International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Threat Modeling for Automotives

Parminder Singh[1], Subarna Panda[2]

[1]Student, 6th Semester MCA – ISMS, Jain University, Bangalore, Karnataka India
[2]Assistant Professor - Department of CS & IT, Jain University, Bangalore, Karnataka India

---

Abstract - *Initially, all vehicles were very motorized, overtime they evolved with electronics, and now they are controlled with computers and micro-computing mechanisms converting them to a high end processing automotive systems. In the coming years the introduction of telematics will make the vehicles more connected not only in terms of vehicle parts but also in terms of vehicle-to-vehicle communication, vehicle to device communication, in simpler terms the vehicle gets connected to the global communication i.e. the internet. Therefore, the vehicles are on the way to get exposed to all together new and existing threats of the cyber world.*

Formerly, the users used to measure vehicles in terms of just safety, for example keys, CAN, a number of airbags, tire pressure, OBD diagnosis. Now, the requirements have progressed towards not only safety but security too. Being connected to the outside world, raises the possibility of hackers can emulate the keys and can take control of your vehicle. In such a case, human life, the assets, also from the point of automotive industry the company's trust and reputation among its customers. Thus, what serves as priority now is, during the production and design phase, how vulnerable are critical infrastructure to attack, threat and impact and then design countermeasure. Once you understand how a vehicle's network works and how it communicates within its own system and outside of it, you will be better able to diagnose and troubleshoot problems.

Key Words: CAN BUS, OBD, Automotive cars, Threat Modelling

1.INTRODUCTION

Cars are becoming more and more smart and inter-connected, but on the other side of the coin, this high-tech transformation also makes modern vehicles susceptible to cyberattacks. These automotive systems were never designed with security in mind before. This raises the concern in the industry and the public with the recent security breaches in the automotive domain; especially when new technologies such as autonomous driving and intelligent transport systems (ITS) are becoming reality, it makes pretty clear that security is a critical issue with a likely impact on public and road safety.

To address safety and security of modern vehicles, rigorous security engineering to the development of automotive systems is required. Scrutiny of security is one of the important building blocks in this process. Since automotive cars are open to various kinds of attacks, since they weren't designed with the security in mind. It is important to comprehend the security for cars since our day-to-day life is dependent on it.

CAN bus is a very important part in the automotive network. If an attacker gets control of CAN bus, an attacker totally controls the car. Developed by BOSCH as a message broadcast system, the CAN bus lays down a thoroughgoing signalling rate of 1 megabit per second (bps). Unlike a old-style network such as USB or Ethernet, CAN does not send large blocks of data point-to-point from one node to another under the administration of a central bus master. In a CAN network, steady data is provided in every node of the system, for example, many short messages like revolutions per minute or temperature are broadcast to the entire network. A CAN bus implementation can be examined, typical waveforms can be presented, and transceiver features can be examined once the CAN signalling scheme are understood which would include message format, message identifiers, and bit-wise arbitration.

1.1 ARCHITECTURE

1.1.1 Europe

Having considered at the different components a vehicle can consist of and via which buses these components can communicate with each other, there are numerous ways of how these are ultimately connected in the vehicle.

Please note that each and every vehicle definitely doesn't the same architecture. In this overview, the safety critical functions will be emphasized. Vehicle's architecture can already differ a lot, even within the same manufacturer. However, some abstract (sub-)architectures do have similar characteristics. Also, note that in these architectures, the location of the unit used for V2V Communication i.e., the On Board Unit (OBU), is highlighted. This particular unit does not yet share a portion of the vehicular IT architecture, but will be in the future. The location of the OBU is added in this architecture, based on EVITA project's assumptions.

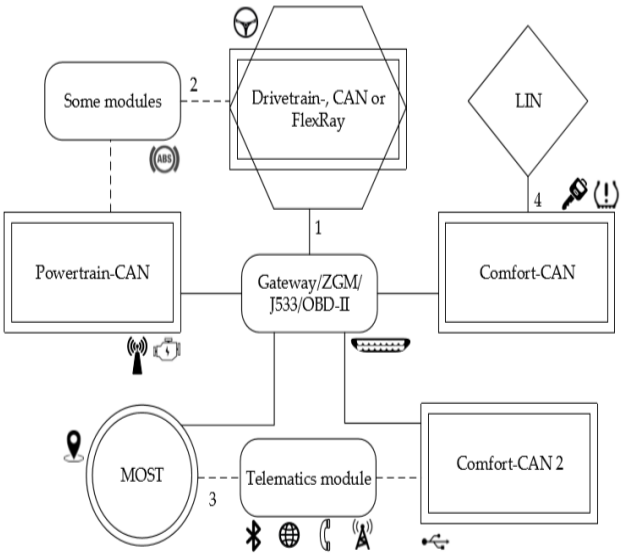


Figure. General IT architecture for a European vehicle.

Please note:

1. The Drivetrain is sometimes a FlexRay bus, and sometimes a CAN bus.

2. Often, there are modules present that reside on both the Drivetrain and the Powertrain.

3. The telematics module sometimes resides on a Comfort-CAN, sometimes on the MOST bus, and sometimes on both.

4. Some Comfort-CAN modules have their own discrete LIN buses for their functionality.

1.1.2 America

The OBD-II port, that has been delegated by the US government is often a separate module that resides on both the High and Low speed bus, however, it is sometimes part of the gateway or BCM module. The telematics segment often exists in on both the High and Low speed bus, although it is not necessarily connected to the High speed bus. The telematics unit is not connected to the drivetrain bus, but is to the powertrain bus, in the case that the High-speed bus is separated. The High speed bus often contains the Keyless Entry System. The Tire Pressure Monitoring System may be located sometimes on the High-speed bus, sometimes on the Low speed bus.

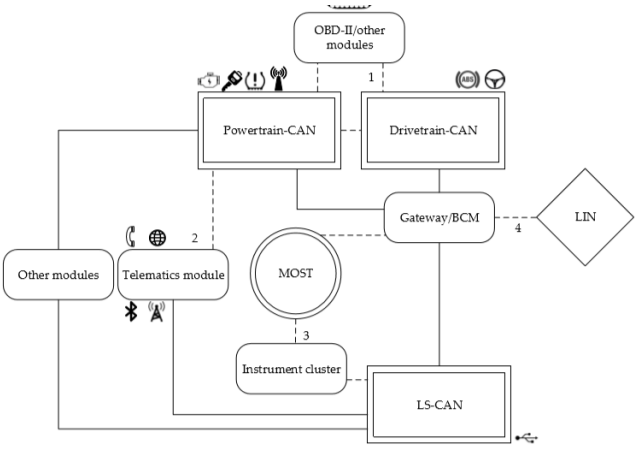


Figure. General IT architecture for an American vehicle.

Please note:

1. The Drivetrain and Powertrain are often one bus, but can be separate sometimes. There are modules that reside on both buses in the case that they are kept separated.

2. The Powertrain sometimes also consists of telematics module.

3. Not all vehicles contain a MOST bus. If the vehicle has a MOST bus, it will then be connected to modules such as the instrument cluster that connects it to the LS-CAN, and to the Gateway.

4. Sometimes, on separate LIN networks, less critical functions are placed. Not all vehicles have this.

1.1.3 Asia

The architectures in the Asia's vehicles differ much more than in America or Europe. Therefore, much harder to construct a general IT architecture for vehicles of this continent. However, it is still probable to note a few universal things in their structural design. Figure below shows a general IT architecture for Asia.

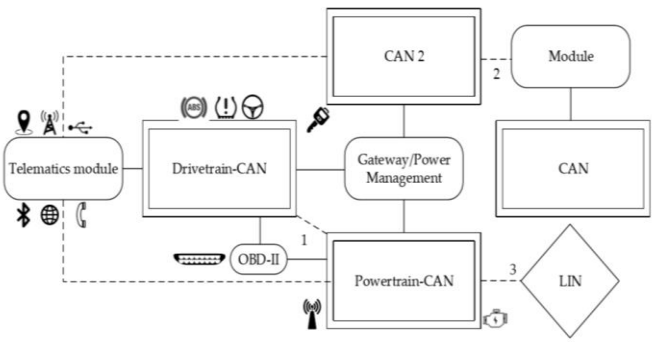


Figure. General IT architecture for an Asian vehicle.

Please note:

1. The Drivetrain and Powertrain are often one bus, but are separated sometimes.

2. Some more advanced modules on the CAN-II bus contain their own CAN bus for communication with sub-modules.

3. Separate LIN networks are sometimes kept for specific modules.

We see a more layered approach followed in buses, in Asian countries. There is often one particular main bus consisting of almost all critical functions. In such a case, some modules have a separate bus for specific functionality. In some cases, the main bus is divided in a Powertrain and a Drivetrain bus.

2. THREAT MODELING

With hacks becoming bigger and risks becoming greater, security has become a major concern in recent years. Today's software needs to be built with the ability to contest and cope with various malicious attacks, and yet, many software developers still might miss a crucial step while creating a secure SDLC (software development lifecycle) process. In order to ensure secure software development process, one of the first steps in your SDLC should be Threat Modelling, alongside performing risk management.

Threat modelling is the method that improves network and software security by identifying and rating the probable threats and vulnerabilities your software may face, so that you can fix security concerns before it's too late. The process is then tailed by outlining the countermeasures, which will prevent those same threats and exploits likely to put your system, here vehicle, at risk. This lets you address threats with the suitable solutions in a rational order, starting with the ones, which possess the greatest risk.

Beginning this process in our SDLC is significant as identifying and rating all probable threats and weaknesses while considering the architecture could lead to significant changes. The process of threat modelling hasn't been well integrated into many automotive suppliers' development process, even though it has been used by some industries for years. The risks and threats are high in automotive industries, since they did not mostly focus over the security aspect of the cars. Unauthorized hacking, which attempts to steal data and get control to the vehicle's control system may render the vehicles uncontrollable leading to information hazards and accidents.

2.1 STRIDE

As cars are getting more connected with other vehicles and the surroundings around them, the security threats will continue to escalate. The automotive industry did not pay much attention to cyber-security, before the concept of a connected car was introduced because the attackers required physical access to perform an attack.

Presently, we have cars with multiple associations to outside networks including a connection to the Internet. In addition to the LTE and Wi-Fi connections, the Car2Cloud technology represents all internal services available because of the existence of Internet connections.

Designed by Microsoft, the STRIDE threat model is used as part of their Security Development Lifecycle (SDLC) to classify and identify automotive risk management techniques 51 potential threats. It is an abbreviation for the following six threat categories:

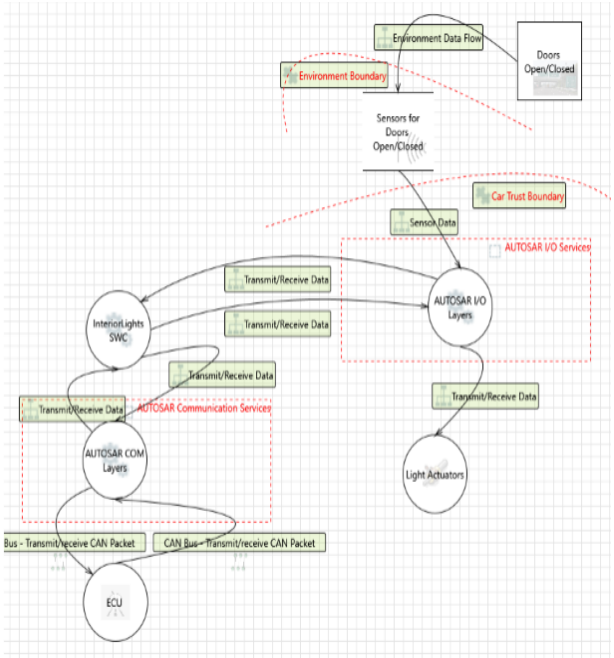
1. Spoofing identity
2. Tampering with data
3. Repudiation
4. Information disclosure
5. Denial of service
6. Elevation of privilege

The idea behind the STRIDE approach is to provide a security professional or non-professional with the tools to give a thought about security threats. STRIDE is originally only part of the SDLC process where threats have to be enumerated and helps at finding the correct threats for a particular element in a Data Flow Diagram. However, sometimes, the STRIDE methodology is referred to as the whole security development lifecycle, ranging from creating diagrams such as Data Flow Diagrams, to mitigating techniques. To reduce the amount of time consumed, not all STRIDE classes need to be tested for all DFD elements, for example, a data flow cannot be spoofed, but only the initiating process can.

We know that that automotive manufacturers have had a rich history in making their products safe by using standardized techniques such as ISO 26262. However, these methods have not been designed to integrate security related safety in the design process.

To be able to cope with these kind of threats, some frameworks such as an extension of ISO 26262 or the NHTSA's modified version of the NIST Risk Management Framework have been designed that do integrate security objectives and threat models in the design process. However, these frameworks do not include any specifics on how such threat analyses should be performed. Some works can be found that does focus on developing such threat models. Several of these models focus on getting a comprehensive outline of the system under development. This is an vital step, since it helps in creating an understanding of the possible outcomes of certain threats, however small they may seem at the beginning.

We choose a specific software application: the interior lights of the car, to demonstrate the STRIDE analysis. The foremost reason for choosing this application is that the Interior lights application is available as an AUTOSAR application, both for a runnable as well as simulation on actual hardware. Furthermore, the Interior lights application implements information flow up to the application level from the ECU level, which is of interest for STRIDE analysis.



DFD created with the MS Threat Modeling Tool 2016 and the NCC Group template.

2.2 DREAD

DREAD is a classification scheme for quantifying, prioritizing and comparing the volume of risk presented by each assessed threat. DREAD modelling influences the thought process behind setting the risk rating, and is used directly to categorize the risks. The DREAD algorithm, is used to compute a risk value, which is an average of all five categories

Using DREAD can be difficult at first. While thinking of Reproducibility, Exploitability, and Discoverability in terms of Probability, it may be helpful to think of Damage Potential and Affected Users in terms of Impact. Using the Impact versus Probability approach (which follows best practices such as defined in NIST-800-30), the calculation always produces a number between 0 and 10. The higher the figure, the more severe will be the risk.

3. PROPOSED THREAT MODEL

A complex threat model that focuses on getting a complete pictorial view of the system under consideration, apply this model to selected forthcoming functionality use cases, and validate this model by cross-examining with a subject matter professional.

The complex threat model consists of three steps.

In step 0, all critical systems and applications should be identified. Then for each identified critical application and system, step 1; the systems and applications are decomposed to get a complete overview and understanding of the system, and step 2; threats are identified and analysed to determine their consequences. These steps are as follows:

0. Identification of critical systems/applications for all identified systems and applications:

1. Decomposition of the system/application a) Create drawing for interconnections of the vehicle b) Create high level flows in the drawing for interconnections

2. Identification and analysis of threats a) Identify threats using STRIDE b) Determination of potential of threats

Please note that these steps are shared by the NHTSA and modified NIST Risk Management Framework.

For a complete overview of the vehicle, all critical systems or applications need to be identified and further investigated. However, applications that are deemed critical could be investigated first when short on time, since they are more likely to result in serious threats. This step could be skipped if all applications or systems are analyzed anyway, and is therefore referred to as step 0. A critical application or system is in this sense is a function that if compromised maliciously, could result in serious consequences, either safety related, or in other ways.

NR	ELEMENT	STRIDE CLASS	SEVERITY S	O	P	F	CONTROL-LABILITY
1	Brake Control Module	STRIDE	4	3	0	0	4
1.1	Emergency brake light	T	0	0	0	0	0
		I	0	0	0	0	0
		D	4	3	0	0	3
2	On Board Unit	STRIDE	4	3	0	0	3
2.1	Emergency Brake Light	T	0	0	0	0	0
		I	0	0	1	0	0
		D	4	3	0	0	3
3	On Board Unit	STRIDE	3	3	0	0	3
3.1	Emergency Brake Request	T	0	0	0	0	0
		I	0	0	0	0	0
		D	3	0	0	0	3
3.2	Emergency Brake Light	T	0	0	0	0	0
		I	0	0	0	0	0
		D	3	0	0	0	3
4	Gateway	STRIDE	3	3	0	0	3
4.1	Emergency Brake Light	T	0	0	0	0	0
		I	0	0	0	0	0
		D	3	3	0	0	3
5	Instrument Cluster	STRIDE	3	3	0	0	3
6	Brake Control Module	STRIDE	3	3	0	0	4

Figure. Threat list with determination of severity for Emergency Brake Light for an EVITA secured vehicle.

There is a slight difference between the EVITA secure vehicle and the modern day vehicle. The modules can no longer be spoofed by other modules on the bus, or tampered with, since messages are now signed and encrypted. However, other threats do still exist. For example, it still gives the possibility to tamper with or spoof messages when controlling a module.

Next to this, Denial of Service attacks are still possible, meaning that the influx of lethal messages such as the Emergency Brake Request cannot be assured. It is also no longer likely to simple replace or add a module on a bus, since it would need appropriate keys to sign a message. However, being able to hack or flash a module does again give access to the necessary keys.

To determine a single threat level, the level of these classes can be utilized. To make sure that a company can determine which kind of threats, and what kind of threat levels it deems most important, it is possible to weight the classes and levels. An example of how levels are subjective within a Severity class is shown below.

SAFETY		OPERATIONAL	
LEVEL	DESCRIPTION	LEVEL	DESCRIPTION
0	No injuries	0	No impact on operational performance
1	Light or moderate injuries	1	Impact not discernible to driver
2	Severe and life-threatening injuries (survival probable) or light or moderate injuries for multiple vehicles	2	Driver aware of performance degradation or Indiscernible impacts for multiple vehicles
3	Life-threatening injuries (survival uncertain) or fatal injuries or Severe injuries for multiple vehicles	3	Significant impact on performance or Noticeable impact for multiple vehicles
4	Life-threatening or fatal injuries for multiple vehicles	4	Significant impact for multiple vehicles
PRIVACY		FINANCIAL	
LEVEL	DESCRIPTION	LEVEL	DESCRIPTION
0	No unauthorised access to data	0	No financial loss
1	Anonymous data only (neither specific driver not vehicle data)	1	Low-level loss ($10)
2	Identification of vehicle or driver or anonymous data for multiple vehicles	2	Moderate loss ($100) or low losses for multiple vehicles
3	Driver or vehicle tracking or identification of driver or vehicle for multiple vehicles	3	Heavy loss ($1000) or moderate losses for multiple vehicles
4	Driver or vehicle tracking for multiple vehicles	4	Heavy losses for multiple vehicles

It is important to note that the determination or exact calculation of the threat level is highly dependent on needs of the manufacturing company.

4. CONCLUSION

In this paper, we saw the architecture of the automotive cars designed in Europe, America, Asia. We had a look on STRIDE and DREAD Model that are used to determine the risks. Our proposed threat model i.e. Composite Threat Model which can achieve and rank threats more effectively as compared.

ACKNOWLEDGEMENT

It is not the completion of the project that is most important but more so, the interaction of roles played by various people in the satisfactory completion. I take this opportunity to express my deep gratitude and appreciation of all those who encouraged me to successfully complete the journal.

With profound sense of gratitude and regards, I acknowledge with great pleasure the guidance and support extended by, I thank Dr. Eshwaran Iyer, Dean, Jain Knowledge Campus, Bangalore, Dr. B.A Vasu, Center Head, Jain Knowledge Campus, Bangalore, Prof. Achutha V, Head, Department of Computer science & IT, Jain University, Bangalore for their interest & encouragement throughout this time period.

I would like to express my deep sense of gratitude to my Guide Mr. Subarna Panda, Professor, Department of MCA, Jain University, Bangalore for his accomplishment and valuable information, direction and sense of perfection to work. He had been main source of inspiration for completion of work and strengthening confidence.

I would like to extend my gratitude and whole hearted thanks to Mr. Priyashloka Arya from RadioJitter Concept Labs for allowing me to undertake this topic for their valuable suggestions, guidance and co-operation during the development of this journal.

I would also thank my parents for their understanding & encouragement, Department Staffs, teaching and non-teaching, my friends, one and all those who supported me.
PARMINDER SINGH

REFERENCES:

[1] Automotive Cyber Seurity, ADI KARAHASANOVIC - UNIVERSITY OF GOTHENBURG, Sweden 2016

[2] The Secure Development LifeCycle, Michael Howard and Steve Lipner – Microsoft

[3] Threat Modeling for Future Vechicles, STIJN Van Winsen

Sites Referred:

- https://www.checkmarx.com/2016/11/08/ultimate-cheat-sheet-threat-modeling/
- http://www.embedded-computing.com/embedded-computing-design/automotive-threat-modeling
- https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/july/the-automotive-threat-modeling-template/

- http://www.autoconnectedcar.com/2017/08/connect-car-can-bus-cant-handle-dos-hacksattacks-researchers-report-can-standard-can-be-changed/
- https://www.kvaser.com/about-can/the-can-protocol/
- https://en.wikipedia.org/wiki/Engine_control_unit