International Journal of Advanced Smart Convergence Vol.4 No.1 1-10 (2015)
http://dx.doi.org/10.7236/IJASC.2015.4.1.1

IJASC 15-1-1

EE03 Development of an Automotive Anti-Theft System

Pulkit Batra[1]

[1]*Delhi Technological University (Erstwhile Delhi College of Engineering), New Delhi, India*
pulkitbatra12@gmail.com

Abstract

Automotive Theft has been an obstinate problem around the world. Design and manufacture of anti-theft systems have become more and more complex due to the rise in complexity of theft in the system. Most of the anti-theft systems available in the market, are the alarm types which audibly deter some thieves away but do not prevent one's car from being stolen and even are not good enough to meet the growing complexity of theft in the country. This paper presents a simple and an efficient anti-theft system which provides improved security by the use of efficient access mechanisms and immobilization systems. This security system can immobilise an automobile and its key auto systems through remote control when it is stolen. It hence deters thieves from committing the theft. It also effectively prevents stealing of key auto systems for reselling by introducing four layers of security features written in the form of firmware and embedded on the Electronic Control Units (ECUs). The particulars of system design and operation are defined in the paper. The experimental outcomes show that this system is practicable and the owner can steadily control his vehicle within a few seconds.

Keywords*: ECUs-Electronic Control Units, Car Communications, Security System, Anti-Theft, Temper Detection, Controller Area Network*

NOMENCLATURE

Symbol	Description [Units]
ASS	Automotive Security System
CAN	Controller Area Network
ECU	Electronic Control Unit
EVI	Electronic Vehicle Identification
GPRS	Global Packet Radio Service
GSM	Global System for Mobile Communications
LED	Light Emitting Diode
RC	Remote Control
SBC	Single Board Computer
SVRS	Stolen Vehicle Recovery System
TPU	Transfer Proof Unit
UART	Universal Asynchronous Receiver/Transmitter

Manuscript Received: Jan. 10, 2015 / Revised: Feb. 5, 2015 / Accepted: Mar. 13, 2015
Corresponding Author: pulkitbatra12@gmail.com
Tel: +91-11-27871018, Fax: +91-11-27871023
Delhi Technological University (Erstwhile Delhi College of Engineering)

1. INTRODUCTION

Automotive theft has been an obstinate problem around the world. In the US alone, 715,373 motor vehicles were stated stolen in 2011, and the equivalent value of stolen motor vehicles was $4.3 billion US dollar [1]. The automobiles have been stolen for different reasons viz. for using the vehicles for transport, commission of crimes and for reusing or reselling parts dismantled from the vehicles or resale of the vehicle itself. Various technologies have been introduced in recent years to prevent car thefts, for example, Immobilizers [2] to distantly disable the lost vehicles, Microdot Identification [3] to identify auto parts using inimitable microdots, Electronic Vehicle Identification (EVI) [4] to identify the vehicle against a registration database, LoJack System [5] to use in-built transponders for tracking down vehicle, GPS [6] to locate the position of the lost vehicles using global positioning system, and so on. However, there are still some security gaps which these technologies do not address. For example, while the immobiliser can prevent a thief from starting a car engine and driving away, it is unable to stop professional thieves from towing the car away. The professional thieves can then dismantle the stolen vehicle and re-sell the components. The thieves will also have the luxury of time to remove the immobiliser and re-sell the car using another identity; while microdot identification has the advantage of being very difficult in removing the microdots, identification and verification of vehicle information is inconvenient as a microdot has to be removed and read from a microscope.

Microdot identification is ineffectual against thieves who export the stolen vehicles or the chopped car parts to countries which do not practise the identification and verification of vehicles; the EVI approach is efficient when it comes to identification and verification of vehicles since this is done electronically. However, EVI is less effective against the chop shop scenario where stolen vehicles are dismantled and their parts are re-sold into the market. In addition, the EVI approach is ineffective against thieves who export the stolen vehicles or the chopped car parts to countries which do not implement the EVI system; while LoJack Systems may be good at tracking the lost vehicles, it may take a few hours/days/months or even cannot find the stolen vehicle. In addition, they cannot disable an automobile and its key auto systems. Thus, if their radio transponders are removed, the stolen automobiles still function well and the thieves can drive them or sell them.The thieves can also dismantle the auto systems and re-sell auto parts; finally, GPS cannot penetrate forest cover, parking garages, or other obstructions. GPS relying on a short visible antenna can easily be broken off by a thief. Thus, greater challenge comes from professional thieves [7] because they are capable of removing the immobilizers, LoJack or GPS parts from the automobile and re-sell the vehicles or auto parts.

The most effective automotive security system is probably one that will lead a thief to abandon the idea of theft that he sets his eyes upon. This will be the case if the thief knows that he will gain little financial benefits from his theft in spite of the risks he will be taking. If a theft knows that an automobile and its key auto systems will be disabled when its owner finds that the automobile is stolen, it will deter the theft from committing the theft. Therefore, this paper presents our automotive security system to disable an automobile and its key auto systems through remote control when it is stolen. The remainder of this paper is organized as follows: in the next section, the proposed security system, further the details of implementation followed by the experimental results and by a conclusion.

2. AUTOMOTIVE ANTI-THEFT SYSTEM

The requirement is to design and develop an automotive security system[8] to disable an automobile and its key auto systems through remote control when it is stolen. Our system will
verify the automobile and its key auto systems before it allows the automobile to start. If our system receives a disable command from the owner, the system will disable the automobile from re-starting and the key auto systems from activating. Thus, the owner still has some control to disable the vehicle from starting and key auto systems from activating after it is stolen. Our solution is targeted for the automobiles with Controller Area Network (CAN) [9, 10] and Electronic Control Units (ECUs) which are integrated with mechanical parts for good enactment. Almost all high-end cars have ECUs incorporated with the different mechanical parts like fuel-injection system, ignition and crank-angle sensor systems. Fig. 1 gives an complete interpretation of the security system from the viewpoint of the automobiles' owners.

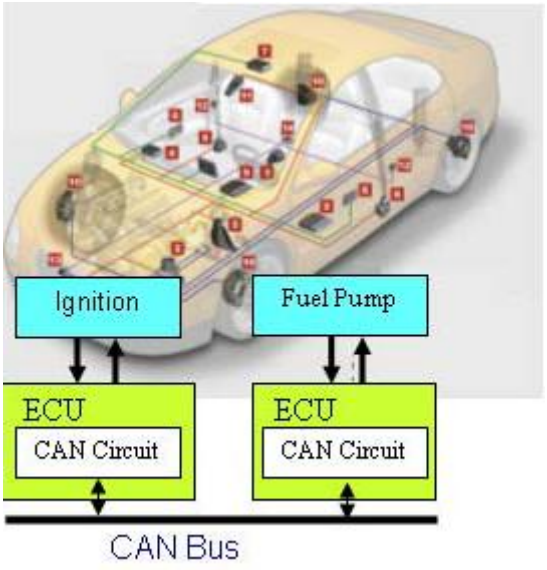

Figure 1. An automotive security system using RC

2.1 Remote Immobilising

Once an owner realizes his vehicle is lost, all he needs to do is to send a "Immobilise" SMS from his mobile phone to a secret and specific phone number which is dedicated to the electronics on the automobile. After the SMS is received, the security system will check the mobile phone number of owner and his allocated automobile numbers for authentication. If there is a match (owner to vehicle), the SMS is forwarded to process and the automobile cannot be started again after it stops. In other word, only owner's mobile number is recognized by the system and an attacker cannot disable the automobile remotely by a SMS message. This system on the automobile carries a single board computer (SBC) which is integrated to a GSM modem. Once a SMS message is received by the GSM modem, the single board computer checks for the correct message that is required to enable or disable the automobile. After this the single board computer gives an appropriate command to a master ECU. The master ECU then transfers the disable signal to the network of ECUs on the automobile and all the individual ECUs will disable the mechanical parts that are connected to them, which include critical systems for starting the car like ignition system and fuel pump system.

2.2 Tamper Detection and Self-Immobilising

Another important feature in our system is that it has the capability of detecting if the ECUs belonging to individual mechanical parts or the automobile's CAN are tampered with. Tampering here could be disconnection and replacement of an ECU from the automobile or introducing an unauthorized listening post into the CAN. The master ECU authenticates each ECU before the automobile is started. If the system detects that one of the ECUs has been tampered with, the master ECU signals all ECUs to disable and disables itself as well. The same happens in the case if it detects an unauthorized ECU. In both remote and self-immobilising mechanisms, the automobile can be made to function only if the owner sends an "Enable" SMS message to the dedicated phone number. This solution not only prevents a stolen car from restarting (disables the car), but also disables the key auto systems so that they cannot function with good performance. Hence, the thief will not be able to re-sell the key auto systems with high price. If an automobile and its key auto systems can be disabled, the thief will be deterred from stealing it in the first place. Thus the effectiveness of our system can be analyzed in Table I. Table I compares our technology with other automotive anti-theft solutions. From the comparison, our automotive security technology is a most effective solution at current stage.

Table 1. Comparison of Different Anti-Theft Solutions

	Chopping of auto parts	Illegal export of stolen vehicle	Automotive theft through robbery/ towing	Automotive theft by breaking into vehicles
Our technology	Effective to some degree	Effective	Effective	Effective
Immobiliser	Ineffective	Ineffective	Ineffective	Effective
Microdots Identification	Effective to some degree	Ineffective	Effective to some degree	Effective to some degree
EVI	Ineffective	Ineffective	Effective to some degree	Effective to some degree
LoJack System	Ineffective	Ineffective	Effective	Effective
GPS	Ineffective	Effective to some degree	Effective to some degree	Effective to some degree
	Can not penetrate forest cover, parking garages, or other obstructions. Rely on a short visible antenna that can easily be broken off by a thief.			

3. APPLICATION

The application includes hardware design and software programming described in the following subsections.

3.1 Hardware Design

The implementation of the system required integration of many individual parts each capable of carrying out the critical functions of the system. The system consists of a single board computer (Soekris Net 4501), GSM modem (iTegno 3800 modem) and multiple ECU boards[14] each with a PIC16F676 chip and integrated CAN adaptor. A picture of the completed system with all the above mentioned components is shown in Fig. 2.

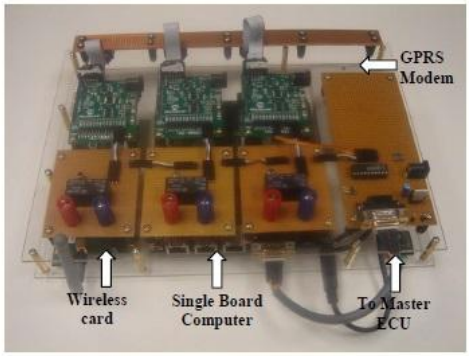

Figure 2. Hardware design of the security system

The details of integration of different parts are as below.

1) ECU & Single Board Computer- The ECU board consists of PIC16F676 chip which does not support UART(Universal Asynchronous Receiver/Transmitter). Thus the master ECU consists of a software implementation of the RS232 serial port communication. The firmware on the PIC16F676 chip for this resides only on the master ECU since it needs to communicate with the single board computer.

2) Single Board Computer & GSM Modem - The single board computer consists of AMD Xeon processor which is similar to i586 architecture[10]. It runs Gentoo Linux OS installed on external flash memory of 2GB. The GSM modem is connected to the single board computer though USB (Universal Serial Bus) and the connection is managed by a program running on the single board computer[11].

The following sections describe briefly the software programming in each critical component of the system.

3.2 Single Board Computer

The single board computer acts as the middle man between the CAN network and the GSM modem. The C program that runs on this keeps polling for messages both from the serial port and GSM modem using different threads A and B[13]. It detects when an SMS is received and checks whether it is Enable or Disable SMS and sends the corresponding command through serial port to the master ECU. Any messages from the master ECU in case of tamper is also transmitted over the GSM modem as an SMS to the automobile's owner. This deals with the part for remote disabling/enabling the automobile.

3.3 Master ECU - 4 Layers of Security

It is assumed that the master ECU is tamper proof (Transfer Proof Unit – TPU) for our system. The master ECU is responsible for transmitting the commands issued by the single board computer to the rest of the networked ECUs over CAN bus[14]. It is also the main ECU that has code for checking authenticity of all the ECUs attached to the CAN bus when the automobile is switched on each time and to detect tampering activity in the network.

1) Layer 1

Detection of tampering is done by the TPU sending out request message to individual ECUs as shown in Fig. 3.Upon receiving the request message[12], the ECU has to reply to the TPU within a short time period. Failure of the ECU in replying within the timing results in the TPU broadcasting the "Disable" message. This is due to the assumption that the particular ECU is being tampered. The TPU also sends the identification of the ECU suspected to be tampered to the single board computer. Subsequent "Enable" messages to the ECU will not results in the enabling of the automobile until all the nodes are reset.

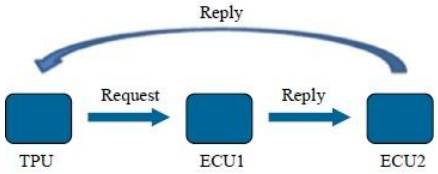

Figure 3. Random Reply Node Methodology

2) Layer 2

Although the TPU is absolutely secure from any tampering, it is still vulnerable to replay attack. One of the scenarios is that the attacker listens to the network and remembers all the requests and replies between the TPU and the ECUs[10]. Then the attacker disconnects the TPU from the network. Since all the previous communications are remembered, the attacker just replays the reply to the TPU for every request. This allows the attacker to tamper the ECUs without the TPU detecting. To overcome this form of replay attack, the messages between the TPU and the ECUs need to be random. Although there are many methods to make the messages random, some of the methods may not be feasible in this project with the limit resource of the ECU boards.

The project introduces the use of the reply node which is a very efficient method. The basic idea is not to reply to the TPU request directly but via another ECU. For example, TPU sends a request message to ECU 1. ECU 2 sends the reply to TPU on ECU 1 behalf as shown in Fig. 3. To randomize the reply node, it requires an initialization phase where the TPU assigns each ECU with a random reply node id.

3) Layer 3

Another scenario is that the attacker is able to successfully emulate some ECUs. This will break the above mentioned defense as the TPU will not notice the activity. However the attempt will still not be fruitful as each ECU is also equipped with a layer of security feature. The ECU is always listening to the network. Inside each ECU, there is a counting mechanism. Every time a message from the TPU is received, the counter will be reset. The ECU will disable itself if the counter increment to a predefine value.

4) Layer 4

Another possible attack is by removing the security feature in ECUs. This requires an attacker the understanding of the coding residing in the ECU[11]. In order to overcome this attack, code obfuscation is applied to the coding. This will mess up the coding and make it complicated for the attacker. Since the program is distributed in its native form, only binary obfuscation technique is used. Fig. 4 shows the difference between obfuscated code and non-obfuscated code. It can be clearly seen how difficult and time consuming it should be to reverse engineering the whole code on each ECU from binary to disassembly and finally to source code. There are different forms of binary obfuscation by source code manipulation.

4. EXPERIMENT

The experiments are carried out to test functionality of the system. A prototype has been developed and tested with automobiles.

4.1 Remote Immobilising

When all the ECUs are first powered up, all the LEDs are on. This means that the system is being disabled. A SMS with the “Start engine” content is sent to the single board computer. After a while, the LEDs on all

the ECUs are off – system is enabled and the vehicle is allowed to start. A second SMS with "Stop engine" content is sent. After a while the LEDs on all the ECUs are on - system is disabled and the vehicle is not allowed to start. Our demonstration shows that a car owner can use his mobile phone to securely protect his car from theft. When the owner discovers that his car is stolen, the owner uses his mobile phone to send a "Stop engine" message to the security system inside his car so that the car is prevented from being re-started. This is achieved by disabling the key auto systems such as ignition system, fuel pump and so on. After the car is found, the systems can be enabled again by the owner simply sending a "Start engine" message to the security system to enable his car to be started.

4.2 Tamper Detectability

If any of the ECUs, for an instance, ECU 1 is removed, the ECU 1's LED is on after a while, followed by the TPU and the rest of the ECUs. This shows that when any of the ECUs are detached from the system, the whole system will be disabled. Also at the same time, a SMS is sent to the owner's mobile phone with the content saying ECU 1 is being tampered. In this way, any part of the system is removed or tampered, the system is able to detect and disable the automobile from re-starting and key auto systems from activating.

Obfuscated code	Non-Obfuscated Code
LED = (y * y + z * z) % (y + z); 0EE 0836 MOVF 0x36, W 0EF 00C7 MOVWF 0x47 0F0 0835 MOVF 0x35, W 0F1 00C6 MOVWF 0x46 0F2 0836 MOVF 0x36, W 0F3 00C5 MOVWF 0x45 0F4 0835 MOVF 0x35, W 0F5 00C4 MOVWF 0x44 0F6 23B9 CALL 0x3b9 0F7 0848 MOVF 0x48, W 0F8 1283 BCF 0x3, 0x5 0F9 00B7 MOVWF 0x37 0FA 0849 MOVF 0x49, W 0FB 00B8 MOVWF 0x38 0FC 0834 MOVF 0x34, W 0FD 00C7 MOVWF 0x47 0FE 0833 MOVF 0x33, W 0FF 00C6 MOVWF 0x46 100 0834 MOVF 0x34, W 101 00C5 MOVWF 0x45 102 0833 MOVF 0x33, W 103 00C4 MOVWF 0x44 104 23B9 CALL 0x3b9 105 0837 MOVF 0x37, W 106 07C8 ADDWF 0x48, F 107 1803 BTFSC 0x3, 0 108 0AC9 INCF 0x49, F 109 0838 MOVF 0x38, W 10A 07C9 ADDWF 0x49, F 10B 0848 MOVF 0x48, W	LED = 0; 0EE 1107 BCF 0x7, 0x2

10C 00C4 MOVWF 0x44 10D 0849 MOVF 0x49, W 10E 00C5 MOVWF 0x45 10F 0834 MOVF 0x34, W 110 00C7 MOVWF 0x47 111 0833 MOVF 0x33, W 112 00C6 MOVWF 0x46 113 0835 MOVF 0x35, W 114 07C6 ADDWF 0x46, F 115 1803 BTFSC 0x3, 0 116 0AC7 INCF 0x47, F 117 0836 MOVF 0x36, W 118 07C7 ADDWF 0x47, F 119 2066 CALL 0x66 11A 0C44 RRF 0x44, W 11B 1C03 BTFSS 0x3, 0 11C 291F GOTO 0x11f 11D 1507 BSF 0x7, 0x2 11E 2920 GOTO 0x120 11F 1107 BCF 0x7, 0x2	

Figure 4. Obfuscated code versus non-obfuscated code

4.3 Results

The experiment was five times and the value in the last row is the average time of the five experiments. From the results, it is clear that the time spent in our embedded software is relatively low, thus it can be concluded that the proposed anti-theft solution is technically feasible and under normal circumstances, the owner can securely control his car within a few seconds. (T1 - t2), (T2 – t4), and (T3 – t6) are the messages communication time between mobile phone and GPRS modem. The observations are shown in the table as under-

TABLE 2. TIME MEASUREMENTS

Stop Engine		
T_1 **(second)**	t_2 **(second)**	$(T_1 - t_2)$ **(second)**
6	2	4
5	1	4
8	1	7
4	1	3
8	3	5
6.	**1**	**5.**

Start Engine		
T_2 **(second)**	t_4 **(second)**	$(T_2 - t_4)$ **(second)**
6	1	5
8	1	7
6	1	5
8	2	6
6	1	5
7	**1**	**5**

Tamper Detection		
T_3 **(second)**	t_6 **(second)**	$(T_3 - t_6)$ **(second)**
12.8	4	8.8
12.3	4	8.3
12.4	4	8.4
14.7	4	10.7
14.9	4	10.9
13.42	**4**	**9.42**

5. CONCLUSION

This paper presents an automotive security system to disable an automobile from re-starting and its key auto systems from activating through remote control when it is stolen. Our security technology is also very effective solution to prevent the automobile stealing with the aim of reselling key auto systems. This is achieved by introducing four layers of security features written in the form of firmware and embedded on the ECUs. Hence, our system deters thieves from committing the theft because they will gain little economic benefits from his theft in spite of the risks he will be taking. Therefore, our automotive security technology is a most effective anti-theft solution at current stage. The experimental results show that the owner can securely control his vehicle within a few seconds, and the running time of our security software is acceptable. In our future works, the security system will be further improved to function as an integrated data security system for car communications, such as vehicle-to-vehicle, vehicle to- infrastructure communications. It will ensure that all data exchanged with inside and with outside automobile is protected from abuse and security attack.

ACKNOWLEDGEMENT

This paper has been supported by Delhi Technological University (Erstwhile Delhi College of Engineering), Delhi, India. All the research work was conducted at CASRAE (Centre for Advanced Studies and Research in Automotive Engineering) lab at Delhi Technological University, Delhi, India.

REFERENCES

[1] Uniform Crime Report, *US Department of Justice*, September 2012.
[2] AutoTheft, Insurance Information Institute, May 2011, *http://www.iii.org/media/ hottopics/insurance/test4*
[3] Immobiliser, WHATCAR, *http://www.whatcar.com/news-specialreport.aspx?NA=22 0071*
[4] Data Dot DNA, Data Dot Technology, *http://www.datadotdna.com/dtl_technology_ourtechs_dot.htm*
[5] Foundation for Tackling Vehicle Crime, Motor Vehicle Identification – Why EVI is so important, Mar. 2011, *http://www.stavc.nl/pdfdb/publicaties/identificationreport.pdf*
[6] Lojack system, *http://lojack.com/*
[7] P. H. Dana, Global Positioning System Overview, *http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html*
[8] R. Carroll, "Insurance Practices and Professional Vehicle Theft," Insurance and Corporate Fraud Conference, 2011, *http://www.carsafe.com.au/speeches/presentation_29.doc*
[9] H. S. Cheng, H.Q. Guo and Y.D. Wu, "A Method and System For Tamper Proofing A System of Interconnected Electronic Devices," *US PCT patent application*, No.60/900,317. February 2008.
[10] Robert Bosch Gmbh, Controller Area Network (CAN), *http://www.semiconductors.bosch.de/en/20/can/index.asp*
[11] Mohammed, A., Muntaser,M., Sayel, F. and Suleiman, A.E, "A Practical Design of Anti-Theft Car Protection System Based on Microcontroller," *American Journal of Applied Sciences*, Vol. 9, No. 5, pp. 709-716, 2012.
[12] David Lane, *Car Alarm System*, Carlifornia Polytechnic State University, 2012.

[13] Montaser, N.R., Mohammad, A.A., Sharaf A.A, "Intelligent Anti-Theft and Tracking System for Automobiles," *International Journal of Machine Learning and Computing*, Vol. 2, No. 1, February 2012.
[14] Visa, M. I., Asogwa, A. V., Musa, S.Y, "GSM Based Anti-theft Security System Using AT&T Command," *International Journal of Computational Engineering Research (ijceronline.com)*, Vol. 2 Issue.5, September 2012.
[15] Ali. A Design for CAR Anti-Theft System Using Cell Phone.