2020 IEEE International Conference for Innovation in Technology (INOCON)
Bengaluru, India. Nov 6-8, 2020

CYBER SECURITY IN VEHICLE COMMUNICATION

Manjula R Parmar
Dept. ECE
RV College of Engineering
Bengaluru, India
manjularparmar@gmail.com

M Uttara Kumari
Dept. ECE
RV College of Engineering
Bengaluru, India
uttarakumari@rvce.edu.in

Ramesh S N
ESD-NR
RBEI
Bengaluru, India
Ramesh.Naidu@us.bosch.com

***Abstract*—In the Automotive Industry, cyber security implementation is low. A car has multiple Electronic Control Units (ECUs) and every ECU communicates a huge number of messages to another ECU through Control Area Network (CAN). If the hacker invades the system, then it is like an open source of resources and any amount of valuable information can be manipulated. This can lead to a great damage. This is a motivation to verify various existing cyber security features, understand the system and then implement the cyber security features. In this paper, key slot verification design, maximum authoritative counter verification design and user mode implementation have been discussed. The Automotive Open Source Architecture (AUTOSAR) platform is used for development in the automotive industry.**

***Keywords* – Electronic Control Unit (ECU), Control Area Network (CAN), Automotive Open Source Network (AUTOSAR), key slot, authoritative counter, supervisor mode and user mode.**

I. INTRODUCTION

In recent years, as it is seen that the mechanical system are being replaced by the electronic components. Now, cars are no longer a mechanical device and an electronic device, the connectivity makes it an Internet of Things (IOT) device. In the automotive industry, a single car has many Electronic Control Units (ECUs) [4]. These ECUs have been programmed to execute many functionalities. Cyber security earlier were only with computers for various attacks of the hacker. Nowadays, there are many cyber security features implemented on non-computers, such as, house appliances, transportation, utilities and various industries. Many factories and industries are gaining grounds as every device is moving towards automation and IOT. As the connectivity is increasing, the IOT concepts are widely being used in the automotive industry. This increase in connectivity also increases the cyber risk which is a serious issue and a social concern. The ECU is programmed with many functionalities which is used in cars, such as driver assistance, air bags and many other applications. These ECUs are connected to each other through Control Area Network (CAN) [3], which is the communication protocol widely used in the vehicles. There are many messages transmitted on the CAN bus and certain message are very critically related to the safety. If these safety signals are manipulated on the CAN bus, the effect on the vehicle is dangerous and no security in the vehicles would lead to a huge risk.

II. THEORY AND METHODOLOGY

A. *SECURE COMMUNICATION*

The transmitter ECU and the receiver ECU are connected by the CAN bus. The transmitter has the Hardware Security Module (HSM), which is capable of calculating Message Authentication Code (MAC) [7]. The input to the HSM to calculate MAC is the timestamp and the message or payload. The MAC is generated and sent to the receiver ECU along with the message and timestamp. The receiver is also associated with the HSM, which has the capability to verify MAC which has been sent by the transmitter through the CAN bus. Once the MAC is verified by the HSM, the message is accepted by the receiver.

In this case the timestamp is shown as 7'O clock as shown in Fig 1. There is a hacker ECU monitoring the bus and intentionally it has captured the message on the bus. When the hacker ECU captures the message, it is obvious that the MAC and the timestamp 7'O clock is also captured from the bus. Now, the hacker ECU sends the same message at a different timestamp. The different timestamp in the Fig 1, is 9'O clock. At 9'O clock, the hacker ECU sends the same message through the CAN bus to the receiver. When the receiver is verifying the MAC, the timestamp doesn't match. The receiver do not have information about the different timestamp. Therefore, the message is rejected.

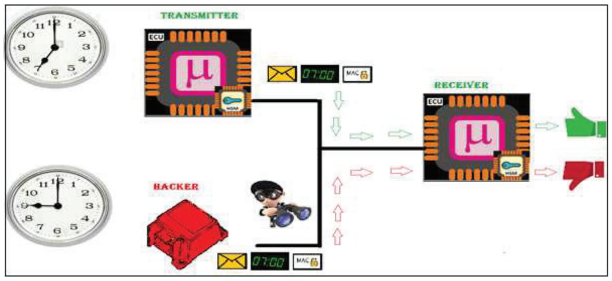


Fig. 1. Message Authentication

978-1-7281-9744-9/20/$31.00 ©2020 IEEE

Now, there can be an instance that there is time delay between transmitter and receiver and the message along with MAC and timestamp reaches the receiver with some delay. There would not be any issue as the timestamp is nothing but a counter. The counter value by which MAC is calculated and the information at the receiver about the counter would remain the same. The counter value at the receiver would not increment. Hence, even if there is a certain delay on the bus, MAC will be verified by the receiver.

B. CIPHER BASED MESSAGE AUTHENTICATION CODE

Cipher based Message Authentication Code (CMAC) is an algorithm used for MAC generation and verification. This algorithms processed in the Hardware Security Module (HSM), in the ECU. CMAC algorithm is coupled with the corresponding key slot of the transmitter as shown in the Fig 2. The payload or the message and the anti-replay counter is given as the input to the CMAC algorithm for MAC generation. This is the counter associated with the secure message. Therefore, the inputs to CMAC algorithm is payload and anti-replay counter. Every secure transmitter message is associated with a key slot.

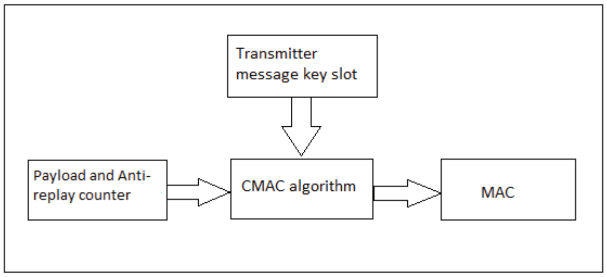


Fig. 2. CMAC Generation

The key slot is also known as Key ID [5]. The Key ID is the slot where keys are provided. The keys are given in the key slot provided and then MAC only flag is set. There is certain internal value for MAC Only flag which is set. This flag is used for MAC generation. These generated keys are coupled to the CMAC algorithm which would generate MAC with payload and anti-replay counter as inputs. The value used for MAC verification is different and that flag value can only verify MAC. The secure receiver messages are given different Key ID compared to the secure transmitter message. The MAC Verification value is set after the keys are provided. The MAC Verification Flag has an internal value which is set. This process would generate the keys for MAC Verification. Therefore, these keys are coupled to CMAC layer, either for MAC generation or MAC verification.

C. USER MODE AND SUPERVISOR MODE

The two privilege mode operations are the supervisor mode and the user mode. The supervisor mode will have access to all resource control operation. It is like the administrator which has read, write and executable permission all the memory location. All the task run in a single platform and none except the administrator can change can change any task or the code or any configuration. This makes the system very rigid. In the automotive industry, one of the electronic devices in the cars, is ECU. This ECU runs only in the supervisor mode. The registers and memory location can be accessed only in the supervisor mode. All the application run in the supervisor mode.

When the processor is made to run on the user mode it would allot restricted access to the system. If user mode is implemented, then in this mode, the user will have limited access to resource control operation and certain section of memory location will have restricted permission. To understand the switching from supervisor mode to user mode and retrieve back to supervisor mode. It is important to understand the Machine State Register (MSR). This MSR defines the state of the processor. The MSR is a 32 bit register. The Problem State Register (PR) bit in the MSR, indicate whether the processor is in user mode or the supervisor mode. If the PR bit = 0, the processor is in supervisor mode. If the PR bit = 1, the processor is running in the user mode.

The ECU runs in supervisor mode. One of the function is to be defined to run in user mode. Therefore, the code is developed in the function, for the ECU to run that particular function in user mode. When the code is being executed, the PR bit of the MSR is set to 1 without disturbing any other bit in the MSR. The ECU is now running in the user mode after changing the PR bit to 1. If the ECU has to switch back to supervisor mode, the system call or the interrupt has to be executed, to change the PR bit of the MSR register to zero.

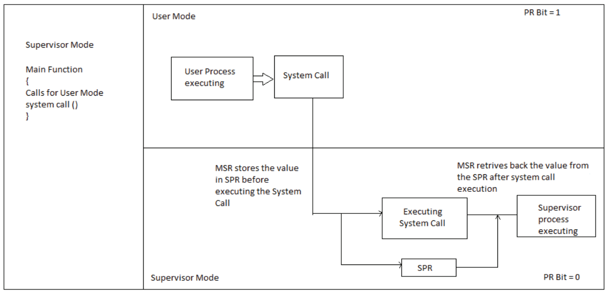


Fig. 3. User Mode Concept

The MSR stores its value in the Special Purpose Register (SPR), while executing the system call. The SPR is made to change the PR bit location of the MSR value to 1. When MSR retrieves its value from the SPR. The instruction to it, is to stay in supervisor mode, as the PR bit of the MSR would be 1. The concept proves that there can be switching from supervisor mode to user mode and vice versa. The user and supervisor mode can be successfully implemented in the ECU by using this concept.

III. DESIGN

The design for three features of cyber security will be explained in this section, the first two design will prove the existing code is working well. The third design is the implementation of the user mode in the ECU.

A. KEY SLOT VERIFICATION

Verify that no single ECU shall use the same key slot within the security peripheral to both generate and verify MACs. The ECU is calibrated to generate valid non-zero MAC. Distinct keys for MAC generation and verification have been used.

ACTIONS

Trigger ECU to transmit secure message. Select secure transmitter message to be sent by the ECU on the bus and form the necessary data to be sent to the MAC Generate interface. Manipulate the application code to send the data in key slot number 4 to the MAC Generate interface with key slot number corresponding to the Receiver message key slot number. The design for key slot verification is as shown in the Fig 4.

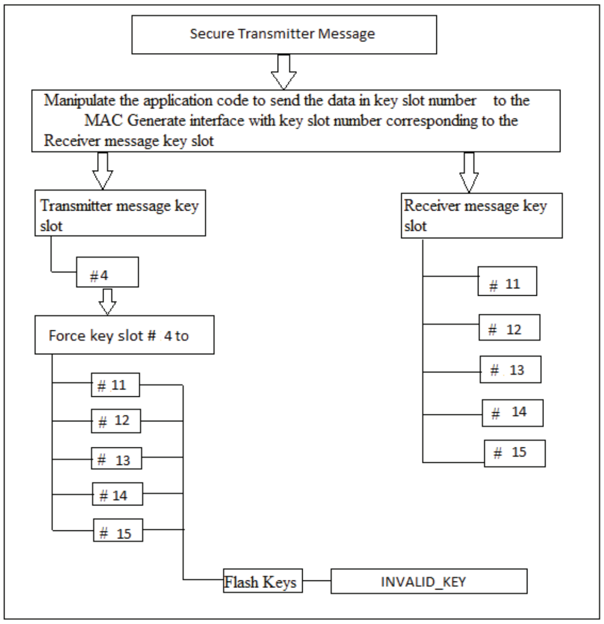

Secure Transmitter Message
Manipulate the application code to send the data in key slot number to the MAC Generate interface with key slot number corresponding to the Receiver message key slot
Transmitter message key slot
#4
Force key slot # 4 to
# 11
# 12
# 13
# 14
# 15
Receiver message key slot
# 11
# 12
# 13
# 14
# 15
Flash Keys
INVALID_KEY

Fig. 4. Key Slot Verification Design

The design shows that, key slot number 11, 12, 13, 14, 15 are the receiver message key slot number and these key slots are forced on key slot number 4, one at a time. The MAC generate keys are flashed which were associated with the key slot 11, 12, 13, 14, 15. These keys should be generated. This action will trigger error. The error being INVALID KEY. All the key slots are verified and the application code provides the same error every time different receiver key slots are used.

B. MAXIMUM AUTHORITATIVE COUNTER VERIFICATION

Ensure that the ECU set a DTC when the Authoritative counter reaches its maximum value and send zero MACs.

ACTIONS

Trigger ECU to transmit secure message. Verify that the ECU is sending all the transmitter messages it supports. Select a secure transmitter message and manipulate the application code to set the corresponding authoritative counter to its maximum value.

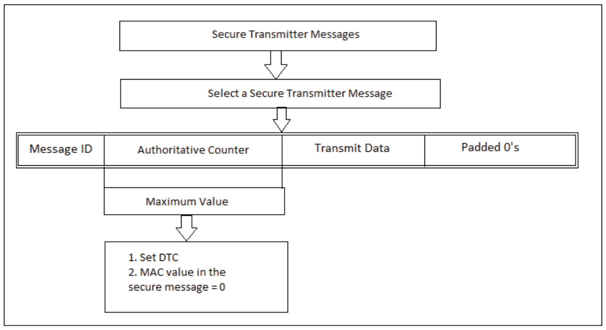


Fig. 5. Maximum Authoritative Counter Verification Design

The authoritative counter is the internal counter associated with the secure transmitter message. If the counter reaches its maximum value, then the application code should set the Diagnostic Trouble Code (DTC). It is also observed that the MAC Value in the selected Secure Transmitter Message should be zero. The DTC is the set when there is an error in the code. The DTC can be configured to be set for various errors by this the application layer intimates that certain things are not working as per expected.

IV. USER MODE VERIFICATION

Initially the ECU will be executing functions in supervisor mode. At the end of supervisor mode functions a chain task is introduced and a user mode defined function is given as a parameter. The functions cannot access the registers in user mode, as they are untrusted functions, so the wrapper is being introduced as shown in Fig 6, which shows the user mode implementation design.

These are untrusted functions mapped to the trusted functions to call the original functions to be executed in user mode. When the wrapper is called in the function. It should be configured in the Real Time Operating System (RTOS), the functions are configured as trusted functions.

This gives access to registers and functions to execute in user mode. Now, to switch the ECU running in the user mode to supervisor mode, a chain task at the end of user mode function is called and the parameter passed to it is a supervisor

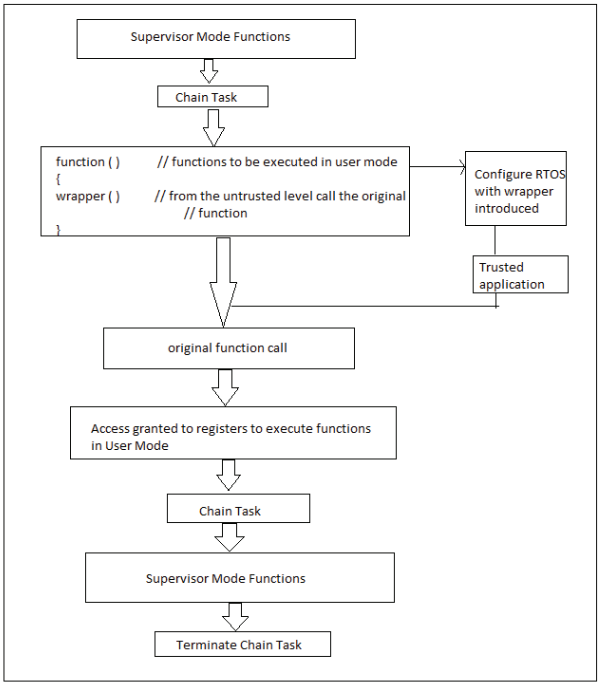

Supervisor Mode Functions
Chain Task
function ( )
{
wrapper ( )
}
// functions to be executed in user mode
// from the untrusted level call the original
// function
Configure RTOS with wrapper introduced
Trusted application
original function call
Access granted to registers to execute functions in User Mode
Chain Task
Supervisor Mode Functions
Terminate Chain Task

Fig. 6. User Mode Implementation Design

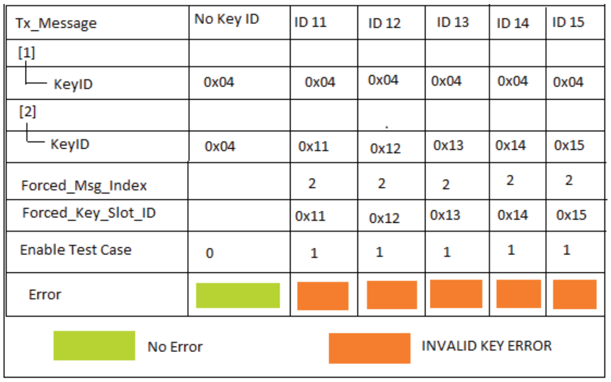
mode function. Therefore, the ECU would run in supervisor mode. At the end of the execution of the function, a terminate chain task is called, which would terminate this process.

V. RESULTS

The results of all the three designs are shown in this section.

A. *KEY SLOT VERIFICATION RESULTS*

The CAN bus is normally transmitting all the transmitter and receiver messages, as configured to the ECU. The messages would contain their original Key Slot assigned to every message. The selected secure transmitter message contain the key slot ID as 4, this is originally assigned Key ID. There would be no error. The test case is also not enable.



Tx_Message	No Key ID	ID 11	ID 12	ID 13	ID 14	ID 15
[1]						
KeyID	0x04	0x04	0x04	0x04	0x04	0x04
[2]						
KeyID	0x04	0x11	0x12	0x13	0x14	0x15
Forced_Msg_Index		2	2	2	2	2
Forced_Key_Slot_ID		0x11	0x12	0x13	0x14	0x15
Enable Test Case	0	1	1	1	1	1
Error	🟩	🟧	🟧	🟧	🟧	🟧

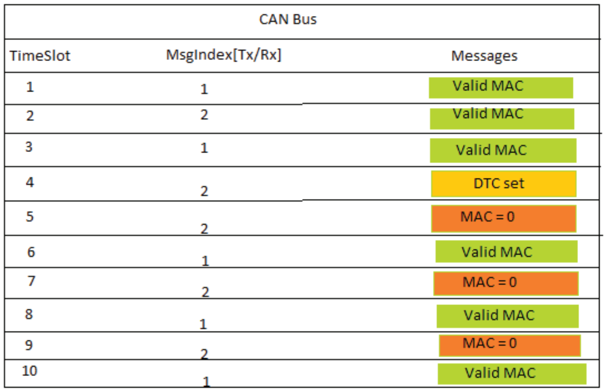
🟩 No Error 🟧 INVALID KEY ERROR

Fig. 7. Result of Key Slot Verification

Now, the test case is enabled and receiver key slot ID, one at a time is forced to the application code for a particular selected transmitter message. In the Fig 7, the receiver key slot number 11, 12, 13, 14, 15 is forced. After the keys are provided, the error is raised by the application code. The error raised is INVALID KEY error. In this case, transmitter message 2 is forced to accept the changed key slot 11, 12, 13, 14, 15. All the receiver key slot ID gives the same error, hence, it would prove that no single ECU can function, when the receiver key slot is forced in place of the transmitter key slot.

B. *MAXIMUM AUTHORITATIVE COUNTER RESULTS*

The transmitter index 2 is selected to make the authoritative counter to the maximum. This would result in setting the DTC for secure transmitter message 2 and the MAC Value transmitted is also zero. This is been shown in the Fig 8.



CAN Bus

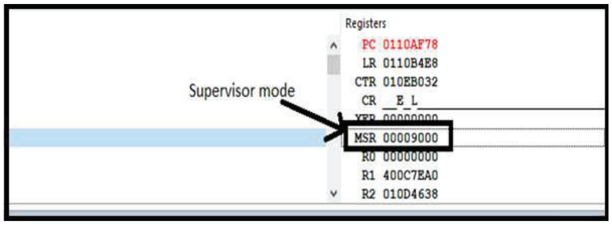
TimeSlot	MsgIndex[Tx/Rx]	Messages
1	1	Valid MAC
2	2	Valid MAC
3	1	Valid MAC
4	2	DTC set
5	2	MAC = 0
6	1	Valid MAC
7	2	MAC = 0
8	1	Valid MAC
9	2	MAC = 0
10	1	Valid MAC

Fig. 8. Results of Maximum Authoritative Counter Verification

The results prove that the test cases are verified and successful. The DTC is also being set and the MAC Value for the particular message is zero. Other messages will normally execute a valid MAC.

C. *USER MODE RESULT*

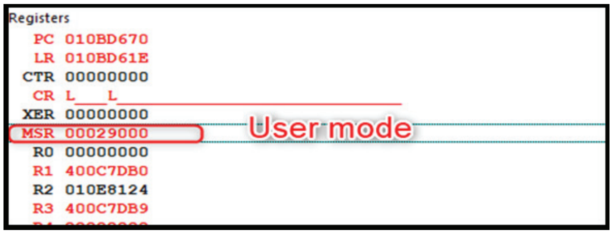
The results for Supervisor Mode is shown in Fig 9. The register which defines the state of the ECU is the MSR. In the Fig 9, the value of the MSR is 00009000. This shows that the seventeenth bit is 0, which is the PR bit defining supervisor mode.



```
Registers
 PC 0110AF78
 LR 0110B4E8
CTR 010EB032
 CR __E_L
XER 00000000
MSR 00009000
 R0 00000000
 R1 400C7EA0
 R2 010D4638
```

Fig. 9. Result of Supervisor Mode

The MSR register value is 00029000 as shown in the Fig 10. This clearly indicate that the PR bit of the MSR is equal to 1. This is representing that the processor is running in user mode. Fig 10.



```
Registers
  PC 010BD670
  LR 010BD61E
 CTR 00000000
  CR L   L
 XER 00000000
 MSR 00029000
  R0 00000000
  R1 400C7DB0
  R2 010E8124
  R3 400C7DB9
```

Fig. 10. Result of Supervisor Mode

All the other bits are not being effected and the ECU has the ability to switch and execute functions in user and supervisor mode. It is even able to access the privileged register and memory locations required.

VI. CONCLUSION

Cyber Security was only seen in computers due to high rate of attacks. Now, cyber security in vehicle communication has become the integral part of the automotive industry. Without key there is no security. Therefore, keys play an important role in the HSM concerning the security. There are only three features discussed, designed and implemented, but cyber security in automotive industry is a huge study. There are many features implemented, and every feature requires a deep understanding of the platform which is AUTOSAR, CAN Communication and many other features. Once these feature are understood then, the other security feature can be designed and implemented.

VII. ACKNOWLEDGEMENT

The writers would like to thank Robert Bosch Engineering and Business Solutions for this platform and support during the entire work process.

VIII. REFERENCES

[1] Jin Hyun Kim, Inhye Kang, Sungwon Kang and Abdeldjalid Boudjadar “A Process Algebraic Approach to Resource – Parameterized timing Analysis of Automotive Software Architecture”. IEEE Transaction on Industrial Informatics, VOL. 12, NO. 2, April 2016.

[2] Simon Schliecker, Jonas Rox, Mircea Negrean, Kai Richter, Marek Jersak and Rolf Ernst, “System Level Performance Analysis for Real-Time Automotive Multicore and Network Architecture”. IEEE Transaction on Computer-Aided of Integrated Circuits and System, VOL. 28, NO. 7, July 2009.

[3] Yong Xie, Gang Zeng, Ryo Kurachi, Hiroaki Takada and Guoqi Xie, “ Security/Timing- Aware Design Space Exploration of CAN FD for Automotive Cyber Physical Systems”. IEEE Transaction on Industrial Informatics, VOL. 15, NO. 2, February 2019.

[4] Wonsuk Choi, Hyo Jin Jo, Samuel Woo, Ji Young Chun, Jooyoung Park and Dong Hoon Lee, “Identifying ECUs Using Inimitable Characteristics of Signal in the Control Area Network”. IEEE Transaction on Vehicular Technology, VOL. 67, NO. 6, JUNE 2018.

[5] Hengchuan Tan, Maode Ma, Houda Labiod, Aymen Boudguiga, Jun Zang and Peter Han Joo Chong, “ A Secure and Authentication Key Management Protocol (SA-KMP) for Vehicular Networks”. IEEE Transaction on Vehicular Technology, VOL. 65, NO. 12, December 2016.

[6] Xui Yi, San Ling and Huaxiong Wang, “Efficient Two Server Password Only Authenticated Key Exchange”. IEEE Transaction on Parallel and Distributed Systems, VOL. 24, NO. 9, September 2013.

[7] Xiaofu Wu, Zhen Yang, Cong Ling and Xiang-Gen Xia, “Artificial-Noise-Aided Message Authentication Codes with Information-Theoretic Security”. IEEE Transaction on Information Forensics and Security, VOL. 11, NO. 6, June 2011.