WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Risk Detection Methods of Cyber Security in Vehicle

Prof. Supriya More, Akanksha Raje

[1]Assistant Professor, Department of Information Technology, AISSMS's Institute of Information Technology, Pune-411001, INDIA
[2]TE.(Information Technology), AISSMS's Institute of Information Technology, Pune-411001, INDIA

A B S T R A C T

The classification of vehicle cyber security risks will serve as a useful guide for the management of intelligent connected vehicles' cyber security given the swift development of their network technology. In the process of risk assessment, the method of classifying the cyber security risk of automobile parts is introduced in this study. The automobile cyber security-related products are located, and data on their important features is extracted, utilising a hybrid analysis method that combines qualitative and quantitative analysis. The quantitative evaluation method based on attack potential is also used to determine the danger level. Additionally, the T-Box vehicle information terminal is used as an example to demonstrate the efficacy of this strategy. I need the ho Disposing of bio medical waste (BMW) is a crucial yet difficult undertaking. Medical waste contains potentially dangerous bacteria that could infect hospital patients, medical personnel, and members of the public. Hazardous medical waste exposure can cause illness or harm. The Bio Medical Waste (Management and Handling) Rules, published in 1998, the draught of the Bio Medical Waste (Management and Handling) Rules, published in 2011, and most recently, the Bio Medical Waste Management Rules, published in 2016. Evidence from several Indian regions demonstrates that this is the need of the hour.

Introduction

With the rapid development of intelligent connected cars, cyber security issues are becoming more and more important. In recent years, more and more automakers and suppliers have begun to address the issue of automotive cybersecurity.Risk assessment is a very important link to improve the cybersecurity level and capabilities of automotive companies. A risk assessment can determine the extent to which stakeholders may be affected by potential circumstances or events.

Motivation

We see nowadays most of the cars have intelligent features in it. Cars also contain some features which need network communication and internet connection which make today's intelligent vehicles are vulnerable because of various cyber threads .So predicting its risk level at prior basis is very important so developing such risk classification system is necessary.

Aim and Objective of the work

- To check cyber security risk level in vehicle
- To check with syntactical and semantic approach.
- To make exceptional classification methods for checking risk factors.
- To detect level of risk factor precisely.

A Brief Intro to Li-Fi

Identification of Cyber Security Related Functional Items
Identify cyber security related functions for auto parts, with the specific steps as follows (Figure 1 below):

Step 1:
Classify the functional items of auto parts according
to the following functional classes:
1) Related functions of vehicle remote control.
2) Related functions of communication between vehicles and cloud.
3) Related functions of vehicle short-range communication

4) Related functions of vehicle local physical interface

5) Related functions of key service of vehicle operation.

When the functional items of auto parts meet one or more of the above functional categories, enter the second step; When the functional items of auto parts meet any of the above functional categories with less than one item, the process is ended, and it is determined that the auto parts have no cyber security risk level.

Step 2:

Every functional item needs to analyze the relevant assets, according to the classification principle

1) whether there are directly connected in-vehicle CAN networks, LIN networks, Flex-Ray networks and Ethernet networks. 2) Whether there are directly connected Bluetooth networks, Wi-Fi networks, NFC networks, and radio frequency networks outside the vehicle.

3) Whether or not the in-vehicle network and the outside network are indirectly connected.

4) Whether it contains intelligent software systems or hardware or advanced sensors.

Step 3:

Get a list of functional elements that are candidates for auto part cybersecurity.

If the functional element of the automotive part satisfies one or more of the above optional primary elements, it is considered a cybersecurity candidate functional element and proceeds to Stage 3. if

If the functional elements of the auto part meet any of the above principles and the number of elements is less than 1, the process ends and the auto part is determined to have no cybersecurity risk level.

3.2 Analysis of Cybersecurity Capabilities

Cybersecurity feature analysis is performed on functional elements that are candidates for cybersecurity of automotive parts. The individual steps are as follows (Figure 2 below).

step 1:

Determine whether a candidate cybersecurity functional element for an automotive part possesses cybersecurity characteristics according to the following principles:

a) Whether 3 or more people are directly exposed

Debug, CAN, LIN, Flex-Ray,

Ethernet, Serial, USB, HDMI, OBD.

b) Whether your software code contains high-risk his CVE vulnerabilities such as: B. Operating Systems, Software Components and Applications.

c) whether there is more than one public communication protocol; B. CAN public communication protocol, LIN communication protocol, Wi-Fi communication protocol, Bluetooth communication protocol.

Step 2: Determine that the candidate functional item of cyber security of automotive parts is the functional item of cyber security of automotive parts.

When the candidate function item of cyber security of automotive parts has any two or more cyber security features above, enter the second step; Otherwise, the process is ended, and the cyber security risk level of the automotive parts is determined as "Low Risk".

3.3 Quantitative Attack Potential Analysis

C. According to the cyber security function of automotive parts, the attack potential evaluation value AL is calculated from the following five aspects, and the parameters are AR,PE, KT, WOand EM.

Use the example formula:

AL= AR *1.905+ PE *0.952+ KT *0.952+ WO *1.905+ EM *1.905

(0 <= AL <= 73.3).

TABLE II. CALCULATION METHOD OF ATTACK POTENTIAL

Parameter	0	1	2	3	4	5	6	7	8	9	10	11
Attack range: AR	Without	Single object						Multiple objects				All
Professional experience: PE	Outsiders.			Professional			Expert		Multidisciplinary expert group			
Knowledge of target: KT	Open information			Strictly controlled data				Sensitive confidential information				Very confidential information
Window of opportunity: WO	Unlimited contact	Remote contact			Close contact				Local contact		Very difficult	
Equipment requirement: EM	General standard equipment requirements				Professional equipment			Customized equipment		Multiple customized equipment		

Classify the cyber security risk level for auto parts, with the specific steps as follows:

Low ,medium ,high

Benefits and Advantages

There are many advantages and benefits of Li-Fi technology as follows:
(1) Compared with existing vehicle risk assessment methodologies, the proposed framework has more effective specific risk assessment processes and systematic risk assessment methods.
(2) The proposed framework presents a comprehensive method for analyzing possible attack vectors of system resources by integrating the STRIDE model and attack trees.
(3) This framework takes into account changes in the threat environment, the TOE, and available information, and proposes three methods for assessing the feasibility of attacks. Therefore, the proposed systematic risk assessment framework can be applied throughout the vehicle lifecycle.
(4) The automotive cybersecurity risk matrix was created using a global scoring algorithm that can generate quantitative risk indicators and improve the objectivity of scoring results.

Conclusion:

In this paper, the research on cyber security risk classification of intelligent connected vehicles is mainly carried out, and the risk classification process is standardized and quantified. Combined with the characteristics of automotive cyber security, cyber security related item identification, security feature analysis and quantitative evaluation based on attack potential are set up , to distinguish the cyber security level of automotive parts.The method can be used to classify the evaluation objects in the process of automotive cyber security risk assessment, which can accurately obtain the scope of the evaluation objects and improve the efficiency of risk analysis. This can further promote the improvement of the automotive cyber security level, which is of great significance to the development of intelligent connected vehicles in the future.

References

Bharati, S., Podder, P., Mondal, M., Robel, M. and Alam, R., 2020. Threats and countermeasures of cyber security in direct and remote vehicle communication systems. arXiv preprint arXiv:2006.08723.
Han, K., Weimerskirch, A. and Shin, K.G., 2014. Automotive cybersecurity for in-vehicle communication. IQT QUARTERLY, 6(1), pp.22-25.
Raiyn, J., 2018. Data and cyber security in autonomous vehicle networks. Transport and Telecommunication, 19(4), pp.325-334.