CAN Bus Risk Analysis Revisit

Hafizah Mansor, Konstantinos Markantonakis, Keith Mayes

CAN Bus Risk Analysis Revisit

Hafizah Mansor, Konstantinos Markantonakis, and Keith Mayes

Information Security Group, Smart Card Centre,
Royal Holloway, University of London
Hafizah.Mansor.2011@live.rhul.ac.uk,
{K.Markantonakis,Keith.Mayes}@rhul.ac.uk

Abstract. In automotive design process, safety has always been the main concern. However, in modern days, security is also seen as an important aspect in vehicle communication especially where connectivity is very widely available. In this paper, we are going to discuss the threats and vulnerabilities of a CAN bus network. After we have considered a number of risk analysis methods, we decided to use FMEA. The analysis process allowed us to derive the security requirements of a CAN bus. Experimental setup of CAN bus communication network were implemented and analysed.

Keywords: Risk analysis, ECU, FMEA, CAN bus network

1 Introduction

Safety is always the first priority in automotive application. With the advanced technologies and introduction of multiple intelligent applications for automotive, security is now a very crucial criteria to ensure the safety and reliability of a car.

In modern vehicles, the operations are controlled by embedded microcontrollers called ECUs (Electronic Control Units). These ECUs are interconnected through multiple network buses, such as Controller Area Network (CAN) [9], Media Oriented Systems Transport (MOST) [13], Local Interconnect Network (LIN) [14] and FlexRay [12].

This paper will discuss the risk analysis of a CAN bus network using Failure Mode and Effect Analysis (FMEA). The objective of this paper is twofold. While analysing the security requirements on CAN bus network, we also want to highlight the method we used for risk analysis.

The next section will discuss background and related works on vulnerabilities and threats on vehicular networks, their method for risk analysis and their proposals for secure solutions. Our CAN bus risk analysis using FMEA is decribed in the following section. From the analysis, we discuss the security requirements of a CAN bus network. The last section describes the experimental CAN bus implementation that we conducted with basic communication and incorporating crypto operations to introduce security to the CAN bus communications.

1.1 Background

Since in-car network connectivity is becoming very widely used and available, people are interested on how this may improve the operations of a vehicle. Thus, some parties have higher motivation, whether to gain financial profit or recognition by attacking the system. This is even easier by the availability of many interfaces (On board diagnostic (OBD), Bluetooth, wireless) and the weaknesses proven [10][5][8] in the current system.

1.2 Related Work

In this section, we are going to discuss a number of industrial projects and their security requirements analysis methods.

The focus of EVITA project [2] was security for onboard networks. In their security requirement analysis, they identified use cases and threat scenarios to obtain the security requirements. Hence, they designed a secure onboard architecture and secure onboard communications protocols.

In the SeVecom project [1], they introduced cluster analysis for security requirement analysis process [11]. The objective of SeVecom project was to find a future-proof solution to the problem of vehicle to vehicle (V2V) and and vehicle to infrastructure (V2I). Focusing on communication specific to road traffic, it proposed a security architecture and security mechanisms by proposing cryptographic algorithms and secure device for vehicular networks.

The PRESERVE project [4] combines the results of several projects such as SeVecom, PRECIOSA (Privacy Enabled Capability in Co-operative Systems and Safety Applications) [3], EVITA and OVERSEE. The objective of this project is to create an integrated vehicle to X (V2X) security architecture. In this project, they use the method introduced by [11] to obtain their security requirements and countermeasures [15].

In European Telecommunication Standard Institute (ETSI), a standard for Intelligent Transport Systems (ITS) was made to ensure efficient and reliable communication in transport system. In [6], the ETSI (ITS) document lists seven steps to identify risks using threat, vulnerability and risk analysis (TVRA). In the TVRA method, the security requirements are listed first, then only the threats to the requirements are analysed.

2 Risk Analysis

There are different methods and tools available to conduct a risk analysis of a system. In this paper, we conduct our risk analysis based on FMEA. In FMEA, risk is the product of the probability that an event (potential failure mode) may occur in a specified system and the impact on the system if the event occurs and to what extent the event can be detected in the existing environment.

2.1 CAN Bus Risk Analysis Using FMEA

In this security risk analysis, we take the approach of viewing the risks of a CAN bus from four different views, i.e car lifecycle, CAN bus operations, entities involved and ECUs. While the lists are not exhaustive, our analysis mainly focuses on common use cases without V2V and V2I communications. From the different views of risks, we can highlight the risk levels and thus propose proper mitigation actions to overcome the threats and vulnerabilities accordingly.

Table 1. Probability Rating

Probability of failure	Failure	Rating
Very High	>=1 in 2	10
	1 in 3	9
High	1 in 8	8
	1 in 20	7
Moderate	1 in 80	6
	1 in 40	5
	1 in 2,000	4
Low	1 in 15,000	3
	1 in 150,000	2
Remote	1 in 1,500,000	1

Table 2. Severity Rating

Effect	Severity of effect			Rating
	Safety	Reliability	Financial	
Catastrophic	Multiple deaths	Overall system failure	Total loss	10
Extreme	At least one death	System failure	Extremely high loss	9
Very High	Major injury	Partial system failure	Very high loss	8
High	Bad injury	Very bad distraction	High loss	7
Moderate	Moderate injury	Distraction	Moderate loss	6
Low	Small injury	Loss of comfort	Small loss	5
Very low	Very small injury	Uncomfortable	Very low loss	4
Minor	Minor injury	Minor loss of comfort	Minor loss	3
Very Minor	Very minor injury	Very minor loss of comfort	Very minor loss	2
None	No effect	No effect	No effect	1

In FMEA, the ratings for probability, severity, detection and risk depend on the process or product being analysed. In this analysis, the ratings scale is an initial starting point that could be refined following discussion with industry. Tables 1, 2, 3 are ratings related to probability, severity and detection respectively.

Table 3. Detection rating

Detection	Likelihood of detection	Rating
Absolute uncertainty	Control cannot detect	10
Very remote	Very remote chance the control will detect	9
Remote	Remote chance the control will detect	8
Very low	Very low chance the control will detect	7
Low	Low chance the control will detect	6
Moderate	Moderate chance the control will detect	5
Moderately high	Moderately high chance the control will detect	4
High	High chance the control will detect	3
Very high	Very high chance the control will detect	2
Almost certain	Control will detect	1

Table 4. Risk level

Risk level	RPN	Label
Unacceptable	301<=RPN<=1000	U
High	201<=RPN<=300	H
Moderate	101<=RPN<=200	M
Low	1<=RPN<=100	L

Table 4 assigns the risk priority number (RPN) values, which is the product of probability, severity and detection, to the different risk levels.

Car life cycle Car life cycle starts from the manufacturing state, followed by selling, use by owner, reselling and forensics. In each state of the life cycle, there are many different potential failure modes. Table 5 shows the FMEA for car life cycle. From the analysis, we conclude that the highest risk is during the usage of the car by the user or the owner. During this state of life cycle, the CAN bus network is most vulnerable whether to attacks or to any failure modes that might occur deliberately or not.

Entities There are a number of different entities involved in a car lifecycle. They are the car manufacturer, car parts supplier, firmware developer, technician and mechanic at workshop, car agent and dealer, insurance agent, owner, user and interested parties in car hacking (car manufacturing competitor, hobbyist, researcher, technical enthusiast, thief and terrorist). From the analysis, the car manufacturer and the insurance agent are seen as low risk entities, while car parts supplier is considered at moderate risk. Other entities are found to be at unacceptable risk level.

CAN bus operations The risks are also analysed from the weaknesses of CAN bus operations that might be used by the attacker to cause failure modes. For example, for message reception, an attacker can cause failure by making improper filtering. Other general weaknesses that can be threats to the CAN bus are the broadcast nature of the network, priority bus based arbitration and unlimited number of nodes. These manipulations can cause severe effects

Table 5. FMEA of car life cycle

Life cycle	Failure mode	Mechanism		Effect	Probability	Severity	Detection	RPN	Risk level	Mitigation
		Entity	Why							
Car manufacturing	Wrong parts	Manufacturer	Financial/ negligence	safety/ comfort	4	7	2	56	L	Parts authentication
	Counterfeit parts			safety/ comfort	4	8	2	64	L	Parts authentication
	Incompatible firmware			safety/ comfort	8	6	4	192	M	Firmware version control
	Bad parts			safety	4	8	2	64	L	Parts authentication
Car selling	Change of firmware	Car agent/ Technician	Financial	safety/ comfort	1	8	7	56	L	Firmware version control
	Broken wire			safety/ comfort	1	8	7	56	L	ECUs authentication
	Change of data in ECU			safety/ comfort	1	8	7	56	L	Authentication, data integrity
Service	Change of firmware	Owner/ Technician	Financial	safety/ comfort	7	9	5	315	U	Firmware version control
	Change of data in ECU			safety/ comfort	5	7	5	175	M	Authentication, data integrity
	Counterfeit parts			safety/ comfort	7	7	9	441	U	Parts authentication
	Used parts			safety/ comfort	7	7	8	392	U	Parts authentication
	Bad parts	Technician	Financial/ Negligence	safety	4	9	1	36	L	Parts authentication
Repair	Counterfeit parts	Owner/ Technician	Financial	safety/ comfort	7	7	9	441	U	Parts authentication
	Used parts			safety/ comfort	7	7	8	392	U	Parts authentication
	Bad parts	Technician	Financial/ Negligence	safety	4	9	1	36	L	Parts authentication
On the road (OTR)	Bad handling of car	User	Negligence	safety/ comfort	7	9	4	252	H	Data logging on ECU states
	Sudden breakdown	(faulty parts)	-	safety/ comfort	4	9	9	324	U	Data logging on ECU states
	Sudden breakdown	Attacker	Financial/ Crime/ Interest	safety	3	9	10	270	H	Authentication
Insurance	Undeclared upgrades	Owner	Financial	safety/ comfort	8	7	10	560	U	Data logging on ECU states
	Undeclared accidents			safety/ comfort	8	9	5	360	U	Firmware version control
Reselling	Change of firmware	Car agent/ Technician	Financial	safety/ comfort	8	8	5	320	U	Firmware version control
	Broken wire			safety/ comfort	8	8	2	128	M	ECUs authentication
	Change of data in ECU			safety/ comfort	8	8	5	320	U	Authentication, data integrity
Forensics	Data not available	Technician/ Insurance agent	-	reliability	8	10	10	800	U	Backup of latest state
	Unretrieved data			reliability	8	10	10	800	U	Backup of latest state
	Broken ECU			reliability	8	10	10	800	U	Backup of latest state

if they involve critical ECUs. The detection level for failure mode is very remote.

ECUs and car operations Each ECU has different functionalities. Using FMEA, we can conclude which ECUs are more critical in terms of safety and therefore require extra protection. The ECUs related to comfort are considered as lower risk ECUs as the severity of failure is less compared to ECUs related to safety. There is minimal control to detect any failure mode that might occur to these ECUs, and thereby causing the risk to be higher.

FMEA as a risk analysis and security design tool With the increasing reliance on car technology and security, FMEA should be given greater attention in the future. From Table 5, it shows that risk analysis has better coverage by not only considering threats, vulnerabilities and attacks, but also considering the potential failure modes in the overall life cycle of a car and the entities involved. Attacks are conducted intentionally on vulnerabilities of the system, but unintentional actions may also lead to failure modes of the system. Therefore, it is important to consider all possible failure modes in our risk analysis. The detection attribute in the FMEA helps to address the effectiveness of countermeasures being introduced.

2.2 Security Requirements

After the preliminary analysis, the security requirements for a CAN bus are concluded in Table 6. We divided the security requirements of a CAN bus into two parts. They are the security of the nodes (ECUs) and the security of the communication protocols.

Table 6. Security requirements of a CAN bus

Security requirements	Node	Communication protocol
Authentication	✓	✓
Integrity	✓	✓
Availability	✓	✓
Non-repudiation		✓
Freshness		✓
Confidentiality	✓	
Access control	✓	✓
Tamper resistance	✓	

3 Experimental Work

From the analysis it appears that the CAN bus will be a weak link in our system unless the traffic can be better secured. However security may come at a performance cost and so to investigate this, an experimental system was created.

3.1 Method

Components In this experiment, we tried to emulate the communications between the wheel rotation and the odometer on the instrument panel cluster (IPC). We chose MCP25050 and PIC18F4580 (with built in CAN driver) as the CAN processors and MCP2551 as the CAN transceivers. MCP25050 is a configurable chip which makes the CAN bus setup much easier without the need of a microcontroller. The setup is as shown in Figure 1 and 2. The nodes were connected using MCP25050 development board with an oscillator clock of 16MHz. The communications at 125kbps were observed using CAN bus analyser. The CAN bus analyser application monitored the messages sent across the CAN bus.

Setup Firstly, we used MCP25050 for Node 1 and Node 2. Node 2 was an exact copy of Node 1 in terms of its firmware. It would transmit the same message as Node 1 (including ID and data) once it received a wheel rotation signal from the sensor. In our experiment, the signal from wheel rotation was emulated using a switch pulse. For the IPC node, we used PIC18F4580. The IPC was programmed so that it would receive the messages (with specific ID) sent to the CAN bus and increment its counter once the message was successfully received. The counter was shown using LEDs at the output port.

Security implementation To incorporate security into the network, we included encryption and MAC using AES on the data field. Table 7 shows the different configurations of setups. For these setups, we used PIC18F4580 for IPC and Node 1, because MCP25050 is just a configurable IC and is not able to perform security computation as required. In this simple security experiment, we append the MAC as part of the data field in the message to be sent. For MAC computation, we used AES128 and concatenated the result to 2 bytes, then appended the MAC as part of the data field. For a standard frame format, the total number of bits per message is 108 bits (1 bit of start of frame, 11 bits of ID, 1 bit of remote transmission request, 1 bit of ID extension bit, 1 bit of reserved bit, 4 bits of DLC (data length code), up to 8 bytes of data field, 15 bits of CRC, 1 bit of CRC delimiter, 1 bit of ACK slot, 1 bit of ACK delimiter and 7 bits of end-of-frame). Therefore, we decided to put the MAC in the data field and truncate the MAC to 2 bytes only. The firmware codes for CAN communications (transmit and receive functions) and AES computation used for these experiments were taken from Microchip website given as part of PIC18 library [7]. The total code size for AES computation was about 4700 bytes and CAN communication was about 2500 bytes. No optimisation in terms of code size or performance was implemented.

3.2 Result

The latency caused by implementation of security features are as shown in Table 8. These operations executed at external clock of 16MHz using the development

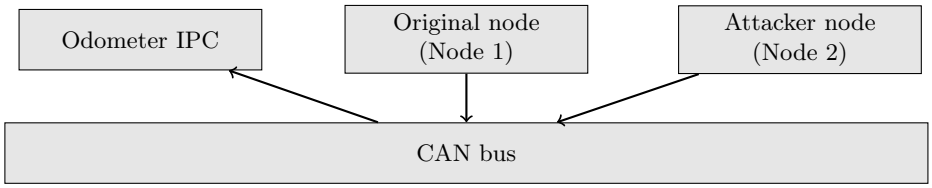

Fig. 1. CAN bus experimental setup

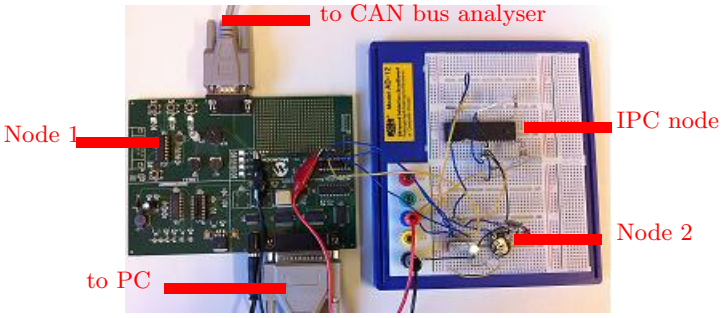

Fig. 2. Actual CAN bus experimental setup

board's oscillator. For a 125kbps communication, this would result in a total messages of 1157 for a standard ID (108 bits) in a second. By adding security, it took up 0.737% of total capacity of bus for send and receive operations.

3.3 Discussion

In the basic setup, it was clear that CAN bus network is very vulnerable to attacks such as sniffing, denial of service, message manipulation and many others. In our experiment, we were able to demonstrate masquarading attack on CAN bus. The attacker node sent the same message as the original node and accepted by the IPC node. From this experiment, we can conclude the requirements of a CAN bus as discussed earlier and summarised in Table 6.

In the setup with MAC, only valid nodes (nodes that have the key to generate the MAC) were able to send messages across the bus. The MAC introduced authenticity and integrity to the network. However attacker can still participate in the bus communication by listening to the network (sniffing).

Finally, in the setup with encrypt and MAC, valid nodes can transmit messages across the bus. If any node attempted to sniff the messages sent across the CAN bus, the messages were encrypted. This setup introduced confidentiality to the network while the MAC gave authenticity and integrity. However, the attacker can still send the same message by replaying the message. Therefore, freshness is further required in the communication. Freshness can be introduced by using counter or timestamp.

Table 7. Steps of operations

Setup	Node 1	Node 2	Odometer	Message	MAC	Encrypt
Basic	Tx (M)		1. Rx (M)	M	✗	✗
			2. counter incremented			
		Tx (M)	1. Rx (M)	M	✗	✗
			2. counter incremented			
With MAC	Tx (M1)		1. Rx (M1)	M1	✓	✗
			2. verify MAC			
			3. counter incremented			
		Tx (M)	1. Rx (M)	M	✗	✗
			2. verify MAC			
			3. counter not incremented			
Encrypt+MAC	Tx (M2)		1. Rx (M2)	M2	✓	✓
			2. verify MAC			
			3. decrypt data			
			4. counter incremented			
		Tx (M)	1. Rx (M)	M	✗	✗
			2. verify MAC			
			3. counter not incremented			

Table 8. Additional computation time for security implementation

Process	Operation	Time (ms)
Generate MAC	AES encryption	1.59
Verify MAC	AES encryption	1.59
Encrypt data	AES encryption	1.59
Decrypt data	AES decryption	2.58

The key management needs to be handled properly to ensure successful security implementation, especially considering the car lifetime. It is expected for parts replacements, which include ECUs, and hence the cryptographic keys need proper handling. The synchronisation of counter or timestamp is also crucial.

While security is important, cryptographic implementation alone does not guarantee a successful system. We also have to consider the limitations and constraints of the system. The latency caused by including the security features can be further optimised to ensure availability of messages in time. Appending MAC as part of the message in the data field may cause potential unavailability since some messages may require to send 8 bytes of data in one message transmission. Furthermore, MAC is not able to provide non-repudiation. A message has to be signed in order to provide non-repudiation. Therefore, this requires further work in order to provide overall security to the CAN bus which include security to the nodes as well as the communication protocol. This includes attestation during start up of operation. The constraints of automotive applications will have to

be considered in proposing a secure solution. This will be included in our future work.

4 Conclusion

This paper discusses the security risk analysis of CAN bus network using FMEA and it shows that security is a process required in the automotive applications. Our experimental CAN bus communications showed that the processing appears to be quite efficient and so adding a security protocol may well be feasible. With the increase use of networks connectivity to improve and assist performance of vehicles, this justifies the need of security to ensure privacy, safety and reliability.

References

1. SeVeCom project. `http://www.sevecom.org/`.
2. EVITA project. `http://www.evita-project.org/`.
3. PRECIOSA. `http://www.preciosa-project.org/`.
4. PRESERVE project. `http://www.preserve-project.eu/`.
5. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, 2011.
6. ETSI. ITS:Security: Threat, Vulnerability and Risk Analysis (TVRA). Technical report, ETSI, 2010.
7. David Flowers. AN953:Data Encryption Routines for the PIC18, 2005.
8. Rob Miller Ishtiaq Rouf, Hossen Mustafa, Sangho Oh Travis Taylor, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *19th USENIX Security Symposium, Washington DC*, pages 11–13, 2010.
9. Road vehicles – Controller Area Network (CAN) – part 1: Data link layer and physical signalling. Standard, International Organization for Standardization, February 2013.
10. Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462. IEEE, 2010.
11. Antonio Kung. Security architecture and mechanisms for V2V/V2I. Technical report, SeVeCom, 2008.
12. Rainer Makowitz and Christopher Temple. Flexray- A communication network for automotive control systems. In *2006 IEEE International Workshop on Factory Communication Systems*, pages 207–212, 2006.
13. Media Oriented Systems Transport Specifications, 2006.
14. Matthew Ruff. Evolution of Local Interconnect Network (LIN) solutions. In *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, volume 5, pages 3382–3389. IEEE, 2003.
15. Jan Peter Stotz, Norbert Bimeyer, Frank Kargl, Stefan Dietze, Panos Papadimitratos, and Christian Schleiffer. Security requirements of vehicle security architecture. Technical report, PRESERVE, 2011.