Journal of the Korea Convergence Society
Vol. 8. No. 10, pp.29-35, 2017 https://doi.org/10.15207/JKCS.2017.8.10.029

Pseudonym Management in Autonomous Driving Environment

Hong Jin Keun[1*]
[1]Division of Information and Communication, Baekseok University, South Korea

자율주행환경에서 가명성 관리

홍진근[1*]
[1]백석대학교 정보통신학부

Abstract In this paper, we describe certificate policy and characteristics in cooperation condition with Cooperative intelligent transport system and autonomous driving vehicle. Among the authentication functions of the vehicle, there is a pseudonym authentication function. This pseudonymity is provided for the purpose of protecting the privacy of information that identifies the vehicle driver, passenger or vehicle. Therefore, the purpose of the pseudonym certificate is to be used for reporting on BSM authentication or misbehavior. However, this pseudonym certificate is used in the OBE of the vehicle and does not have a cryptographic key. In this paper, we consider a method for managing a pseudonym authentication function, which is a key feature of the pseudonym certificate, such as location privacy protection, pseudonym function, disposition of linkage value or CRL, request shuffling processing by registry, butterfly key processing, The authentication policy and its characteristics are examined in detail. In connection with the management of pseudonymes of the vehicle, the attacker must record the BSM transmission and trace the driver or vehicle. In this respect, the results of this study are contributing.

• Key Words : Vehicle, Security, Driving, Certificate, Attack

요 약 본 논문에서는 협업 지능형교통시스템과 연동되는 자율주행 차량과 연동되는 환경에서 인증서 정책과 특성에 대해 살펴보았다. 차량의 인증 기능가운데는 가명 인증기능이 있다. 이 가명성은 차량 운전자, 승객이나 차량을 식별하는 정보에 대한 프라이버시를 보호할 목적으로 제공된다. 그러므로 가명인증서의 사용 목적은 BSM 인증이나 오 동작에 대한 리포팅을 위해 사용한다. 그런데 이 가명 인증서는 차량의 OBE에서 사용되며 암호 키는 없는 것이 특징이다. 본 논문에서는 이 가명인증서의 주요 기능인 위치 개인정보 보호나 가명기능, 그리고 링키지 값이나 CRL의 폐기 처리, 등록 기관에서 요청 셔플링 처리, 버터플라이 키 처리 등을 살펴보면서, 동시에 가명인증 기능 관리를 위한 제반 인증정책과 그 특성들을 세부적으로 고찰하였다. 차량의 가명관리와 관련하여 공격자는 BSM 전송을 기록하여 운전자나 차량의 추적할 수 있으므로 이에 대한 대책으로 연결 해제 기능을 부여해야 한다. 이러 측면에서 본 연구의 결과는 기여하고 있다고 할 수 있다.

• 주제어 : 차량, 보안, 드라이빙, 인증서, 공격

Corresponding Author : 홍진근(jkhong@bu.ac.kr)
Received August 29, 2017 Revised September 24, 2017
Accepted October 20, 2017 Published October 28, 2017

1. Introduction

Recently, under the background of the purpose of providing efficient vehicle driving service, collaborative intelligent traffic system technology and autonomous vehicle technology have been developed in cooperation with each other. However, intelligent vehicle transport systems that support this connectivity and are automated and collaborative must meet the key elements of safety (ISO 26262), security and privacy (SAE J3061), interoperability, and performance requirements to provide the core services. In NHTSA, autonomous driving technology is classified into four stages, and it is expected that fully autonomous driving service will be achieved by 2025. This fully autonomous driving means that all the items of the driving environment, the driving environment, and dynamic driving job monitoring are determined and processed by the vehicle system. Collaboration intelligent traffic system technology is linked to several technologies (DSRC + WAVE + 4G / 5G + WiFi). In this internetworked environment, vehicle status information is collected and a dynamic map database is constructed. In addition, it aims to provide safe and efficient information to drivers and traffic control centers by providing vehicle information and peripheral information through communication channels between vehicles, vehicles, vehicles and infrastructure based on location information collecting device and open platform. However, security management technology must be a foundation for efficient service of autonomous navigation technology and collaborative intelligent transportation system[1,2,3,4,5]. In this paper, we discuss pseudonymity management as one of the key elements of security management technology. We focused on the characteristics of certificate authority and certification cycle for pseudonymity management. In the Security Certificate Management System (SCMS), it is used to protect the privacy problem of the driver or vehicle identification information from the vehicle tracking, and it is essential to lower the traceability. To do so, it is necessary for the vehicle to frequently change the unique identification information in response to the attacker tracking the vehicle[6,7,8,9,10]. Therefore, we want to emphasize the need for this study of pseudonymity management. In order to provide pseudonymity in the management of pseudonymity, all application IDs of vehicles must be changed frequently. This is the background for supporting the temporary ID field of the BSM delivered from the vehicle. Also, in the case of network identifiers, information such as MAC address should be changed frequently. Information that encrypts the vehicle's own information should also be changed frequently. The composition of this paper first discusses the view of related research in Chapter 2. In Chapter 3. we discuss pseudonym management in vehicle environment. In Chapter 4, we will look at quality characteristic of convergence software. In Chapter 5 several conclusions are drawn.

2. Related Research

Badis Hammi et al. studied the specification of certificates defined by ETSI[11]. This research proposes a public key infrastructure for collaborative intelligent transportation systems. Researchers, of course, are proposing the definition of ASN.1 for ETSI certificates, unlike the IEEE1609.2 security standard. Pierpaolo Cincilla et al. focused on the extensibility of vehicle PKI certificates[12]. Their interest lies in the scalable application of public key infrastructure in collaborative intelligent transportation systems. Jan Durech et al. Have studied PKI structure safety in C-ITS environment[13]. Jan et al. Conducted a security analysis of public key structures based on elliptic curve digital signature algorithms in vehicular traffic systems[14]. Binod Vaidya et. al review multi domain public key infrastructure[15]. Their work is on lightweight public key infrastructures that use implicit certificates and are applicable to vehicles.

3. Pseudonym Management of Vehicle

3.1 Certificate Policy for Certificate Management

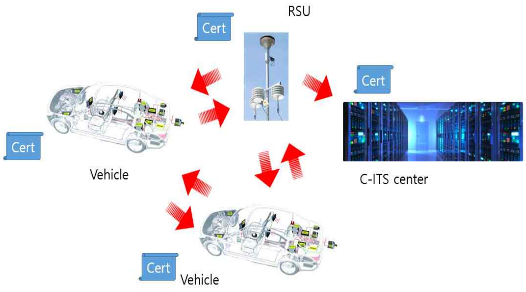
Vehicle certificate structure applied in USA is applied based on IEEE1609.2 standard and SCMS standard. This certificate has Root CA, Intermediate CA, PCA, RA, LA structure. Signed certificates include signer ID Singer_id, application permissions, geographical area, valid time, retract time, public key, and signature value of the originator. However, certificate policies provide multiple certificates for privacy protection when designing certificates. At this time, the certificate generates about 20 pieces per week, and all IDs are changed in the stack. Among the problems raised in signing is that the information is too heavy and slow when signing the group. Also, if the certificate goes to a specific device, there is a problem that CA can become a link. When issuing a certificate, a secure credential management system, SCMS, is required, which has a mechanism to protect privacy. This mechanism should be linked to the CAs to provide the ability for the vehicle to track vehicle terminals whose identity is malfunctioning without exposing them, and to block tracking after the certificate revocation.

Another problem is the quarantine issue, which should ensure that a particular vehicle can not be tracked due to insider or DB problems. The certificate shall contain the linkage value and the linking authority shall be associated with the registration authority (RA) and the malfunction detection authority (MA). Of course, a pseudonym institution (PCA) must also be connected to the RA or MA. When generating the linkage value, the pre-linkage value is generated by XOR processing, and the pre-linkage value is generated from the linkage seed through the hash. That is, the linkage value is obtained by XORing the pre-linkage value sequence obtained from the linkage seed 1 sequence and the pre-linkage value sequence obtained from the linkage seed 2 sequence. The ID certificate is applied between the vehicle and the infrastructure road side unit and is used in OBE of the vehicle. However, this ID certificate can use the encryption key determined by the butterfly key mechanism. This certificate can be used for a long time, and for OBE it is useful as a single certificate for a specific application. The butterfly key used is automatically generated and used by the RA in advance. The withdrawal of the identity certificate is done through the CRL. In a road side unit, the registration certificate is the identity of the road side unit itself. This certificate is provided to the road side unit during the bootstrap process, and the registration certificate has one or more PSIDs. If the registration certificate has more than one PSID, the app must be essentially similar. The registration certificate used at this time should be reset and does not include the entire operation life of the road side unit. When canceling a registration certificate, it should be handled based on the black list managed by the registry. The road side unit uses application certificates for authentication and encryption purposes. This certificate can only be used within the validity period, which is divided into a short validity period and a long validity period. The short validity period can be in days or hours and does not require a CRL. However, the long validity period can be a few years or a few months, and a CRL is required.

3.2 Characteristics of Certificate Authority

The root certification authority (CA) is located at the top of the trust domain. This certification authority is used to verify other certification authorities that exist below. However, in order for the root certification authority to authenticate its own trust problem, another approach is needed. In fact, the certificate of the root certification authority has a very long cycle. The integrity of the certificate of the root certification authority must establish other authentication methods, including encryption, such as hardware or software verification. Another certification authority is ICA, an intermediate certification body. The certificate of this

CA issues a certificate for use between the SCMS and the SCMS. The ICA may issue CRLs and may also have CRL rights to revoke them. The certificate of the registered certification authority (ECA) is a certificate used for the final entity including the onboard unit and the road side unit. The person having the certificate includes the response cipher key temporarily issued in the request message. The revocation of this certificate is handled through the CRL. Certificate revocation involves a certificate expiration schedule, which excludes short downtime. There is only one CRL certificate. Other certification bodies include PCAs. This certificate is used for end-end entities, including on-board units and road side units. The revocation of this certificate is handled through the CRL. The certificate for the CRL generator is issued by the root CA and is used to sign the CRL. The certificate for the policy generator is issued by the root CA and is used to sign the global policy configuration file. The policy for validity of the policy generator is the same as the policy defined in the certificate of the CRL generator. LA certificates are those of linkage agencies that do not interact with the end entity, and the cycle is short. The RA certificate must be long enough to allow the end entity to accept the certificate provisioning request after bootstrapping. The MA certificate needs to be long enough so that the end entity does not need to retrieve this certificate.



[Fig. 1] Certificate of Vehicle & C-ITS

3.3 Certificate Period

The following is a certificate cycle for provisioning and disposal.

- Provisioning phase

In the onboard unit, the registration certificate is granted one certificate to the end entity for each PSID category. At this time, the pseudonym certificate cycle of the onboard unit requires 20 certificates per week over three years. The ID certificate of the onboard unit needs one per cycle. However, the registration certificate of the road side unit requires one certificate for each end entity for each PSID category. The application certificate of the road side unit requires one certificate per cycle for the road side unit having connectivity. But the time period is short. Of course, road side units that do not have connectivity require one certificate per cycle. However, the time period is long. So what about the certificate cycle in the revocation phase?

- Discard phase

At this stage, the registration certificate of the onboard unit manages the blacklist. Of course, pseudonym certificates are linkage values. The identity certificate of the onboard unit adds the certificate digest of all issued certificates. What about the registration certificate of the road side unit? This certificate manages the RA blacklist. The application certificate of the connectable road side unit can not renew the certificate due to the RA blacklist of the registration certificate. What about the application certificate for a road side unit that has no connectivity? This adds a certificate digest of all issued certificates. On the other hand, which certificate is associated with the response encrypted by the pseudonym certificate authority. The pseudonym certificate relates to the onboard unit's pseudonym certificate, the onboard unit's identity certificate, and the application certificate of the road side unit, regardless of connectivity. The response is encrypted by the PCA. registry RA to Shuffle is associated with the onboard unit's pseudonym certificate. Of course, the CRL for an end-to-end device is related to the onboard unit's pseudonym certificate, the identity certificate, and the application certificate without the connectivity of the road side unit. Concurrent validation problems for a given PSID are related to the onboard unit's pseudonym certificate. The linkage value is also related to the pseudonym certificate of the onboard unit, and the butterfly key is associated with the onboard unit's pseudonym certificate or identity certificate.

Depending on the multi-time period, certificate issuance is related to the onboard unit's pseudonym certificate or identity certificate. Pseudonymity relates to the onboard unit's registry and pseudonym certificate. Reporting of misbehavior can be accomplished using the onboard unit's pseudonym certificate, the onboard unit's ID certificate, and regardless of connectivity, it is related to the application certificate of the road side unit. The cryptographic key is associated with an application that has connectivity to the road side unit.

- Certificate expiration cycle

So what happens to the expiration period of a PoC certificate? The certificate expiration date used to register the onboard unit is six years and will be updated thereafter. Of course, it is issued by ECA. The number of valid certificates is one and the certificate size is required to be about 87 bytes. What about the pseudonym certificate of the onboard unit? The pseudonym certificate is issued by the PCA, the one week is the expiration period, and the revocation period is 1 week + 1 hour. Of course, the number of valid certificates is 20 + 20. The size of the certificate is 86 bytes. The ID certificate of the onboard unit is issued by the PCA, and the period of use is 1 month and the withdrawal is 1 month + 1 hour. The certificate size is 89 bytes. Certificate enrollment is issued by the PCA and has a usage period of 6 years and has a size of 89 bytes. The application certificate of the road side unit is issued by the PCA. Of course, the use period of one week and one week + one hour is the discard period. It has a certificate size of 89 bytes. The issuing authority of the ECA certificate is ICA. The certificate is valid for three years and requires renewal three months in advance and the expiration period is eleven years. The certificate size is 150 bytes. The issuing authority of RA certificates is also ICA. You can use it for three years and ask for renewal three months in advance, and the disposal is three years plus one week. The size of the certificate is 217 bites. The LA issuance authority is ICA, the number of certificates is two, and the certificate validity institution is three years. You must request renewal three months in advance and the expiry is three years plus one week. It has a certificate size of 205 bytes. PCA certificates are issued by ICA, and the number of certificates is 4, which is valid for one year. You must request renewal three months in advance and the expiration period is four years. The OBE pseudonym value is generated by the PCA and has 20 + 20 valid certificate counts, requiring one week for renewal and one week + 1 hour for expiration. A certificate size of 86 bytes is required. The OBE ID is issued by the PCA and has a certificate size of 89 bytes and a certificate number of 1 + 1. It has an expiration time of 1 month and an expiration time of 1 month + 1 hour. The road side unit application certificate is issued by the PCA and has a certificate size of 89 bytes and has an expiration time of one week + one hour and a validity period of one week. The ICA is issued by the root CA, has 1 + 3 certificates, and is valid for 4 years. You must request renewal three months in advance and have an expiration period of 13 years. It has a certificate size of 195 bytes. The root CA authenticates itself and has three certificates. It has a validity period of 12 years and a retraction period of 12 years. It must be renewed three months in advance and has a certificate size of 166 bytes.

The CRL generator certificate is issued by the root CA and has a certificate size of 190 bytes. It has two certificate counts and has a certificate validity of four years. The renewal must be notified three months in advance and the withdrawal period is four years plus one week.

The policy generator certificate is generated by the root CA and has a certificate size of 172 bytes and two certificates. The renewal must be notified three months in advance of the four-year certificate validity period. Certificate revocation is 4 years + 1 week.

5. Conclusion

Pseudonymity is provided for the purpose of protecting the privacy of information that identifies the driver, passenger or vehicle of the vehicle. The purpose of the pseudonym certificate is to be used for reporting on BSM authentication or misbehavior. It is used in the OBE of the vehicle and has no encryption key. The analysis of this study is a useful study focusing on certification authority and certification cycle related to the management of pseudonymity applied to vehicle PKI.

ACKNOWLEDGMENTS

This research paper is made possible through the project funding of Industry Academia Cooperation Group in Baekseok University.

REFERENCES

[1] Vrizylynn L. L. Thing, Jiaxi Wu, “Autonomous Vehicle Security : A Taxonomy of attacks and Defences,” GreenCom & CPSCom— SmartData2016, pp.164-170, 2016.

[2] Michael Jaynes, Ram Dantu, Roland Varriale, Nathaniel Evans, “Automating ECU Idenfitication for Vehicle Security,” ICMLA2016, pp.632-635, 2016.

[3] Xiaoyu Lan, Liangtian Wan, Guangjie Han, Lei Shu, “A Fast modified DOA estimation algorithm with rotation array for vehicle security in intellignet transportation system,” UIC-ATC-ScalCom2015, pp.484-489.

[4] Leonar Petnga, Huan Xu, “Security of unmanned aerial vehicles:dynamic state estimation under cyber physical attacks,” ICUAS2016, pp.811-819, 2016.

[5] Jan Lastinec, Ladislav Hudec, “Comparative analysis of TCP/IP security protocols for use in vehicle communication,” ICCC2016, pp.429-433.

[6] K. A. Mamun, Z. Ashraf, “Anti theft vehicle security system with preventive action,” APWC on CSE 2015, pp.1-6, 2015.

[7] Chandra Shekar Ramaiah, S. Zahid Hussain, S. Asif Hussain, Yahya Al Balushi, “Smart vehicle security system for defending against collabrative attacks by malware,” ICBDSC2016, pp.1-5, 2016.

[8] Pravin Selukoto Paupiah, “Vehicle security and forensics in Mauritius and abroad,” ICCCS2015, pp.1-5, 2015.

[9] Pritpal Singh, Tanjot Sethi, Bunil Kumar Balabantaray, Bibhuti Bhushan Biswal, “Advance vehicle security system,” ICIIECS2015, pp.1-6, 2015.

[10] Zachary Birnbaum, Andrey Dolgikh, Victor Skormin, Edward O’Brein, Daniel Muller, Christian Stracquodaine, “Unmanned Aerial Vehicle security using behavioral profiling,” ICUAS2015, pp.1310-1319, 2015.

[11] Badis Hammi, Jean Philippe Monteuuis, Eduardo Salles Daniel, Houda Labiod, “ASN.1 Specification for ETSI Certificates and Encoding Performance Study,” MMD2017, pp.291-298, DOI: 10.1109/MDM.2017.47, 2017.

[12] Pierpaolo Cincilla, Omar Hicham, Benoit Charles, “Vehicular PKI scalability consistency trad offs in large scale distributed scenarios,” VNC2016, pp.1-6, DOI: 10.1109/VNC.2016. 7835970, 2016.

[13] Jan Durech, Maria Franekova, Peter Luley, Emilia Bubenikova, “Safety aspects of PKI architecture within C-ITS and their modelling,” ELECTRO2016, pp.400-405, DOI:10.1109/ELECTRO.2016.751210, 2016.

[14] Brigitte Lonc, Pierpaolo Cincilla, “Cooperative ITS security framework: standard and implementations progress in Europe,” WoWMoM2016, 1-6, DOI:

10.1109/WoWMoM. 2016.7523576, 2016.

[15] Binod Vaidya, Dimitrios Makrakis, Hussein T. Mouftah, "Multi-domain Public Key infrastructure for vehicle to grid net work," MILCOM2015, pp.1572-1577, DOI: 10.1109/MILCOM.2015.7357669. 2015.

저자소개

홍 진 근(Jin-Keun Hong) [정회원]

- 1991년 2월 : 경북대학교 전자공학과 (공학사)
- 2000년 2월 : 경북대학교 일반대학원 전자공학과 (공학박사)
- 2004년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야> : 융합보안, 융합교육, 융합기술