International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:11, 2007

A Security Module for Car Appliances

Pang-Chieh Wang, Ting-Wei Hou, Jung-Hsuan Wu, and Bo-Chiuan Chen

***Abstract*—**In this paper we discuss on the security module for the car appliances to prevent stealing and illegal use on other cars. We proposed an open structure including authentication and encryption by embed a security module in each to protect car appliances. Illegal moving and use a car appliance with the security module without permission will lead the appliance to useless. This paper also presents the component identification and deal with relevant procedures. It is at low cost to recover from destroys by the burglar. Expect this paper to offer the new business opportunity to the automotive and technology industry.

***Keywords*—**Automotive, component identification, electronic immobilizer, key management.

I. Introduction

ACCORDING to statistic of NICB [10] in U.S.A., the highest automobile loss ratio was in the city of Modesto in California in 2005. Every 100,000 people suffering automobile loss were 1418.80. Developing future generation of the reliable car used the anti-theft system has been very urgent.

In order to build vehicle anti-theft system, the automotive industry has used electronic immobilizer to reduce thefts. The electronic immobilizer combines machinery guarding and a computer management system to run a special recognition procedure. This is depictured in Fig. 1. There is a chip which is integrated in the ignition key of the car. It will require an inside reader to compare with the data before starting the car each time. New cars almost have this electronic option now. This kind of cars needs original key to ignite, so better protection for vehicles can be provided. If electronic immobilizer combines component identification and biometrics, it will be able to bring more reliable vehicle anti-theft security system in the industry.

Manuscript received October 31, 2007. This work was supported in part by Contract Number 96C039 from the Automotive Research and Testing Center in Taiwan.

Pang-Chieh Wang is a Ph.D. student with the Department of Engineering Science, National Cheng Kung University, Tainan City, Taiwan (e-mail: pangchieh@nc.es.ncku.edu.tw).

Ting-Wei Hou is an Assoc. professor with the Department of Engineering Science, National Cheng Kung University, Tainan City, Taiwan (corresponding author to provide phone: 886-6-2757575-63334; fax: 886-6-2080526; e-mail: hou@nc.es.ncku.edu.tw).

Jung-Hsuan Wu is with the Department of Engineering Science, National Cheng Kung University, Tainan City, Taiwan (e-mail: ot@nc.es.ncku.edu.tw).

Bo-Chiuan Chen is with the R&D Division, Automotive Research and Testing Center, Lukang Town, Changhua County, Taiwan (e-mail: blissdom529@artc.org.tw).

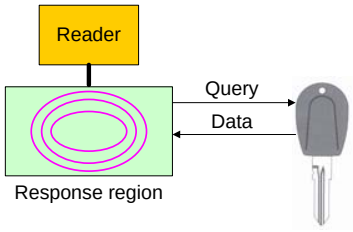

Fig. 1 Electronic immobilizer

Beside car itself, electrical appliances, such as audio/video player, are also prone to be stolen. How to prevent them from stolen is also an important issue. It is little information about the vehicle anti-theft security system can be taken into discussion public. We present security-critical vehicular applications that rely on electronic immobilizer, component identification and biometrics. It can be applied to highly security-critical environments. Therefore, we first discuss the background information in section II that are based on the security module, component identification, and CAN bus. In section III, we present a vehicle anti-theft security system that relies on section II. In section IV, we evaluate and discuss the referred system in this paper. Finally, we conclude our contribution about challenges and opportunities for the automotive industry in vehicles.

II. Background Information

A. Security Module

In our view, a car appliance which is featured in high price need to connect with in-car network and transmits sensitive data. This sensitive data must have been encrypted. So, such an appliance should embed a cryptographic security module. The security modules provide secure management of private keys. The private keys never leave the module unencrypted. The security module can offer a more secure hardware-based key generation technique than software-based generation. A security module may be based on a smart card microcontroller [7] or a TPM (trusted platform module) [6]. We assume all appliances that each of them needs to be anti-theft must have a security module embedded.

B. Communication Interface

CAN (Controller Area Network) [8][9] is getting used as communication interface in the automotive industry. It both has fault-tolerance ability and easy-build characteristic. Because the number of the ECUs (electronic control unit) is continuously increasing in the automobile, using traditional method will lead ECUs to exchange information following a lot

of connection ports. It will cost much more and cause longer circuit. This will result in the lower reliability of the automobile and the higher connection port failure rate. The appearance of CAN has solved the above communication problem among ECUs. It can reduce the number of signal lines and let all ECUs connect with CAN.

C. Component Identification

Component identification enables each appliance of a vehicle to have a unique identification (ID). It provides the centralized system with authentication mechanism, which verifies each appliance that the ID is legal and unique. One of implementation example of component identification is developed by RFID tag. The vehicle key which was stored on a tag is regarded as ID. A tag is attached to each crucial appliance. According to the RFID transponder attached with the centralized system, the check of a vehicle key will be performed. As depicted in Fig. 2, if any check fails in the security check process, an alarm is issued. Each appliance had assigned its unique certificate by a trusted third authority. If a new appliance is added to the vehicle, the certificate is checked. Only appliances that have a valid certificate are able to obtain the secret vehicle key. In [2], it performed cryptographic operations to transmit sensitive data as ID. Such scheme provides a more secure protection against counterfeits and theft.

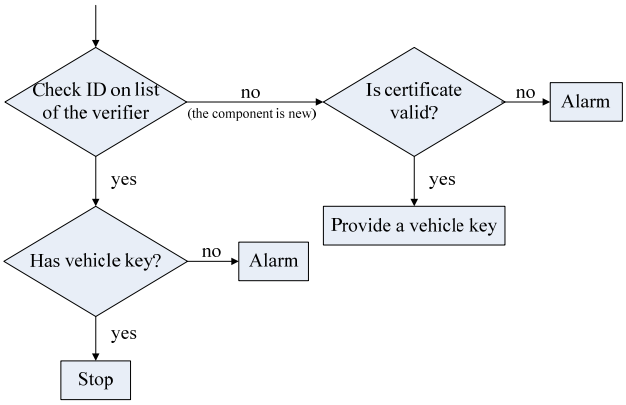

Fig. 2 Security check process example

There are some points should be discussed:

1) If the thief destroys the authorized system before or after stealing, other anti-theft appliances will not work.

2) The price to repair or reinstall the components from stolen or breakdown should be low. The new component can install and work immediately or needs to reset the system.

3) If the user removes a component in the car intentionally, the system should not reset. The process of removing the component can be smoothly and not causing the system warning.

III. System Architecture

The design of this paper is an anti-theft system like Fig. 3. The new appliance to the car can not work if it is not recognized. The car PC is the authorized center in the car to store all the IDs of the appliances. As the appliance starting, the security module in the appliance will request the ID from car PC by the CAN module and compare it to the one which it stored before. If the comparison is pass, the appliance works. The transmission between car PC and appliance is encrypted by to prevent illegal recording.

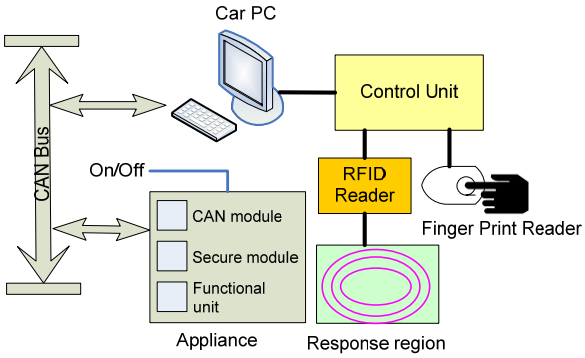

Fig. 3 System Architecture

The car PC and each appliance which connects to the CAN bus are all embedded a security module to identify each other and the relation. If the car PC is not power on, all the connected components can not activate.

The anti-theft of the car PC is described in section 2. The control unit will recognize the finger print and the data in the key to activate the car PC. The Table I is the anti-theft method of the components in the car. Even the whole system is stolen, it can not use in other place. The activation of the car PC is depended on the original key of the car, so the other appliances can not activate as the original key of the car is not used. This makes the car equipments more safety.

TABLE I
ANTI-THEFT OF ELECTRIC EQUIPMENTS

The activation of the all components	
Car PC	Depend on the original key of the car
Others appliances	Depend on the ID of the car PC

A. Encryption of the Data on CAN bus

When the appliance starts, the equipment related data will send to car PC, in order to prevent someone recording these data and attack the system. A digital signature is proposed in the CAN bus transmission, and a security module is to provide the key pairs and secure storage. The key pair is used to encrypt and signature the transmission data and the secure storage is used to store the sensitive data of the appliance or car PC.

The Table II defines the symbol of the signature process and the Fig. 4 shows the transmission between the car PC and the Appliance1.

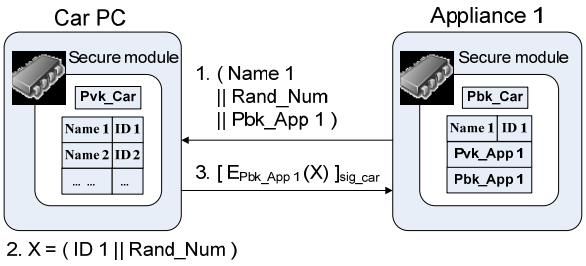

Fig. 4 The transmission between the car PC and the appliance

TABLE II
SYMBOL TABLE

Name	Public appliance serial number (both the car PC and the appliance have stored)
ID	Identification
Pbk_App	Public key of the appliance (generated by the security module of the appliance)
Pvk_App	Private key of the appliance (generated by the security module of the appliance)
Pbk_Car	Public key of the car PC (generated by the security module of the car PC)
Pvk_Car	Private key of the car PC (generated by the security module of the car PC)
$E_{puk\_App}[\ ]$	encrypted data by using of Pbk_App
$(\ )_{sig\_car}$	Encryption Signature by using of Pvk_Car
Rand_Num	Random number
||	Concatenation

It assumes that the car PC has the all appliance names, the IDs of the appliances and Pvk_Car. The appliance has the name, ID, Pbk_App, and Pvk_App of itself. The recognizing process is described as the follows:

STEP1: The appliance sends the Name1 to car PC, and the car PC looks up the related ID1 and Pbk_App1 by the Name1. At the same time, the Car PC gets the Rand_Num and Pbk_App1 from the Appliance1.

STEP2: Combines the ID1 and Rand_Num as X. Encrypts the X as Epbk_App1(X) by the Puk_App1 and signatures it as [Epbk_App1(X)]sig_car by Pvk_Car.

STEP3: Returns the [Epbk_App1(X)]sig_car to Appliance1. The Appliance1 verifies the [Epbk_App1(X)]sig_car by Pbk_Car whether the [Epbk_App1(X)]sig_car is from the Car_PC.

B. ID Generating Procedure

To prevent the ambiguous of the same ID of the different appliances in different cars, an ID generating procedure is needed. As the Fig. 5, the key distribution center (KDC) stores the master keys of the cars. The KDC use the unique number like the engine number to generate the derived key from the master key for each car. The derived key is a unique key for each car and stores in the car PC privately. The car PC can use this key to generate various Dynamic keys to regard as the IDs for each appliance and stores in their security module. The Fig. 6 shows how the keys derived in each step.

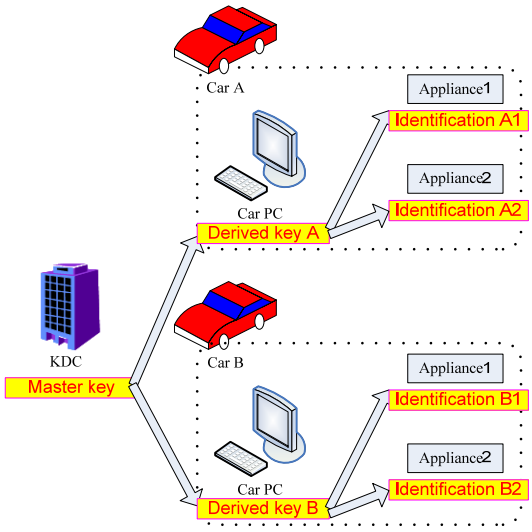

Fig. 5 The key generating procedure

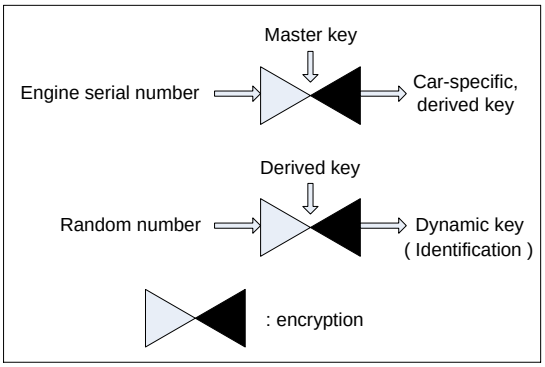

Fig. 6 The keys derived in each step

To achieve the same ID owned by the car PC and appliance, there should be some additional information for management. Table III defines the fields for management.

TABLE III
FUNCTION OF MANAGEABLE FIELD

Manageable field	
00(Default)	Compare identification
01	Reserved
10	Reserved
11	Write related information

In previous recognized process, there is:

$$X = (ID \,||\, Rand\_Num)$$

For the purpose of management, the X concludes the management field as the bottom. The management field is set as 00 initially.

$$X = (00 \,||\, ID \,||\, Rand\_Num)$$

As the appliance is power on, it will request the car PC to return an X and check the management field. When the security

module checks the field is 00, it compares the Rand_Num to decide if it should go to next step to check the ID and continues.

C. System Initialization and ID Update

As the car PC and appliance being work at first time, the related data should be initialized. The initialized process is defined according by Section III-B as follows:

1) Car PC and appliance generate the independent key pair.
2) Transmit the Public key Pbk_Car from car PC to appliance.
3) Car PC generates the ID of appliance and transmits to the secure storage of appliance.

The installation process should be done autonomous and can be modified by the user (the user needs not going back to factory). The car PC still provides a management interface for user to install and operate. This management must recognize the finger print and the car key of the user to activate to assure the security. As the same, an additional device like smart card can be used here optionally.

There are three management modes here:

As Fig. 7, the car PC transmits the key generation command to the new appliance. The security module will generate a key pair as public key and private key and stored. The private key should be stored in the secure storage. This command does not need encryption because if attack occurs, it can be send again and re-generate a key pair in the appliance. The mode-1 should run once in the new appliance for the initialization. As the mode-1 is done, the other operation of management or identification can be activated.

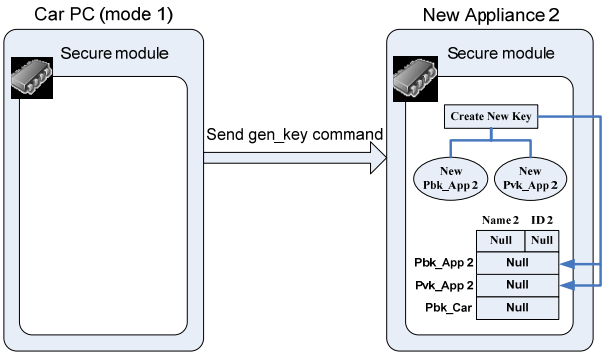

Fig. 7 Mode-1 for installing the new appliance

As the mode-2 depictured in Fig. 8, the car PC transmits the key generation command to its security module. The security module generates the key pair and store as the mode-1. The car PC should do this operation at first time and it can go to mode-3 to initialization.

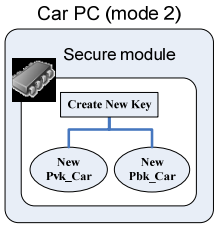

Fig. 8 Mode-2 for installing the car PC

When installs the car PC or appliance, the old ID of them should update. As the user operates the management interface to install the appliance to car PC for example, the appliance will send this message to car PC as:

$$(\text{Null} \,||\, \text{Rand\_Num} \,||\, \text{Pbk\_App})$$

As the mode-3 depictured in Fig. 9, the car PC receives this message and finds the ID of the appliance is not defined (compare to the database of car PC). It will generate a number as Name2 and uses the derived key and random number to generate a dynamic key. The dynamic key is the new ID2 of Appliance2 and these new Name and ID will store in the security module of car PC and appliance.

When transmits to appliance and stores it, the management field is set to 11 in the X to operate.

$$X = (11 \,||\, \text{Name} \,||\, \text{ID} \,||\, \text{Pbk\_Car} \,||\, \text{Rand\_Num})$$

At this moment, if the Pbk_Car in Appliance2 is null, Appliance2 will request the car PC to transmit the Pbk_Car.

As the security module of the appliance check the management field is 11, it will compare the Ran_Num and Pbk_Car are right or not. If they are right, the Name, ID and Pbk_Car will be store in the security module and the initialization is finished for the future recognizing process.

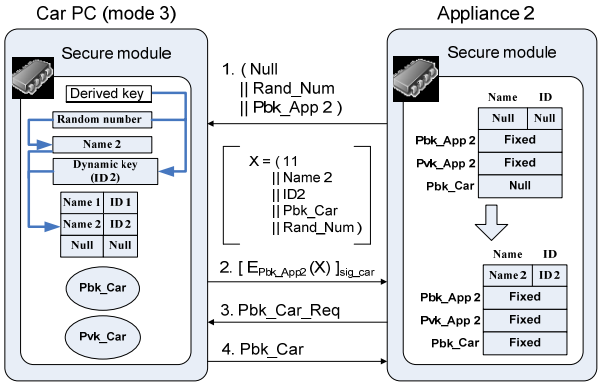

Fig. 9 Mode-3 for installing the car PC and appliance (1)

If the appliance has been used before, it means that there are old Name, ID and Pbk_Car. As buying old one to install in the user's car, the ID and Pbk_car should be changed and the name may change if repeat in the Car_PC. The update process is shown in Fig. 10 and is the same with Fig. 9.

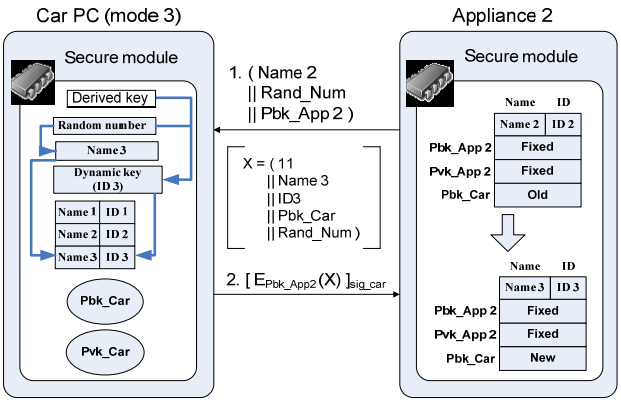

Fig. 10 Mode-3 for installing the car PC and appliance (2)

When the mode-3 is finished, the car PC and appliance can process the recognizing process of section III-A as every time starting to work.

D. Security Module Operation Algorithm

The appliance can work after the initialization. Every time as power on, it sends the Name, Rand_Num and Pbk_App to Car_PC and waits for recognition. No matter in which operation, the security module first decrypts the message X by it's own private key and do the related operation of the X. The Fig. 11 shows the interactive procedure of secure and functional unit:

IV. Solutions, Open Issues and Limitations

Based on the above text, we now discuss aspects to be when building this vehicle anti-theft system.

A. Security Analysis

The procedure can prevent from known key attack and key replayed attack and we will explain it.

Preventing known key attack: In each round, each node generates a unique random number, any attacker cannot compute even if he knows any of the previously compromised ones.

Preventing key replay attack: In section III, the fake car PC can receive Name, Rand_Num and Pbk_App accordingly and replay to take ID cheating appliance. However, replay attack is not successful in this system. Appliance also received the signature information from the car PC at the same time. After checking by stored Pbk_Car, appliance can convince that the message is not a replayed one and confirm that this message is original from the car PC. In the same way, the fake appliance could generate the key-pair and transmit Name, Rand_Num and Pbk_App in order to obtain ID and store it. It is meaningless for the movement because this architecture does not exclude the general appliances existing in a car. Only the appliance will lose anti-theft function if we install a general one. Our purpose is to express that the appliance built-in security module cannot be used in a non-owner's car.

The character of this procedure that allows the user to start the appliance does not decide by the central system, but the appliance itself.

```
Step 1.  receive the encryption cipher
Step 2.  if Pbk_Car is not Null
           if the signature verification is correct
             decrypt cipher into plaintext
           else
             send error message to car PC
             go to Step 4
         else
           send Pbk_Car_Req command to car PC
           wait Pbk_Car from car PC and store
           go to Step 2
Step 3.  interpret the plaintext
         if current Rand_Num matches previous Rand_Num
           case manageable field of
           "00"
             if the identification is legal
               send command to the functional unit
             else
               send error message to car PC
               go to Step 4
           "11"
             set the new number of variables
             (Name, ID, Pbk_Car)
         else
           send error message to car PC
           go to Step 4
Step 4. procedure stop
```

Fig. 11 Pseudocode for the security module interacting phase when power on

B. Remove the Car PC or the Appliance

In case of contingency, the car PC was stolen by the thief and installed on other car. It looked like scrap because the car PC needed to check the vehicle owner's electronic immobilizer and fingerprint to start. Similarly, if the general appliance was also stolen and installed on non-owner's car. It still will check the particular car PC to start. Even if both the car PC and the appliance were stolen at the same time, the thief wanted to use the stolen components also needed the owner's electronic immobilizer and fingerprint. This design corresponds with the section 2's point of view. Even though the central system is broken by the thief, the appliances might still be unable to start.

C. Recovery Cost and Convenience

In our architecture, if an appliance should be repaired and uninstalled, the central system does not want to reconfigure. It solves the problems 2 and 3 of the section 2's viewpoints. But it must be configured in first installation. However, it is already have the less recovery cost we shall have on the configuration. And it is the same of convenience on the car PC which should be repaired and uninstalled.

V. Conclusion and Future Work

This paper presents a vehicle anti-theft system that provides a protected component be moved to other vehicles without permission, it will be unable to use. It is at low cost to recover from destroying by the burglar. We have proposed an encryption procedure, the production and the update of the ID, the implementation of the component identification. Finally, we discuss the feasibility of this system. Expect this paper to offer the new business opportunity to the automotive and technology industry.

By using our solution, it can provide to easily protect the vehicle according to the development of electronics. The central system would be easy to trace each appliance when it was produced and where it was installed in. A security module can return error messages to car PC. If we can diagnosis these messages, it will provide users with more useful information. On the other hand, this vehicle anti-theft system also can operate in coordination with other alarm system or GPS. It should be able to create new applications.

References

[1] Kerstin Lemke, Ahmad-Reza Sadeghi and Christian Stüble, "An Open Approach for Designing Secure Electronic Immobilizers", Information Security Practice and Experience, First International Conference, ISPEC 2005, Singapore, April 2005
[2] André Weimerskirch, Christof Paar, Marko Wolf, "Cryptographic Component Identification: Enabler for Secure Vehicles", IEEE 62nd Semiannual Vehicular Technology Conference, VTC, Dallas, Texas, USA, September 2005
[3] Sundeep Bajikar, Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper, Mobile Platforms Group, Intel Corporation, June 20, 2002, available at http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf
[4] Steven Kinney, Trusted Platform Module Basics - Using TPM in Embedded Systems, Newnes Ltd., July 2006
[5] Bruce Schneier, Applied Cryptography, 2nd Ed., John Wiley & Sons Ltd., 1996
[6] Trusted Computing Group. Trusted Platform Module Main Specification. June 2006, Version 1.2, Revision 94, available at http://www.trustedcomputinggroup.org
[7] Wolfgang Rankl, Wolfgang Effing, Smart Card Handbook 3rd Ed., John Wiley & Sons Ltd., January 2004
[8] Bosch's Controller Area Network Homepage, available at http://www.can.bosch.com
[9] Can in Automation (CiA) Can Protocol introduction, available at http://www.can-cia.de/can/protocol/
[10] National Insurance Crime Bureau (NICB), available at https://www.nicb.org