The new mobile environment requires management of traffic controllers and management of systems. Software updates and development are needed for the applications that support them. When applying the SCMS model, the U.S. government envisions an SCMS model that allows security to be applied to all types of communications that support v2x systems. This highlights the need for governance models or models that can ensure ongoing operations. when it is considered these models, measure schemes should be taken to address availability or inconsistent services. In addition, limitations in implementing security policies or processes can affect interoperability, reliability, and security vulnerabilities.

Thus, SCMS expansion is an important factor in identifying potential strategies and assessing their feasibility in developing guidelines or strategies. In this respect, the SCMS extension relates to the review of the trust model, ownership, and governance model between V2Xs. It is also related to improving the ownership or governance model or establishing an execution model.

5. Conclusion

In this paper, we analyzed the SCMS and pilot policy, which is pursued by the U.S. government in connected vehicles. SCMS ensures authentication, integrity, privacy and interoperability. The SCMS Support Committee of U.S. government has established the National Unit SCMS and is responsible for system-wide control. Of course, it introduces security policy, procedures and training programs making. The status of the pilot project for connected vehicles currently being pursued by the U.S. government was analyzed. In addition to the environment used for the test, the relevant messages were also discussed. Future research projects will be analyzed on security service cases of self-driving & C-ITS services of EU. Related research of test beds and security certification systems in U. S. DOT. are considered to apply to related studies in South Korea.

REFERENCES

[1] H. Yasa (2018). Experiment Exposed Credentials in GitHub Public Repositories for CI/CD. *IEEE SecDev2018*. (pp.123).
DOI : 10.1109/ SecDev.2018.00039

[2] R. Li, J. Zhang & A. Dang. (2018). Cooperative system in free space optical communication for simultaneous multiuser transmission. *IEEE Communication Letters, 22(10),* 2036-2039.
DOI : 10.1109/LCOMM. 2018. 2865734.

[3] P. Karkhanis, G. Mark, J. Van den Brand & S. Rajkamikar. (2018). Defining the C-ITS reference anrchitecture. *IEEE International conference on software architecture companion(ICSA-C)2018*.
DOI : 10.1109/ICSA-C. 2018.00044.

[4] P. Cincilla, A. Kaiser, B. Lonc, H. Labiod, R. Blancher, C. Jouvray, R. Denis & A. Boulanger. (2015). Security of C-ITS messages: A practical solutions the ISE project demonstrator. *7th International conference on New Technologies, Mobility and Security (NTMS)2015*. DOI : 10.1109/NTMS.2015.7266520.

[5] W. Tang, M. Yang, Z. Lv, Q. Qian, T. Su, B. Wang & C. Wang. (2018). MicroIV: A Cooperative driving hardware simulation platform for cooperative ITS. *IEEE Transactions on Vehicular Technology, 67(10),* 9173-9182.
DOI : 10.1109/TVT. 2018. 2862416

[6] E. Cinque, F. Valentini, A. Lovine & M. Pratesi. (2017). An adaptive strategy to mitigate instability in the ETSI DCC: Experimental validation. *15th ITSI2017*.
DOI : 10.1109/ ITST.2017.7972223.

[7] Z. Kailong, W. Min, S. Hang, Y. Ansheng, A. de La Fortelle & M. Kejian. (2017). QoS-ITS: A simulator for servie oriented cooperative ITS of intelligent vehicles. *IEEE/ACIS 16th ICIS2017*.
DOI : 10.1109/ICIS. 2017.7960093.

[8] R. D. Mushrall, M. D. Furtado & H. Liu. (2018). EmuLab of security credential management system (SCMS) for vehicular communications. *IEEE 88th Vehicular Technology Conference (VTC-Fall) 2018*. DOI : 10.1109/VTCFall. 2018.8690778.

[9] M. D. Furthado, R. D. Mushrall & H. Liu. (2018). Threat analysis of the security credential management system for vehicular communication. *IEEE HST2018*.
DOI : 10.1109/ THS.2018.8574206.

[10] M. Randriamasy, A. Carbani, H. Chafouk & G. Fremont. (2019). Formally validated of novel tolling service with the ITS G5. *IEEE Access*, 7, 41133-41144.
DOI : 10. 1109/ACCESS.2019.2906046

[11] M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini, M. Vinicius & M. Silva. (2018). The unified butterfly effect: efficient security credential management system for vehicular communications. *IEEE VNC2018*.
DOI : 10.1109/ VNC.2018.8628369.

[12] C. W. Chen, S. Y. Chang, Y. C. Hu & Y. W. Chen. (2017). Protecting vehicular networks privacy in the presence of a single adversarial authority. *IEEE CNS2017*.
DOI : 10.1109 /CNS.2017.8228648.

[13] S. Jha, C. Yavvari & D. Wijesekera. (2018). Pseudonym certificate validations under heavy vehicular traffic loads. *IEEE VNC2018*.
DOI : 10.1109/VNC.2018.8628399

[14] M. A. S. Junior, E. L. Cominetti, H. K. Patil, J. Ricardini, L. Ferraz & M. V. Silva. (2018). Privacy preserving method for temporarily linking/revoking pseudonym certificates in VANETs. *17th IEEE TrustCom/BigDataSE2018*.

[15] R. Barskar, M. Ahirwar & R. Vishwakarma. (2016). Secure key management in vehicular ad hoc network: A review. *SCOPES 2016*.
DOI : 10.1109/SCOPES.2016.7955730.

[16] H. Liang, M. Jagielski, B. Zheng, C. W. Lin, E. Kang, S. Shiraishi, C. N. Rotaru & Q. Zhu. (2018). Network and System Level Security in Connected Vehicle Applications. *IEEE/ACM ICCAD2018*.
DOI : 10.1145/3240765.3243488.

[17] M. A. Simplicio Jr., E. L. Cominetti, H. K. Patil, J. E. Ricardini, M. Vinicius & M. Silva. (2018). ACPC: Efficient revocation of pseudonym certificates using activation codes. *Journal of ScienceDirect ELESEVIER, 90,* 2019.
DOI : 10.1016/j. adhoc.2018.07.007.

홍 진 근(Jin-Keun Hong) [정회원]

- 1991년 2월 : 경북대학교 전자공학과 공학사
- 1994년 2월 : 경북대학교 정보통신공학 전공 공학석사
- 2000년 2월 : 경북대학교 정보통신공학 전공 공학박사
- 2019년 현재 : 백석대학교 ICT학부 교수

· 관심분야 : 융합 보안
· E-Mail : jkhong@bu.ac..kr