Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

# SOLUTIONS, COUNTERMEASURES, AND MITIGATION METHODS FOR THE RISE OF AUTOMOTIVE HACKING

**SALMAN UBAID BHATTI**
Lecturer, Department of Computer Science, NCBA & E University, Lahore, Pakistan.
Email: Salman.batti51@gmail.com

**KHALID HAMID***
Department of Computer Science, Superior University, Lahore, Pakistan & Assistant Professor University of Education Township, Lahore, Pakistan. Correspondence Email: Khalid6140@gmail.com

**ADNAN BASHIR**
Lecturer, Department of Computer Science, NUML University, Mianwali, Pakistan.
Email: Hadnanb@gmail.com

**ZISHAN ZAFAR**
Lecturer, Department of Computer Science, University of Narowal, Narowal, Pakistan.
Email: zishan.zafar@uon.edu.pk

**AHMAD RAZA**
Department of Computer Science UET Lahore, Pakistan. Email: m.ahmadraza457@gmail.com

**MUHAMMAD WASEEM IQBAL**
Associate Professor, Department of Software Engineering, Superior University, Lahore, Pakistan.
Email: waseem.iqbal@superior.edu.pk

**Abstract**

Automobile hacking is a growing issue in social media and the internet. Since current vehicles have a large number of IOTs. Automobiles are hence susceptible to outside assault. To help the auto industry place more emphasis on creating a secure vehicular information system, this study discusses the problem of car hacking, one of the true threats to automation and the automobile. It also explains how we can prevent it by learning more about the controller area network (CAN) bus architecture. The report also examines risk mitigation strategies that may be used to reduce such dangers.

## 1. INTRODUCTION

One of the most common types of industrial production is the vehicle. Safety is an essential and required factor of an automobile. In the past, it was not a concern for auto designers that a car may be targeted and taken over by hackers. IT crimes, however, have seen substantial development in recent years, making them a serious issue that cannot be disregarded. More attention has to be paid to the lack of safety in the automotive electrical and information systems[1].

Considering modern vehicles, it is quite easy to immediately picture a scenario where a car is controlled using a smartphone. Moreover, this leads to a rise in autonomous vehicles as well as self-driving cars, and this represents the next logical step and is a reality for the current scenario. Due to a rise in the complexity of the electronic circuit of vehicles, there is a need to understand these electronic control units (ECUs) as well as

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

their importance in monitoring the various subsystems of a car. Additionally, modern cars include wireless interfaces that they may use to connect to other devices, which might expose the internal network of the car to security flaws. We think that the sophisticated internal communication systems employed in automobiles today aren't equipped to manage attacks from outside intruders. There are several onboard computers and circuits in contemporary cars. In a car, the computer and circuit systems carry out both straightforward and complex tasks. They thus became the most expensive and advanced components in contemporary autos. These computer-assisted systems handle everything, including the music and visual entertainment systems and engine controls. These computers, also known as electronic control units (ECUs), are connected by several different networks and protocols, including the Controller Area Network (CAN). A component used to connect the engine and braking control is the controller area network. Similar to how a contemporary car has several circuits. These cars were referred to as "connected automobiles." This complexity leads to both greater technological improvements and more vehicle breakdowns. A potential attacker (Hacker) may find those newly linked automobiles to be an easy target. It may occur through a variety of channels and techniques [2].

In-vehicle CAN (communications bus) networks are insecure, allowing an attacker to influence the operation of safety-critical ECUs or limit communication throughout the system. Traditional bus access attacks need physical interfaces; however, researchers have demonstrated the ability to get access remotely. This protest grabbed the attention of manufacturers, suppliers, and foreign regulatory authorities, resulting in the recall of 1.4 million vehicles [3].

Modern in-car networks are vulnerable to attack due to the addition of wireless connection (e.g., Bluetooth, smartphone, Wi-Fi) that provides a variety of services to vehicle owners. Some of these ECUs have made the in-car network vulnerable to assaults by allowing outside penetration. In recent years, several scholars have demonstrated the practicality and accessibility of launching assaults against the CAN bus [4].

Consumers are growing more concerned about cybersecurity vulnerabilities in connected and self-driving cars. A recent Munich research of around 1,500 American people found that 37% are either extremely worried about cybersecurity and the protection of connected and autonomous automobiles. Similarly to this, 35% of respondents were worried that a vehicle's data, equipment, or operating systems may be harmed or destroyed by the flu, malware, or other stealthy cyberattacks [5].

Several methods have been suggested to improve the security of the in-vehicle CAN system. They include secure CAN hardware solutions, intrusion detection systems (IDSes), and message authentication. Future cars should be compelled to incorporate security measures like IDSes, according to regulatory agencies. Given the possible societal ramifications of automobile assaults, it is critical to investigate how to effectively guard against car cyber-attacks [6].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

Currently, ECUs are often utilized in automobiles to regulate and perform the majority of automotive tasks. There might be dozens or even hundreds of ECUs in a car. In this instance, CAN functions as a link connecting the ECUs. The CAN bus is the name of the CAN hardware. The fact that CAN uses a massage-based protocol for information transport is one of its features. The content of CAN messages in an actual automobile is up to the car's designer, but the format of these messages must adhere to a certain standard (ISO 11898). As a result, simply reading these signals may be used to analyze them. Additionally, the CAN data frame message form, which is used to communicate instructions or status information, lacks space for message sender identification [7].

## 2. DIFFERENT WAYS TO UNLOCK A CAR

### 2.1 Using an Arduino-Based Rf Transceiver

The first attack we performed was done by a radio device that cost just 2000 INR with a radio receiver, and a small control board, but is capable of spying and extracting continuous code values used by keyless entry systems.

We included code values in the signal which is sent whenever a driver presses the key buttons, which is then used together to emulate a key that is unique for every vehicle. Then we performed reverse engineering into one component inside a car’s network and were able to extract a cryptography key. Then we combined the two secret keys, which enabled us to clone the key fob and access the car.

### 2.2 Hijack with Hitag2 and a Radio Device in 60 Seconds

In the second method, we used a cryptographic scheme called HiTag2 which is old but still used in millions of vehicles, including Lancia, Opel, Renault, Ford, Alfa Romeo, Chevrolet, and Peugeot.

To perform this attack, a hacker needs a tiny radio setup that is similar to the one used in the previous hack. Using a radio device, we were able to read and intercept the strings of the coded signals from the car’s key fob.

We discovered that flaws in the HiTag2 scheme with the help of rolling codes would allow cracking the cryptographic key in a second. So these two methods were just for unlocking the car, making it accessible for hackers or thieves to steal it. But if we use a digital system instead of rolling codes, it would be more secure. To hack a car, unlocking it is the first step of every hacker, so that they can tamper the CAN bus system and the OBD port.

### 2.3 Tampering the Can Bus

Two security researchers Javier Vazquez-Vidal and Alberto Garcia Illera have developed CAN Hack, a tiny device, which is even smaller than our mobiles, to hack cars. The device costs 1500 INR, but can give away the entire control of any car to an attacker from headlights and windows to its steering angles[7] and brakes (Figure 2).[8]

Injecting malicious code into the CAN ports makes it possible for an attacker to send wireless commands remotely from a computer. It can take just 5 minutes or less for coming into action and then walk away. Whether it takes 1 minute or 1 year, a hacker

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

could wait and then trigger it to do whatever one has programmed it to do. Once hackers have control of this network, they can control locks, lights, steering and even breaks

### 2.4 Can Bus Architecture

The CAN bus is sometimes referred to as the brain of a contemporary vehicle's networked systems. All of the data traffic for a vehicle is broadcast over the CAN bus, which is a solitary, centrally located network bus. The CAN bus system relays all commands from the driver, from "apply the brakes" or "roll down the windows" to readouts from sensors indicating tyre pressure or engine temperature. With the advent of the CAN10 bus, efficiency and complexity both increased, resulting in lower wiring costs (Figure 4).

But with the car hacking toolkit (CHT), hackers have already tested on different vehicles and successfully did tricks, which include setting off alarms, affecting the steering, applying brakes, and switching off headlights. We performed this with the help of Bluetooth, but we could also do the same with the help of Raspberry Pi or a WiFi router, enabling the CHT to control the car from a far distance.

### 2.5 Understanding the OBD Port

All the vehicles come equipped with an OBD (On Board Diagnostic) port, which allows the external devices to interface with a car’s computer system. We generally find this connector under the steering column just above the break and accelerator panel or hidden elsewhere on the dashboard.

### 2.6 Layman Procedure

First of all, as soon as we gain access to an OBD board, we can extract every information about the car. We can use that information to understand the architecture and behavior of that car.

But changes could only be done when a hacker or attacker has access to the CAN bus architecture. For communicating with the CAN bus, we require various drivers and software. The best technique would be to amalgamate the CAN tools along with their various interfaces to form a customary interface so that we could easily share and communicate between different tools.

Sockets CAN, an open-source driver of CAN and official API of Linux kernel makes it possible to make tools to support CAN. Socket CAN applications use the standard C socket which comes along with a custom network protocol family, PF_CAN. With the help of this functionality, the kernel handles CAN devise drivers to communicate with existing networking hardware, thus providing user-space utilities and a common interface.

### 2.7 Data Recorder Logging

All vehicles that came after 2015 are equipped with a kind of black box called an event data recorder (EDR), but it can record only a finite portion of the information that a black box on an aircraft could do.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

### Airbag Deployment

Generally airbags open when a car gets hit on its bonnet, but here with the amalgamation of codes we can open it anytime.

### Steering Angles

Turning the steering into the wrong angles might lead to an accident.

### Vehicle Speed

Engine speed could be tampered with using a reverse CAN; thus, acceleration could be suddenly boosted, leading to a major accident.

### Brake Status

Brakes could be applied

### Ignition Cycles

Ignition could get disrupted while driving, causing a sudden stoppage of the car.

### 2.8 Communicating With the Wireshark for Reversing Can Bus

To keep a watch on the activity of CAN, we need a device called OBD-II that could monitor and generate CAN packets. This device will cost around 2000 INR. Open-source hardware and software are ideal to use as it is compatible with the majority of software tools. We used Wireshark to capture and alter the packets and can dump them from the can-utils suite. Every vehicle has a unique CAN system; therefore, common packet investigation won't work for CAN. As there's so much disturbance on CAN, it's very difficult to sort in the order of every packet.

### Wireshark

For networking, we used Wireshark with SocketCAN to capture CAN packets. Both canX and vcanX devices could be listened to with Wireshark. If you need to use a slcanX device with Wireshark, you should change the name from slcanX to canX. If interface renaming doesn't work, then one has to transfer CAN packets from an interface that Wireshark can't read; a single CAN could bridge the two interfaces.

### Hacking Openxc

After our work of reversing CAN signals, one can frame their own OpenXC firmware. As OpenXC is an API for the car, its work is to read as well as translate information from a car's internal network so that the data could become approachable from most Android apps using the OpenXC library. Compiling 17 of our firmware becomes easy which indicates now we could read or write whatever we want and even write code for the "unsupported" signals. To start an engine, we can create a signal for that and then add it to our firmware to provide a layman interface to give ignition to the car. So, this is the power of open source. Consider a signal that renders the speed of the engine. Giving 8-8 will set a basic configuration to return the speed signal of the engine. Then we sent RPM data with a 4-byte-long instruction ID 0x1110 starting at the fourth byte.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

With the help of OpenXC, our modifications of the CAN system are stored in JSON. JSON is used for storing and exchanging data. First of all, we increased the acceleration of the car using the above code, thus modifying the bus by framing a JSON with a text editor. In the code, we framed a signal of JSON for a high-speed bus running at 600 kilobytes per second.

JSON can read the human-readable text for transmitting data consisting of array data types and attribute value pairs. As soon as we have the JSON, we compiled the above code into a CPP format which again could be compiled into the firmware.

**Who Is Waging To Attack?**

Organizations must first think about the individuals behind attacks to recognize and prevent them. There are two main categories for hackers: White Hat and Black Hat.

White Hat hackers, who primarily do research, rarely have bad intentions. Black hat hackers, according to Upstream's assessment, were in charge of 49.3% of public events between 2010 and 2020. The study also discusses incidents that happened as a result of business operations in which customer discovery or unintentional disclosure of private information occurred. The study was carried out by Upstream.

Cyberattacks and black-hat attacks in the IT industry are the end outcome. Detailed assaults using black hat techniques against critical OT infrastructure, such as hospitals, power facilities, and governmental structures. A patient passed away in September 2020 as a result of a cyberattack on a German hospital. Uber's bug bounty program has received more than 1,500 reports of software problems. As a bug bounty incentive in January 2020, Tesla awarded USD 1 million and a Tesla, setting a record for bug bounty programs.

The number of businesses that conduct bug bounty programs has increased recently, including Tesla, GM, Ford, FCA, Daimler, and others. In recent years, more car-sharing businesses, like Uber, have emerged.

Hackers look for ways to get over security barriers to access utilities. White-hat hackers can expose vulnerabilities even if they might not have harmful intentions? It might also be risky to employ "gray-hat" hackers, who hack for their benefit rather than for illegal gain. "In June 2020, a hacker used BMW's Connected Drive software as a starting point to create an open-source program that retrieves real-time data on car charging. A gray-hat hacker created an Android application in December 2019 using an Arduino microcontroller to add functionality to several Mercedes automobile models by inserting CAN signals.

**2.9 Breach of Data and Privacy**

"The average price of a data breach in 2020 was USD 3.86 million." In this industry, it took an average of 9 months to find and stop a violation. Data is typically exploited by hackers to be sold for a profit. In a stunning case that was made public in August 2020, Departments of Motor Vehicles throughout the United States were found to have sold the

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

personal information of drivers. The California DMV alone reportedly generated USD 50 million each year from the sale of this data, according to reports.

A dark web marketplace advertised a variety of personal information on French drivers in August 2020 for Euro 10 per identity. 3.5 million Zoom vehicle users' private information has been made available.

Vehicle theft and break-ins

One of the most notable repercussions of cyber events over the past ten years was the increase in car thefts, which represented 28% of all accidents in 2020. Theft of cars is a growing "market" for thieves, with more cases being reported worldwide. The UK had a 60% spike in auto thefts in 2020. [16] In India, a group of criminals who used technological tools to steal from over 100 automobiles were caught in September 2020. In January 2020, "two Toyota Tacoma trucks and a Toyota 4Runner truck were stolen from driveways in Canadian after hackers allegedly reprogrammed the vehicles' keyless push start ignition." According to a study conducted in February 2020, 75 of the 200 auto thefts reported to the police in Washington, D.C. 2020 involved the usage of a car-sharing app. To increase your revenues, go out and hire out their automobiles.

### 2.10 Financial Loss

Automotive cyberattacks may have serious financial repercussions, both directly and indirectly. Recalls, plant closures, ransomware costs, and accounts or cars that have been stolen are examples of direct costs. Honda was forced to halt production at certain of its businesses in June 2020 as a result of a ransomware assault on its networks in Europe and Japan. In February 2020, a ransomware assault affected 1,000 systems of an Australian company.

In May 2020, the same business had another ransomware assault, which forced it to shut down a number of its IT systems. Trade secrets theft, harm to one's reputation, and unauthorized upgrades and services for vehicles are all examples of hidden costs. In August 2020, a former Google employee who worked on the company's autonomous car division admitted to stealing trade secrets after downloading 14,000 pieces of data, including product prototypes, to his laptop. He founded his own business, which Uber later purchased. As a result, Google sued Uber in 2017 because Uber had bought the former engineer's business to recover the stolen goods. It was revealed in July 2020 that Tesla had sued Rivian, a startup EV business, and four former employees for allegedly gaining trade secrets through new hires. Damage to a brand's reputation has a direct impact on sales, however, it can be challenging to measure. A 2020 study found that 84% of customers would not order another automobile from a store if their information had been compromised in the preceding year [8] [9] [10].

## 3. LITERATURE REVIEW

According to researchers, the problem of automobiles being hacked began to arise with vehicles made after 2005. This problem is similar to an easy puzzle that hackers can

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

solve. According to one of the reports, names and navigation are crucial and can easily reveal personal information, which is a kind of barrier to privacy protection because many companies do not currently have any policies that can protect sensitive information once the ride is over. By controlling communications between the OnStar Remote Link mobile app and the OnStar service, a "White-hat" hacker claimed in a video that he had discovered how to attack the locking system and vehicles. He added that he planned to present technical details on the hack at the Def Con conference in Las Vegas, where tens of thousands of hacking enthusiasts will assemble to learn about new Cyber Security Vulnerabilities, next week. Defense in depth and many levels of protection are the cornerstones of security. Grau, vice president of IoT and embedded solutions, adds that if one component of the security system fails, you must have a backup plan in place [11] [12].

Across several industries, there has been a lot of recent work in automobile cybersecurity. The good news is that auto supplier chains are expanding their offerings of hardware and software to enhance the system's defenses. The bad news is that cybercriminals are also becoming aware of the new features and have already begun to work on them, which might result in a hack or danger. In this article, we'll examine the cybersecurity statistics from Security's four yearly studies on vehicle cybersecurity. One of the New York University faculty members cautions against it and makes a point to take it into account in front of everyone. He asserted that the vulnerabilities must be referred to or handled as an urgent matter of national security. Additionally, he issued a brake warning. He stated that it is conceivable that someone else who has hacked the system would manage the brake, but we will learn about it when the system is only partially compromised, which might result in an accident or even result in death [13].

### 3.1 Comparison Of Techniques And Methods For Mitigating Hacking [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24]

| Title | Technique | Modal | Objective | Precision | Accuracy | Result | Comment |
|---|---|---|---|---|---|---|---|
| Rise of automotive hacking | Attacker Model | Hacking the USB port | Prevent financial or reputational harm | 90% | 50% | Cars can easily be hacked | Keeping cars software updated |
| Automotive cyber security challenges | Creation of mobile mobs | Disabling smartphone access | Prevent Data from being uploaded to cloud | 40% | 60% | Cars can be used as bots | Always check for viruses in your system |
| Towards the Prevention of Car Hacking | Data Recorder Logging | Airbag Deployment, Steering Angles | Harm to an individual or car | 80% | 70% | Amalgamatin of codes | Need more security in code |
| Cyber-Security, | Adaptive cruise control | Collision avoidance system, | Safety system | 70% | 60% | Cars can be made secure with trial and errors | We need to implement more |

**Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/**
**Journal of Tianjin University Science and Technology**
**ISSN (Online):0493-2137**
**E-Publication: Online Open Access**
**Vol: 56 Issue: 06:2023**
**DOI10.17605/OSF.IO/UG6VD**

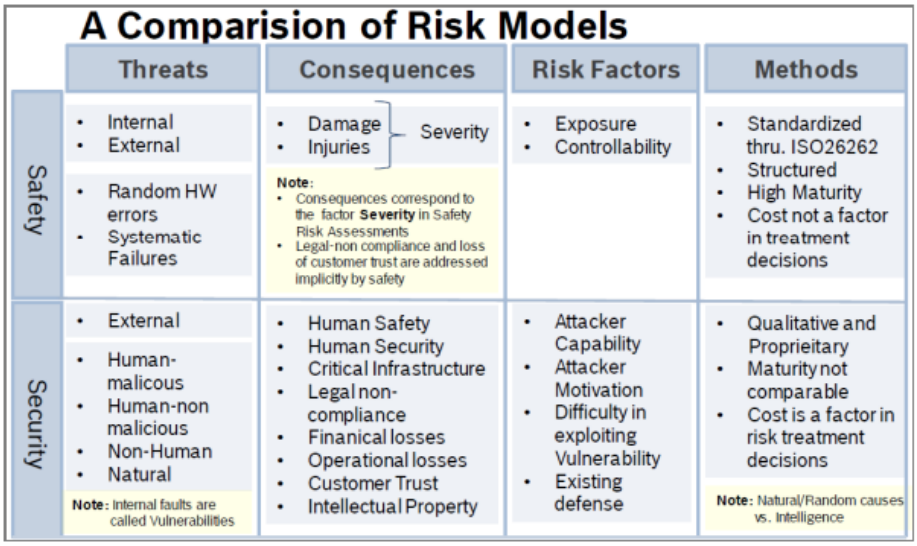
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| a new challenge for the aviation and automotive industries | | Electronic Stability Control, | implementation | | | | security systems |
| Automotive Hacking | Media Oriented Systems Transport | Telematics connection management | High speed vehicle component communications | 60% | 55% | Active cruise control data synchronization | There should be manual cruise option in fully automatic cruise control |
| Car Hacking and Defense Competition on In-Vehicle Network | Intrusion detection techniques | Driving, Stationary, Flooding | Check who can hack the car first | 90% | 80% | Preliminary round datasets are available on website to research | It is a good method to find problems in your system |
| Chrysler Uconnect Hack and Automotive Computer | Uconnect Hack Description and Review | Chrysler Uconnect Hack with CAN | To resolve Chrysler Uconnect software system's problems. | 60% | 70% | Update faulty software and provide USB drives | To Highlights uncovered portion of the Cherokee's PC driven features |
| Developments in Car Hacking | The Interconnected Car | CAN Bus Architecture | Interconnectivity between different car systems | 80% | 65% | Every electrical component in the car has the potential to be exploited by an attacker | Use more secure software to interconnect cars |
| Car hacking: think not, why hack a Desktop when you hack a car? | Exploiting using CANBUS: | CANBUS socket using a popular tool known as "Kayak" | Raw data post exploitation | 60% | 70% | Once the attacker gains access to the car | Using Manual cars is the way to go. |
| Towards the Prevention of Car Hacking: | Using an Arduino-based RF Transceiver | Tampering the CAN Bus | Prevention of Car Hacking | 70% | 60% | Cars will be safe form hacking or other cyber attacks | We should not install third party apps on our car system or them |

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | provided by the car company |
| Automobile Hacking | CAESS Experimental Analysis | Collision avoidance system, Electronic Stability Control, | How cars are hacked | 50% | 60% | How to avoid hackers from attacking your car | Keeping cars software updated so no one can hack it. |
| Automotive Safety and Security Integration Challenges | The Cyclic Redundancy Check | Binary polynomial division | Detect accidental changes in digital networks | 70% | 80% | Detect hardware and software changes | automotive communication CAN bus protocols |
| Analyzing the Capabilities of the CAN Attacker | Disrupting the Target Network | GPIO Configuration | Hack CAN Networks | 87% | 76% | Rx and Tx pins connecting the built-in CAN controller | CAN networks are easy to hack |

## 4. METHODOLOGY

Consideration of a component's or software's security from the beginning is known as "security by design." This is frequently achieved by making sure that every component of the vehicle is planned, built, and tested for security weaknesses, and that any threats found are eliminated. OEMs are primarily responsible for vehicle defense, but all suppliers in the supply chain must also adhere to security-by-design principles. The WP.29 regulation's UNECE handout states that four disciplines must apply cyber security measures, with one mandating "Securing vehicles by design to mitigate risks along the value chain."[25] [26] [27] [28]



Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

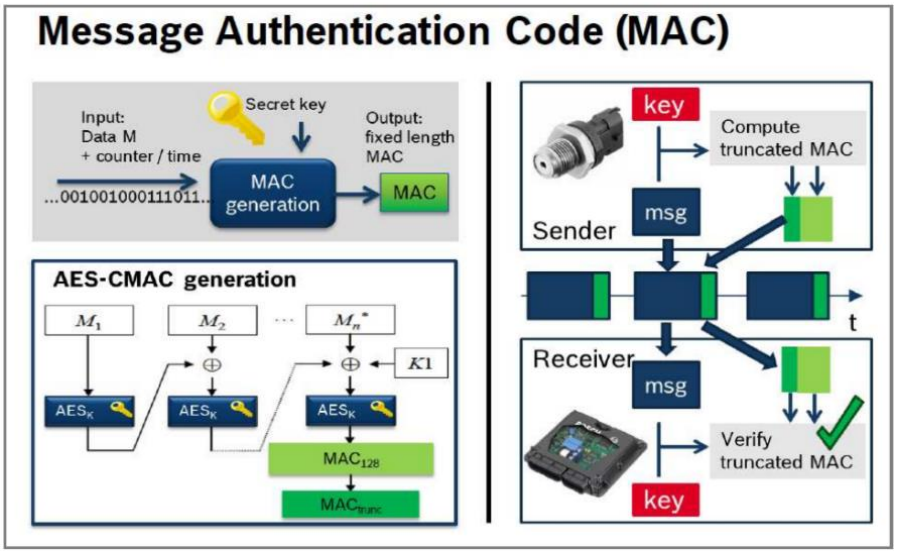
Multi-layered security is essential for IT and business security. Since networks are vulnerable to an increasing variety of attack vectors, businesses should boost their investments in perimeter protection, end-point solutions, cloud security, internal segmentation technology, and other technologies.

## 5. RESULTS AND DISCUSSION

Network management for information technology is currently done by many major organizations using Security Operations Centres (SOCs). The rising sophistication of cyberattacks that aim to protect vehicles, infrastructure, fleets, and users of the road requires OEMs to build integrated vehicle SOCs (or VOCs) to track, identify, and respond to cyber incidents. A VSOC, also referred to as a "car SOC," "mobility SOC," or "automotive SOC," enables cybersecurity for the post-production process and can significantly contribute to ensuring the security of connected vehicles and the smart mobility ecosystem. It also enables businesses to track their entire networks and fleets in real time.

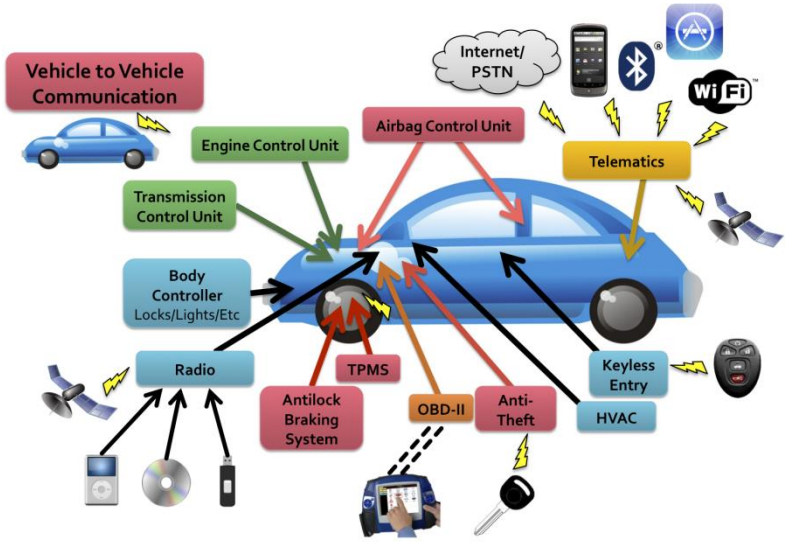
CAN bullet-based attacks be undetectable by existing security measures? A rapid voltage shift in the dominant bit occurs when a message is overwritten. Tracking per-bit voltages at the physical layer is one way to identify such an assault. However, because random faults or true error flags might generate comparable behavior, such a solution would need further pattern recognition in voltage fluctuations.

A family of methods called message authentication codes uses block ciphers or keyed cryptographic hash functions to build integrity tags that can only be generated and assessed with the knowledge of a secret key. The key used for MAC creation and verification is the same, making them members of the cryptographic class of symmetric primitives.



Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 06:2023
DOI10.17605/OSF.IO/UG6VD

The capacity to continue a message transmission, as mentioned in Sec. III is a critical component of effectively attacking the controller. The flexibility of such a countermeasure allows it to be deployed at either the hardware or software level. This strategy may be done if hardware modifications are allowed, by creating reset logic based on the clock signal. This may be accomplished in software by clearing the peripheral transmit buffers when the clock stops. A separate secure chip that monitors the MCU's power utilization might be one host-based detection approach for CAN bullet. Such a chip might contain logic to detect when power dips are unexpected, such as while the vehicle is in motion or awake. It could also identify possibly malicious behaviors by blocking the peripheral clock, which causes a loss of power. Clock gating is the fundamental characteristic that allows CAN bullet in current MCUs. Modern microcontrollers may make it easy for an always-on clock domain for the CAN peripheral, or they may require discrete CAN controllers that take a clock signal out of a different oscillator. If so, disabling clock gating simply CAN leave them unaffected.




## 6. CONCLUSION

Cyber security is now the need of the hour. Smart cars are the most vulnerable and open to any sort of exploitation. One can imagine the situation of being hacked while driving. Even the airbags, brakes and accelerators may not be in one’s control on the wheel. So, manufacturers need to lay much importance on the CAN bus system by making it more hardware-secured and using secret codes.

Due to various significant developments in the field of car device safety in recent years, suppliers are now held responsible by the general public. People's growing awareness of the detrimental effects of real-world automobile security flaws may catalyze reform. The issue is significant and complicated, and there is no easy or cheap solution. But now is the time for producers to stop repairing security flaws and start building safe systems from the bottom up.

**Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/**
**Journal of Tianjin University Science and Technology**
**ISSN (Online):0493-2137**
**E-Publication: Online Open Access**
**Vol: 56 Issue: 06:2023**
**DOI10.17605/OSF.IO/UG6VD**

Here are some thumbs of rules for defenses, or techniques for cyber-attacks relating to the automobile industry.

- Use steering or wheel locks and other physical deterrents to discourage vehicle thieves. It is more beneficial to prevent physical assaults.
- Keep the software in your car up to date by downloading any updates or security patches as soon as they become available. Consider software updates as a means to beat thieves to the punch. Keep it on your list of best practices.
- Install mobile apps only from reputable stores. Since they have been examined to ensure that they follow quality and data security requirements, they are more likely to be reliable.
- Regarding app permissions use caution. An app that demands access to data unrelated to its function is a red flag.
- Remove any identifying information from a car before selling it to prevent passing it on to the next owner. Missing this step is equivalent to opening a door for an assailant with your hands.
- After installing a mobile app, regularly verify your phone's functionality. The battery seems to be swiftly drained by malicious programs since they run in the background undetected. Once it is connected to your car, if this is not addressed, it might become a serious problem.

**References**

1) T. dos S. Pegoretti, F. Mathieux, D. Evrard, D. Brissaud, and J. R. de F. Arruda, ‘Use of recycled natural fibres in industrial products: A comparative LCA case study on acoustic components in the Brazilian automotive sector’, *Resources, Conservation and Recycling*, vol. 84, pp. 1–14, Mar. 2014, doi: 10.1016/j.resconrec.2013.12.010.

2) Z. King, ‘Investigating and securing communications in the Controller Area Network (CAN)’, in *2017 International Conference on Computing, Networking and Communications (ICNC)*, Jan. 2017, pp. 814–818. doi: 10.1109/ICCNC.2017.7876236.

3) N. Weiss, ‘Security Testing in Safety-Critical Networks’.

4) A. Al-Sabaawi, K. Al-Dulaimi, E. Foo, and M. Alazab, ‘Addressing Malware Attacks on Connected and Autonomous Vehicles: Recent Techniques and Challenges’, in *Malware Analysis Using Artificial Intelligence and Deep Learning*, M. Stamp, M. Alazab, and A. Shalaginov, Eds., Cham: Springer International Publishing, 2021, pp. 97–119. doi: 10.1007/978-3-030-62582-5_4.

5) G. Bakioglu and A. O. Atahan, ‘AHP integrated TOPSIS and VIKOR methods with Pythagorean fuzzy sets to prioritize risks in self-driving vehicles’, *Applied Soft Computing*, vol. 99, p. 106948, Feb. 2021, doi: 10.1016/j.asoc.2020.106948.

6) A. Khraisat and A. Alazab, ‘A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges’, *Cybersecur*, vol. 4, no. 1, p. 18, Mar. 2021, doi: 10.1186/s42400-021-00077-7.

**Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/**
**Journal of Tianjin University Science and Technology**
**ISSN (Online):0493-2137**
**E-Publication: Online Open Access**
**Vol: 56 Issue: 06:2023**
**DOI10.17605/OSF.IO/UG6VD**

7) S. Parkinson, P. Ward, K. Wilson, and J. Miller, 'Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges', *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.

8) N. Khan, S. Brohi, and N. Jhanjhi, *Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic*. 2020. doi: 10.36227/techrxiv.12278792.v1.

9) S. Greengard, 'The worsening state of ransomware', *Commun. ACM*, vol. 64, no. 4, pp. 15–17, Mar. 2021, doi: 10.1145/3449054.

10) R. O. Andrade, I. Ortiz-Garcés, and M. Cazares, 'Cybersecurity Attacks on Smart Home During Covid-19 Pandemic', in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, Jul. 2020, pp. 398–404. doi: 10.1109/WorldS450073.2020.9210363.

11) 'Ianelli and Hackworth - 2007 - Botnets as a Vehicle for Online Crime.pdf'. Accessed: May 18, 2023. [Online]. Available: http://www.ijofcs.org/V02N1-P02%20-%20Botnets%20as%20a%20Vehicle%20for%20Online%20Crime.pdf

12) J. N. Bajpai, 'Emerging vehicle technologies & the search for urban mobility solutions', *Urban, Planning and Transport Research*, vol. 4, no. 1, pp. 83–100, Jan. 2016, doi: 10.1080/21650020.2016.1185964.

13) Y. Lu and L. D. Xu, 'Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics', *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019, doi: 10.1109/JIOT.2018.2869847.

14) A. Weimerskirch, *an Overview of Automotive Cybersecurity*. 2015, p. 53. doi: 10.1145/2808414.2808423.

15) P. Sharma, V. Jha, V. Arora, and P. Jain, 'Towards the Prevention of Car Hacking: A Threat to Automation Industry', *Indian Journal of Science and Technology*, vol. 12, pp. 1–6, Nov. 2019, doi: 10.17485/ijst/2019/v12i41/145568.

16) S. Fröschle and A. Stühring, 'Analyzing the Capabilities of the CAN Attacker', in *Computer Security – ESORICS 2017*, S. N. Foley, D. Gollmann, and E. Snekkenes, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017, pp. 464–482. doi: 10.1007/978-3-319-66402-6_27.

17) B. Glas *et al.*, *Automotive safety and security integration challenges*. Gesellschaft für Informatik e.V., 2015. Accessed: May 18, 2023. [Online]. Available: http://dl.gi.de/handle/20.500.12116/2456

18) P. Sharma, V. Jha, V. Arora, and P. Jain, 'Towards the Prevention of Car Hacking: A Threat to Automation Industry', *Indian Journal of Science and Technology*, vol. 12, pp. 1–6, Nov. 2019, doi: 10.17485/ijst/2019/v12i41/145568.

19) T. Ring, 'Connected cars – the next targe tfor hackers', *Network Security*, vol. 2015, no. 11, pp. 11–16, Nov. 2015, doi: 10.1016/S1353-4858(15)30100-8.

20) J. Hayes, 'Hackers under the hood: It's been five years since the first reports of car hacking emerged, but despite progress in vehicle protection standards, automotive cyber-security remains on high alert', *Engineering & Technology*, vol. 15, no. 3, pp. 32–35, Apr. 2020, doi: 10.1049/et.2020.0302.

21) R. Elsaraf, 'Chrysler UConnect Hack and Automotive Computer and Cyber Security'.

22) H. Kang, B. I. Kwak, Y. H. Lee, H. Lee, H. Lee, and H. K. Kim, 'Car Hacking and Defense Competition on In-Vehicle Network', in *Proceedings Third International Workshop on Automotive and Autonomous Vehicle Security*, Virtual: Internet Society, 2021. doi: 10.14722/autosec.2021.23035.

**Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/**
**Journal of Tianjin University Science and Technology**
**ISSN (Online):0493-2137**
**E-Publication: Online Open Access**
**Vol: 56 Issue: 06:2023**
**DOI10.17605/OSF.IO/UG6VD**

23) J. Kennedy, T. Holt, and B. Cheng, 'Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking', *Journal of Crime and Justice*, vol. 42, no. 5, pp. 632–645, Oct. 2019, doi: 10.1080/0735648X.2019.1692425.

24) H. Duchamp, I. Bayram, and R. Korhani, 'Cyber-Security, a new challenge for the aviation and automotive industries'.

25) D. Hussain, S. Rafiq, U. Haseeb, K. Hamid, M. W. Iqbal, and M. Aqeel, 'HCI EMPOWERED AUTOMOBILES PERFORMANCE BY REDUCING CARBON-MONOXIDE', vol. 41, pp. 526–539, Dec. 2022, doi: 10.17605/OSF.IO/S5X2D.

26) R. Khalid, K. Khaliq, M. I. Tariq, S. Tayyaba, M. A. Jaffar, and M. Arif, 'Cloud computing security challenges and their solutions', in *Security and Privacy Trends in Cloud Computing and Big Data*, CRC Press, 2022, pp. 103–118.

27) K. Hamid *et al.*, 'Intelligent Systems and Photovoltaic Cells Empowered Topologically by Sudoku Networks', vol. 74, pp. 4221–4238, Nov. 2022.

28) K. Hamid, M. W. Iqbal, M. Aqeel, X. Liu, and M. Arif, 'Analysis of Techniques for Detection and Removal of Zero-Day Attacks (ZDA)', 2023, pp. 248–262. doi: 10.1007/978-981-99-0272-9_17.