An intrusion defense approach for vehicle electronic control system

Zhou Qin and Fei Li
College of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China
E-mail: joe7in@qq.com

Aiming at the information security issues of modern smart car while communicating with outside, we analyze the security flaws of vehicle's electronic control system and investigate numerous common attacks. Applying Intrusion Detection mechanism, we propose a network anomaly Intrusion Defense Approach for vehicle. An attack example is captured to demonstrate the detection progress in detection phase, and a dynamic response strategy is designed in decision phase and discussed using three exemplarily selected scenarios.

Keywords: Automotive; Information Security; Intrusion Detection.

1. Introduction

Vehicle electronic control system utilizes CAN-bus as its basic communication network which connects all the sensors and ECUs. But all the data in CAN-bus are unencrypted and lack of identity authentication. So anyone can fetch CAN data and send malicious data to each ECU if he connects with CAN-bus. Nowadays, more and more vehicles access to internet to get more information service, which can put fragile system to a viral environment.

K.Koscher[1] introduced a method to hack the car. He connected to the car with OBD-II interface, and hacked the car using only some segment codes. Then he can shut down the brake system, revamp speedometer, turn on the air-conditioner, turn on the music player and lock the door with driver inside. Miller C and Valasek[2] showed how to remotely attack a car which is hundreds kilometres away. By tampering the ECU's firmware (ROM) remotely, they can revamp speedometer, and control the car's windows up and down. Samy Kamkar[3] used homemade hacking-kit Ownstar successfully bypassed the authentication and entered four telematics service provider companies' servers.

In the only researches of defensive methods, most of them focus on encrypting the communication progress, include communications with outside and communications between ECUs. Li Shu-jing[4] implemented SSL protocol

to encrypt the data exchange between vehicle terminal and server. After some simulation tests, this method was proved useful. Zhu Xiao-ling[5] introduced a non-trusted center model to in-vehicle communication which is based on secure decode without trusted center, and designed a decryption model of vehicle's black box which based on secure sharing and elliptic curve cryptography. Wolf, Weimerskirch, and Paar[6] proposed a countermeasure that installing a gateway in the car and deploying PKI (*Public Key Infrastructure*) to encrypt the communication and deliver shared keys. From the above, we can see that encrypting the transporting data can make data safer, but the progresses of encryption and decryption spend numerous time and resources which can delay the communications. The latency of driving commands will make the car out of control which is life-threatening. In addition, in order to encrypt the communication, all the ECUs will be equipped with the ability of decryption and encryption, which would be a big challenge when reconfigure used cars.

In this paper, we introduce an intrusion detection approach for vehicle's electronic control system. We set a detection device inside the vehicle's electronic control system, monitoring the traffic to find the intrusion. It is no need to change the CAN-bus's topological structure, modify ECU, and disturb communication. When the device find the intrusion, it will follow the decision rules to alert driver and give some useful advice to avoid the risk.

2. Schema

Intrusion detection is already a well-developed technology which contains of signature based detection and anomaly based detection. When apply signature based detection, system should persistently maintain the "black list" until it covers all novel attack types. It can't detect unknown attacks, but anomaly based detection can. Because of endless attack modes on vehicle's electronic control system, we choose anomaly based detection. Depend on detection components' location, intrusion detection divide into host based and network based detection. Host based component could be placed on sensitive ECUs to have direct view on the internal activities. In this way they would be able to detect malicious code that has been injected during runtime. Network based components could attach to an entire bus system in form of a separate ECU or as part of gateway. They could scan the on-board communication for indications of active attacks. Considering the cost, we choose network based anomaly intrusion detection. As shown in figure 1, the detection component accesses to gateway which is the central data controller. We can monitor all bus dataflow by access to gateway.

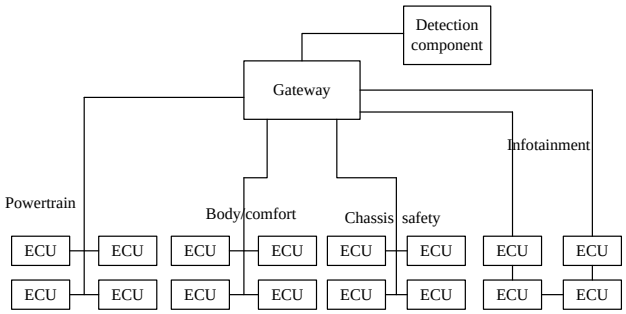

Fig. 1 vehicle's electronic control system's topologic structure

3. Detection Phase

We will show you the basic anomaly based intrusion detection approach using a practical example. The attacked component is the warning light system. As table 1 shows, ECUs usually trigger the warning lights by periodically sending a sequence of CAN messages, which has ID (0x327) and contains a flag to turn on or shut down the indicator lights.

Tab. 1 Messages recorded during normal operation

Time(sec)	ID(Hex)	Data	Command
210.116	327	9	Turn off
210.156	327	9	Turn off
210.167	327	99	Turn on
210.217	327	99	Turn on
210.267	327	99	Turn on
210.317	327	99	Turn on
210.367	327	99	Turn on
210.417	327	99	Turn on
210.467	327	99	Turn on
210.517	327	99	Turn on
210.528	327	9	Turn off
210.578	327	9	Turn off

The attack aims at suppressing the warning lights (when driver put on the break, or the car was forced invaded). Hacker sends commands by malicious component which access to the target bus network, or use an additionally attached device. Because of the CAN's broadcast character, it is impossible to delete or modify existing message. When the malicious component observers a command message on the bus to turn on the warning lights, it instantly react by generating a copy of message telling the responsible ECU to turn off them again.

As shown in table 2, the normal command message is periodically sent every 0.050 seconds, but the spoofed message was sent right after the normal

one in about 0.002 seconds. Since the original messages are immediately followed by the opposite commands, and the receiver ECU doesn't check the sender's authentication, so the spoofed message were smoothly executed. So the lights stay completely dark, or occasionally flicker for a short moment due to latency.

Tab. 2 Messages recorded during the attack

Time(sec)	ID(Hex)	Data	Command
211.031	327	9	Turn off(real)
211.081	327	9	Turn off(real)
211.092	327	99	Turn on(real)
211.094	327	9	Turn off(spoofed)
211.142	327	99	Turn on(real)
211.144	327	9	Turn off(spoofed)
211.192	327	99	Turn on(real)
211.202	327	9	Turn off(spoofed)
211.242	327	99	Turn on(real)
211.244	327	9	Turn off(spoofed)

This attack can be detected by a network based IDS (Intrusion Detection System) without insight to the internal activities of any ECU. Let the system tracks all the message having the ID of 0x327 and evaluates two different characteristics:

- The frequency of normal messages. As shown in the table 1, it is 0 or 21 times per second during normal operation. The attack will be detected when the times per second up to 35.
- The semantical meaning of the previous 8 messages. In normal operation, this value only changes 0-1 times during the interval. When it up to 4 inversions, system can detected it.

4. Decision Phase

Considering drivers have little knowledge about IDS, so it is natural to design the system as automatic response mode. In this way, without drivers' intervention, the system choose the right prepared strategy. But the vehicle's high security requirements prohibit to do so. Considering the responsibility of accidents, final decisions regarding control safety of the vehicle are only to be made by the driver. This is written in laws of many countries. So the interactive system should be designed very carefully.

As shown in figure 2, we divided the common dangers into 3 levels: non-critical level, critical level, and severe level. Dangers like stealing private information, interfering Body Comfort System (e.g. make car window up and down, swing windscreen wiper), interfering Infotainment System (e.g. switch radio, switch music playing, play picture), belong to level 1 due to they are not life threatening. Dangers like interfering Powertrain System (e.g. accelerate the speed, steer the wheel), interfering Chassis Safety System (e.g. make car can't move by repeatedly send brake command) belong to level 2 due to they are life threatening. When a car was attacked while running in the highway, there is no time for driver to take action, so the attack may lead to a serious accident. Dangers like this occurs when car under difficult condition belong to level 3.

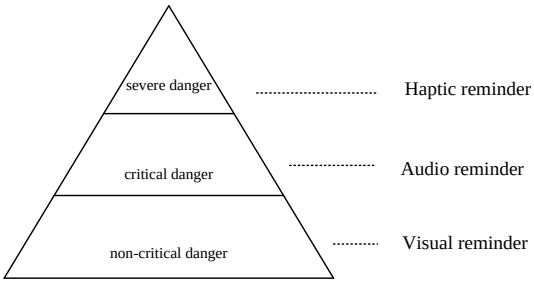

Fig. 2 Three stage respond strategy

To illuminate how to choose the suitable strategy, we introduce three exemplary scenarios as follows. We assume the following preconditions: A hacker, who wants to steal sensitive data or danger the safety of driver, has infected an ECU of the car with malicious code. Once the infected device interact with others in an abnormal way, the detection component may observe it.

- Scenario 1: steal sensitive information. When the hacker get what they want, he would transmit this to the outside using V2V (vehicle to vehicle) or V2I (vehicle to infrastructure) communication. If the IDS detects these, it might remind driver of data leakage warning with text show on screen and advise driver to check his car at a service station soon.
- Scenario 2: DoS attack under regular conditions. The hacker attack the Electronic Stability Control (ESC) with Denial of Service method in order to disable it. Since the ESC only works in exceptional cases, the attacks in the normal stage may not be discovered. Once detected, a warning text and sound could be made to alarm driver to stop the car in safe area, and call workers to fix the threat.
- Scenario 3: DoS attack under difficult conditions. When a car running in the road with loud noise and strong light, drivers may not notice the warning

light and warning voice. The system hasn't wait the response after it sent alarms repeatedly, and then raise the response strategy up to level 3. The system generate some command to shake the wheel or seat to remind driver to watch the warning and take action immediately.

5. Summary and Future Work

In this paper, after we analyze the security flaws of current automotive, we propose an approach that transmit the mature IDS of PC to automotive, and show the procedure by some examples. Considering the complicated driving environment, we propose a dynamic alert processing strategy which choice different method determined by the severity of the detected incident as well as the current driving and environmental conditions. Being the early exploring of future automotive information security, the proposed defense strategy is humanized, efficient, and can be widely implemented.

In future, we plan to apply artificial intelligence algorithm (e.g. artificial neural network) to improve the detection efficiency and expand the detection range.

References

1. K. Koscher, Czeskis A, Roesner F, et al. Experimental security analysis of a modern automobile [C]2010 IEEE Symposium on Security and Privacy. Piscataway, USA:IEEE Computer Society,2010:447-462.
2. Miller C, Valasek C. A survey of remote automotive attack surfaces [J]. BlackHat USA, 2014.
3. Kamkar, S. "Drive It Like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars." Presentation at DEFCON 23 (2015).
4. Li Shu-jing, CHEN Si-guo, LIU Yan-heng,et all. Trusted remote repair framework and implementation of vehicular software.[J]Computer Engineering and Design.2011,32(3):1074-1078(In Chinese).
5. Zhu Xiao-ling, Hou Zheng-feng, Lu Yang. Secure decoding of vehicle black box based on secret sharing without trusted center. [J] Journal of Electronic Measurement and Instrument. 2011,25(3):279-284(In Chinese).
6. Wolf M, Weimerskirch A, Paar C. Security in automotive bus systems [J]. Proceedings of the Workshop on Embedded Security in Cars , 2004.