중소기업융합학회 논문지 제4권 제1호 pp. 41-45, 2014

이모빌라이저 시스템에서 스마트폰을 이용한 인증 프로토콜

신미예*, 정윤수**, 배우식***, 이상호*
충북대학교*, 목원대학교**, 아주대학교, 충북대학교***

APSI : A user Authentication Protocol using Smart phone in Immobilizer System

Miyea Shin*, Yoonsu Jeong, Woosik Bae***, Sangho Lee***
Chungbuk National University*
Mokwon University**
Ajou Motor College***

요 약 이모빌라이저 시스템은 자동차 키에 저장된 코드와 자동차 엔진 ECU에 저장된 암호코드가 일치하는 경우에만 자동차 시동이 걸리는 차량 도난방지 시스템이다. 이모빌라이저 시스템 자동차의 키 분실 및 차량이 도난당했을 경우 이에 대응하기 위해 스마트 폰 등을 이용 KDC와 KMC를 통하여 사용자 인증을 마친 후 새로운 비밀 번호를 부여받는 모델을 제안한다.

주제어 : 이모빌라이저 시스템, 상호인증, ECU, KDC, Smart Phone

Abstract Only if the secret key stored in the engine ECU matches car key stored in the car, immobilizer system is a car anti-theft system that automobile engine takes. To take an action as soon in case of losing car key or being stolen, the ASPI protocol is proposed for assigning a new password after finishing user authentication by the smart phone etc.
The shortcoming point of that directly bring the car to a service center in case of losing key can be complemented by the proposed protocol. In case of the car and key both are theft together, the car can be stopped soon.

Key Words : Immobilizer system, mutual Authentication, ECU, KDC, Smart Phone

1. Introduction

Immobilizer is a system that the car engine starts up by transmitting driving information of injector and fuel pump to the ECU of engine, if and only the secret key that is sent from car key is matched[1].

In this paper, when the stolen car with car keys and key lost, in order to cope with this, a protocol is proposed for assigning a new secret key after finishing the user authentication.

if the car key is lost, the user has to bring the car to a service center directly for assigning a new key and that shortcoming can be complemented by the proposed

논문접수일 : 2014년 2월 1일 심사완료일 : 2014년 2월 15일 논문게재일 : 2014년 3월 31일
*교신저자 : 신미예(myshiny@cbnu.ac.kr)

protocol as well as the car can be stopped right away in case of car theft.

The configuration of this paper is as follow. The features of car remote controller and operation principle of the immobilizer system is described in section 2 and section 3 consists of proposed ASPI protocol. The security of the proposed protocol is analysis in the section 4 finally the conclusion and the direction for future developments are in the section 5.

2. Related research

In this section, characteristics of the remote control of the car and operation principle of the immobilizer system are described.

2.1 Characteristics of the remote control of the car

Remote control of cars that used for starting the engine and automatic alarm of the car has been providing convenience such as gate control, window control of the vehicle.

It is easy to implement the devices for wireless operation and those devices are developing in FM method, even the FM method is expensive than AM method [1].

2.2 Operation principles of immobilizer system

The secret key is stored in the internal transponder in immobilizer system. When the control unit of immobilizer system request, the transponder transmits the secret key.

Transponder inside the car key stores the private key that is stored in the production line of the automobile in the immobilizer system.

If a secret key that is stored in the engine ECU and the private key of the car is transmitted from the transponder matches, drive control information of the fuel pump and injector is transmitted to the ECU, the car start the engine[2-6].

2.3 User authentication

In essence, identification is the means by which a user provided a claimed identity to the system. User authentication is the means of establishing the validity of the claim. Mutual authentication protocols enable communicating parties to satisfy themselves mutually about each other's identity and to exchange session keys. Remote user authentication uses asymmetric encryption. A user request public-key certificate to Key Distribution Center(KDC). A Nonce used to assure that a session key Ks is fresh[7].

3. APSI protocol

This section describe about communication scenario that a new password can be assign after finishing user authentication by smart phone in order to respond fast in case of car and car key both are theft together. However a car key can be bought from the maintenance center and it is assumed that ECU is possible to be used with the chip that stored in transponder.

3.1 communication scenario

Figure1. is an ASPI protocol model. When it occurs on issues such as theft of the car or loss of the car key this protocol can authenticate a car owner using a car engine no, etc. This model supposes car key and ECU can update its secret key.

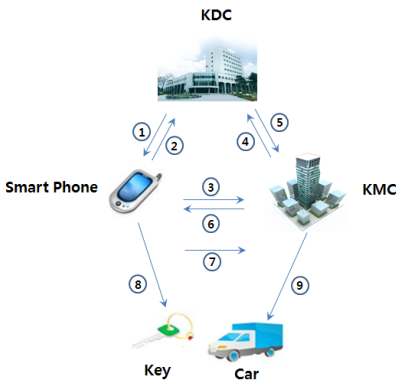

Figure 1. ASPI Protocol

① The vehicle owner requests authentication related to KDC(Key Distribution Center) and KMC(Key Management Center).
② KDC transmits the authentication that related to KMC to the owner.
③ The owner send those information such as engine number, etc. that receive from KDC to KMC.
④ The KMC request the owner's authentication from KDC.
⑤ The KDC sends the owner's authentication to the KMC.
⑥ The KMC sends the session key to the owner and then session is established.
⑦ A retrieves the session key Ks, uses it to encrypt NKMC, and returns it to KMC.
⑧ A saves a new secret key in the car key
⑨ The KMC sends a new secret key to ECU

3.2 Communication protocol

I. A → KDC : IDA || IDKMC
ii. KDC → A : E(PRauth, [IDKMC || PUKMC])
iii. A → KMC : IDA || E(PUKMC, [CAREngNo || Na])
iv. KMC → KDC : IDA || IDKMC || E(PUauth, Na)
v. KDC → KMC : E(PRauth, [IDA || PUA) || E(PUKMC, Na) || E(PUKMC, E(PRauth, [Na||KS || IDA || IDKMC]))
vi. KMC → A : E(PUa, (E(PRauth, [CAREnfNo || Na || KS || IDA || IDKMC] || NKMC) || NewKeyA)
vii. A → KMC : E(Ks, NKMC)
viii. A → Smart Phone : E(NewKeyA)
viiii KMC → CAR : E(NewKeyA)

First, the top five steps(from i to v) regard to mutual authentication between the vehicle owner A and KMC by the KDC.

After mutual authentication, vi and vii steps represent the process that the vehicle owner A receive a new key from KMC using session key and nonce.

Car owner A informs the KDC of its intention to establish a secure connection with KMC (Step 1).

The KDC returns to Aa copy of KMC's public-key certificate (Step 2).

Using KMC's public key, A informs KMC of its desire to communication and sends a nonce Na (Step 3).

KMC asks the KDC for A's public-key certificate and requests a session key. KMC includes A's nonce so that the KDC can stamp the session key with that nonce. The nonce is protected using the KDC's public-key (Step 4)

The KDC returns to KMC a copy of A's public-key certificate and the information [Na||KS || IDA || IDKMC]. This information basically says that KS is a secret key generated by the KDC on behalf of KMC and tied to Na, the binding of KS and Na will assure A that KS is fresh. This triple is in fact from the KDC. It is also encrypted using KMC's public-key so that no other entity may use the triple in an attempt to establish a fraudulent connection with A(Step 5).

The triple {[CAREnfNo || Na || KS || IDA || IDKMC] || NKMC) || NewKeyA} still encrypted with the KDC's public-key is relayed to A, together with a nonce NKMC generated by KMC. Also the triple includes NewKeyA. The NewKeyA will save a car key, All the foregoing are encrypted using A's public-key(Step 6).

A retrieves the session key Ks, uses it to encrypt NKMC, and returns it to KMC (Step 7).

A saves a new secret key in the car key(Step 8).

The KMC sends a new secret key to ECU (Step 9).

The meaning of the main symbols are as follows.

- A refers to the owner of the car using the imobiliszer system.
- The KDC, Key Distribution Center is to be sent to the owner of the car authentication information by KMC.
- KMC is the Key Management Center to provide authentication of the car and the owner of the car to KDC.
- PUKMC is a KMC's public-key.
- IDA is ID of car owner A.

- IDKMC is ID of the KMC.
- CAREngNo means the engine number of the car of their own.
- PUA means a car owner's public key.
- PRauth is KDC's Private-key.
- In order to ensure that it is not intended to be retransmitted, Na means a random value created by A.
- NewKeyA is a new key that are sent to and generate new for the owner of the car in A Key Management Center.

Table 1. Protocol parameters

Symbols	*Mean*
A	Car Owner
KDC	Key Distribution Center
KMC	Key Management Center
IDA	ID of a Customer A
IDKMC	ID of a KMC
CAREngNo	CAR Engine No
PUA	Public Key of A
PUKMC	Public Key of KMC
PRauth	Private key for authentication
Na	Nonce of a
NKMC	Nonce of KMC
NewKeyA	New Key for User A
Ks	Session Key

4. Evaluation

The proposed method in this paper complement the disadvantage of bringing the car to the service center directly in case of losing key and a new genuine key can be obtained by receiving owner's authentication by using only engine number and nonce.

Also in case of car and key both are stolen together, a action can be taken as soon after finishing user authentication process from KDC and KMC by using smart phone.

5. Conclusion

The immobilizer system is a kind of anti-theft system that the engine starts when the secret key that transmitted from transponder and the key that transmitted to ECU are matched. Of course

The process in above must be happened to use the genuine key. Now the proposed system helps to avoid some inconvenience point such as bringing car to the service center directly in case of the car key lost.

The proposed APSI protocol provides user authentication and security using KDC and KMC. The proposed protocol is used for responding as soon in case of car theft or losing key and prospective research may be directed to develop a system that inform the states of vehicle in order to use the vehicle safely and it would help those people who lack of knowledge about their vehicle.

REFERENCES

[1] www.carstart.co.kr

[2] Kyusuk Han, Swapna Divya Potluri, Kang G. Shin, "On Authentication in a Connected Vehicle : Secure Integration of Mobile Devices with Vehicular Networks", Cyber-Physical Systems (ICCPS), 2013 ACM/IEEE International Conference on, pp. 8-11, 2013
Page(s):160 - 169

[3] LI Baolin, WEI Tongmin, FAN Shuai, FAN Jiangpeng, "Study and Design of Gateway Engine Immobilizer based on CAN-bus", Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on, pp. 751-755, 2011

[4] LI Baolin, WEI Tongmin , FAN Shuai, FAN Jiangpeng , "Study and Design of Gateway Engine Immobilizer based on CAN-bus", Consumer Electronics, Communications and Networks (CECNet), pp. 751-755, 2011

[5] Yun-Sub Lee, Kyeong-Seob Kim, Jeong-Hee Yun, Sang-Bang Choi, "The Design and Implementation of Automotive Smart-key System Using general-purpose RFID", Journal of semiconductor technology and science, vol. 46, no. 4, pp.447-455, 2009.

[6] www.madebyesi.com

[7] William Stallings, Cryptography and network security, Prentice Hall(Pearson), USA, 2011

신 미 예(Miyea Shin)

- 1990년 8월 한밭대학교 전자계산학과(공학학사)
- 1998년 8월 충북대학교 전자계산학과 (이학석사)
- 2010년 2월 충북대학교 전자계산학과 (이학박사)

- E-Mail : myshiny@chungbuk.ac.kr

<관심분야> : 정보보호, 네트워크보안, 자동차보안

정 윤 수(Yunsu Jeong)

- 2000년 2월 충북대학교 대학원 전자계산학과 (이학석사)
- 2008년 2월 충북대학교 대학원 전자계산학과 (이학박사)
- 2012년 3월 ~ 현재 목원대학교 정보통신공학과 조교수

- E-Mail : bukmunro@gmail.com

<관심분야> : 센서 보안, 암호이론,정보보호,Network Security,이동통신보안

배 우 식(Woosik Bae)

- 2006년 8월 백석대학교 정보기술대학원 (공학석사)
- 2012년 2월 충북대학교 대학원 컴퓨터교육과(교육학박사)
- 1997년 3월~현재 아주자동차대학

- E-Mail : bws@motor.ac.kr

<관심분야> : RFID 보안, 무선 네트워크, 암호 프로토콜/알고리즘, 정보시스템

이 상 호(Sangho Lee)

- 1989년 2월 숭실대학교 전자계산학과 (이학박사)
- 1981년 3월 ~ 현재 충북대학교 전기전자 컴퓨터공학부 교수
- E-Mail : shlee@cbnu.ac.kr

<관심분야> : 네트워크보안, Protocol Engineering Network Management