Abstract— Automotive theft has been a persisting problem around the world and greater challenge comes from professional thieves. In this paper, we present an automotive security system to disable 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 re-selling by introducing four layers of security features written in the form of firmware and embedded on the Electronic Control Units (ECUs). The details of system design and implementation are described in the paper. The experimental results show that our system is feasible and the owner can securely control his vehicle within a few seconds.

Keywords: Car Communications, Security System, Anti-Theft, Controller Area Network, Temper Detection

I. INTRODUCTION

Automotive theft has been a persisting problem around the world. In the US alone, 1,237,114 motor vehicles were reported stolen in 2004, and the equivalent value of stolen motor vehicles was $7.6 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 deter car thefts, for example, Immobilizers [2] to remotely disable the lost vehicles, Microdot Identification [3] to identify auto parts using unique 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 ineffective 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 stealing the automobile that he sets his eyes upon. This will be the case if the thief knows that he will gain little economic benefit from his theft in spite of the risks he will be taking. If a thief 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, we present our security system, while Section III presents the details of implementation. Section IV presents our experimental results. Finally we conclude the results in Section V.

II. AN AUTOMOTIVE SECURITY SYSTEM

We 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 performance. Almost all high-end cars have ECUs integrated with the different mechanical parts like fuel-injection system, ignition and crank-angle sensor systems. Fig. 1 gives an overall view of the security system from the perspective of the automobiles’ owners.

Figure 1. An automotive security system for remote control.

A. Remote Disabling

Once an owner realizes his vehicle is lost, all he needs to do is to send a “Disable” SMS from his mobile phone to a secret and specific phone number which is dedicated to the electronics on the automobile. After receiving the SMS, 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 can not disable the automobile remotely by a SMS message.

Our 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.

B. Tamper Detection and Self-Disabling

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-disabling mechanisms, the automobile can be made to function only if the owner sends an “Enable” SMS message to the dedicated phone number.

Our solution not only prevents a stolen car from re-starting (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>
<thead>
<tr>
<th></th>
<th>Chopping of auto parts</th>
<th>Illegal export of stolen vehicle</th>
<th>Automotive theft through robbery/ towing</th>
<th>Automotive theft by breaking into vehicles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our technology</td>
<td>Effective to some degree</td>
<td>Effective</td>
<td>Effective</td>
<td>Effective</td>
</tr>
<tr>
<td>Immobiliser</td>
<td>Ineffective</td>
<td>Ineffective</td>
<td>Ineffective to some degree</td>
<td>Effective</td>
</tr>
<tr>
<td>Microdots Identification</td>
<td>Effective to some degree</td>
<td>Ineffective</td>
<td>Effective to some degree</td>
<td>Effective to some degree</td>
</tr>
<tr>
<td>EVI</td>
<td>Ineffective</td>
<td>Ineffective</td>
<td>Effective to some degree</td>
<td>Effective to some degree</td>
</tr>
<tr>
<td>LoJack System</td>
<td>Ineffective</td>
<td>Ineffective</td>
<td>Effective</td>
<td>Effective</td>
</tr>
<tr>
<td>GPS</td>
<td>Ineffective</td>
<td>Effective to some degree</td>
<td>Effective to some degree</td>
<td>Effective to some degree</td>
</tr>
</tbody>
</table>

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.

III. IMPLEMENTATION

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

A. 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 4801), GSM modem (iTegno GSM/GPRS modem) and multiple ECU boards 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.

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. 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.

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

B. 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. 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.

C. 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. 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, 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. Tamper Detection Algorithm.](image)

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. 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. 4. 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. The flow of programming is shown in Fig. 5.

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. 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. 6 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.
IV. EXPERIMENTAL RESULTS

The experiments are carried out to test functionality of the system. The experimental setup is show in Fig. 7. A prototype has been developed and tested with automobiles.

![Experimental Setup](image)

Figure 7. Experimental Setup.

A. Remote Disabling

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.

B. 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.

C. Performance Results

In order to determine the feasibility of the proposed solution, we conducted experiments by measuring time $T_1$ taken from the mobile phone sending out a “Stop engine” message to ECUs disabling the engine to be started. We also took time measurements in the software to determine time $t_2$ from the time GPRS modem receiving the message to when the ECUs disables the engine. Similarly, we also measured time $T_2$ taken from the mobile phone sending out a “Start engine” message to when ECUs enables the engine, and time $t_4$ which is from the GPRS modem receiving the message to when ECUs enables the engine. Furthermore, since we embed security features in ECUs, if an ECU is being tampered, the security system will send out the alert message via the GPRS modem at once to inform the owner. Thus, we also measured time $T_3$ from when an ECU is tampered to when the mobile phone receives the alert SMS message. We further measure time $t_6$ from when an ECU is tampered to when the GPRS modem sends out an alert message. Therefore, $(T_1 - t_2)$, $(T_2 - t_4)$, and $(T_3 - t_6)$ are the messages communication time between mobile phone and GPRS modem. The experimental results are shown in Table II. We conducted each of the experiments 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 we conclude that the proposed anti-theft solution is technically feasible and under normal circumstances, the owner can securely control his car within a few seconds.

<table>
<thead>
<tr>
<th>Stop Engine</th>
<th>$T_1$ (second)</th>
<th>$t_2$ (second)</th>
<th>$(T_1 - t_2)$ (second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6</td>
<td>2</td>
<td>4.6</td>
<td></td>
</tr>
<tr>
<td>5.5</td>
<td>1</td>
<td>4.5</td>
<td></td>
</tr>
<tr>
<td>8.5</td>
<td>1</td>
<td>7.5</td>
<td></td>
</tr>
<tr>
<td>4.7</td>
<td>1</td>
<td>3.7</td>
<td></td>
</tr>
<tr>
<td>8.6</td>
<td>3</td>
<td>5.6</td>
<td></td>
</tr>
<tr>
<td>6.78</td>
<td>1.6</td>
<td>5.18</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Start Engine</th>
<th>$T_2$ (second)</th>
<th>$t_4$ (second)</th>
<th>$(T_2 - t_4)$ (second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>1</td>
<td>5.4</td>
<td></td>
</tr>
<tr>
<td>8.0</td>
<td>1</td>
<td>7.0</td>
<td></td>
</tr>
<tr>
<td>6.0</td>
<td>1</td>
<td>5.0</td>
<td></td>
</tr>
<tr>
<td>8.4</td>
<td>2</td>
<td>6.4</td>
<td></td>
</tr>
<tr>
<td>6.9</td>
<td>1</td>
<td>5.9</td>
<td></td>
</tr>
<tr>
<td>7.14</td>
<td>1.2</td>
<td>5.94</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tamper Detection</th>
<th>$T_3$ (second)</th>
<th>$t_6$ (second)</th>
<th>$(T_3 - t_6)$ (second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.8</td>
<td>4</td>
<td>8.8</td>
<td></td>
</tr>
<tr>
<td>12.3</td>
<td>4</td>
<td>8.3</td>
<td></td>
</tr>
<tr>
<td>12.4</td>
<td>4</td>
<td>8.4</td>
<td></td>
</tr>
<tr>
<td>14.7</td>
<td>4</td>
<td>10.7</td>
<td></td>
</tr>
<tr>
<td>14.9</td>
<td>4</td>
<td>10.9</td>
<td></td>
</tr>
<tr>
<td>13.42</td>
<td>4</td>
<td>9.42</td>
<td></td>
</tr>
</tbody>
</table>

V. 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.

REFERENCES

http://www.iii.org/media/hottopics/insurance/test4/

[2] Immobiliser, WHATCAR.

http://www.datadotdna.com/dt1_technology_ouretechs_dot.htm

http://www.stavc.nl/pdfdb/publicaties/identificationreport.pdf


http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html


http://www.semiconductors.bosch.de/en/20/can/index.asp

http://www.can-cia.org/can/