Sri Lanka Institute of Information Technology

Automotive Hacking

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT21049354	A.M.I.R.B.Athauda

Date of submission
24/04/2022

Table of Contents

Abstract

In today's automobiles, there is a symbiotic relationship between information systems. The attack surface of a computerized car grows as it becomes more and more automated. Autonomous vehicles and computerized systems face a genuine threat from automotive hacking that can be prevented by examining the relevant aspects in greater detail. At the moment, network security experts are concerned about car hacking. Because of the current and anticipated increase in the number of vehicles on the road, there is potential harm to passengers, drivers, and other road users. The Automotive Cyber Security Initiative is now researching many aspects of network security, which is the focus of this poll. For non-critical operations like steering and accelerator/brake/clutch, hijacking is possible by sending orders. To protect millions of people from black hat hackers, this study provides a general overview of authenticating the vehicle's security features, preventing millions of people from being victims of such menacing cyberattacks.

1. Introduction

The developed world is almost entirely reliant on cars. It's rare nowadays to find a family without access to a car or other mode of transportation. The US Department of Transportation estimates that over 250 million vehicles have been registered annually. And it's only going up. Computers, servers, phones, electronic structures, associations, and data are protected from malicious attacks by cyber security. It is commonly referred to as "information development security" or "electronic information security". Vehicle hacking will increase in network insurance.

As more devices and frameworks are linked, the Internet of Things is being investigated. As a result, hackers target internet-connected cars. Manufactures have already started taking steps to protect their vehicles' computers from OEM exploitation. Automobile security does not imply hacking into a car or vehicle in any way. Today's vehicles are more autonomous than ever. There are a number of new technologies that are aimed at making driving more efficient such as wifi,automatic software updates..etc. Because car technology hasn't kept up with today's hostile security environment, millions remain vulnerable.

From engine management to steering and brakes, climate control, navigation, and entertainment, computers have been used in cars since the 1980s. The F-35 fighter jet and the Boeing 787 passenger airliner have over 100 million lines of code[1]. Due to its reliance on computers, the modern car has a large attack surface and a wide range of vulnerabilities.

As a result, automakers are more concerned than ever about protecting their vehicles' systems. Securing vehicular systems is still a work in progress. Others use litigation to keep security researchers quiet and vulnerabilities hidden from the public. In recent years, European security researchers discovered a vulnerability in Volkswagen's remote keyless entry system [2]. Finally, the big automakers' safety stance does nothing. To address vulnerabilities and improve overall vehicle security, a more proactive approach is required.

1.1. What is automotive hacking?

Figure 1

Automotive Hacking is the practice of exploiting weaknesses in a vehicle's product, equipment, and communication frameworks. An attack on the software or hardware that drives a vehicle is known as automotive hacking. An attacker can take benefit of weaknesses in the vehicle's software and communication systems. The ECU (Electronic Control Unit) and CONTROLLER AREA NETWORK (CAN) are two of the many electronic features found in today's automobiles[3].

Many of today's cars' systems have become more vulnerable to attack because of their increasing complexity. More advanced software features have been added to their automobiles, as well.

1.2.The Interconnected Car

First, it is necessary to understand how interconnected modern automobiles are, in order to understand their security issues.

Physical control components are shown in blue, safety components are shown in pink, and entertainment and convenience components are shown in yellow in the diagram below. Unlike the early 1980s engine control units, today's modern automobile computer systems go far beyond the engine itself. As shown in Figure 2, the vehicle's engine management system is interconnected with the brake controller, airbags, seatbelt pretensioners, doors, and gauge clusters, as well as a sound system and CD changer, as well as the vehicle's communications system and telematics unit, among other things. Sensor data and vehicle control commands are exchanged via a network of wires that run throughout the vehicle. Controllers can also be seen in Figure 2 in the shape of long rectangular boxes. In response to sensor data or driver commands, the vehicle's controllers send commands to the various components that make up the automobile.

As these systems are interconnected, an attacker could gain access to the vehicle's safety or control systems by exploiting a vulnerability in the vehicle's infotainment system. It is possible for an attacker to take advantage of any of the components listed here. Additionally, each highlighted component represents a potential entry or pivot point for an intruder, as well. The rest of the vehicle's systems could be compromised if an attacker finds a weakness in even one of these components[4].

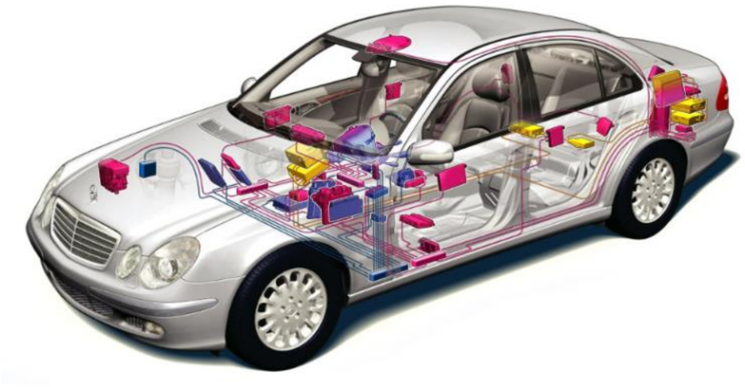

Figure 2:Electronic components in a car

1.3.Types of Hacking on Automobiles

The navigation system, audio and video components, and even the gas gauge were all featured in hack demonstrations. The term "car hacking" refers to the practice of exploiting flaws in vehicle electronics to gain control of the vehicle. It's a problem that car manufacturers are aware of and are working on solutions to avoid. Huge moving computer systems are now standard equipment in automobiles, making them vulnerable to security breaches and viruses. Most car hacks necessitate a high level of expertise and equipment, making them difficult for amateur hackers to pull off.

Today's automobiles are more computer-dependent than ever prior to this point in time. As a result, hackers have multiple entry points into a vehicle's systems. Depending on the vehicle, a particular type of car hack may be appropriate. Upstream has been cataloging major car hacking incidents around the world for a decade and has identified a few trends. According to its findings, automakers should focus their cybersecurity efforts in this area [5].

- **Key Fob Hacks**

  Hackers use automated key fobs to get access to cars nowadays, mainly to steal them (or what is inside of it). This is usually done via spoofing or duplicating the signal used by a car and key to communicate.

  Researchers in Beijing, for example, could increase the range of a key fob by convincing a car that they were nearby with only $22 worth of readily available technology. They did this without the driver's knowledge.

  A cloned Tesla Model S key fob was used by other security researchers, despite Tesla's large security staff and encrypted keys (the encryption turned out to be the weak link). Upstream's data shows two instances of key fob hacking, both for academic purposes. Therefore, automakers must pay special attention.

- **Mobile App Hacks**

  The mobile app market has grown hugely since Apple's App Store was launched in 2008. The auto industry quickly followed suit.

Automotive mobile applications are convenient for customers, but their increased use has also given hackers new ways to access cars. And the risk can be hugely damaging if hackers gain access to the data and control provided by automotive apps.

For example, a hacker found that he could remotely kill thousands of cars' engines by exploiting weak password protocols in two GPS tracking apps (ProTrack and iTrack). Similarly, a security researcher discovered that they could control a Nissan Leaf's functions using only the VIN number from the car's windshield and the associated smartphone application.

Figure 4:iTrack-GPS Tracking System

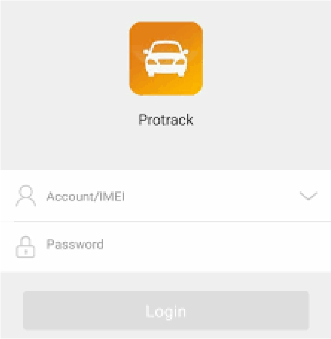

Figure 3:Protrack GPS

- **Server Hacks**

A hacker who gains access to a central computer has access to everything, including sales data, mobile apps, and even vehicle controls. "Multi-vehicle or fleet-wide attacks are exceedingly harmful for all parties involved, from OEMs to telematics service providers, fleet managers to drivers," Upstream warns. In 2015, researchers Charlie Miller and Chris Valasek demonstrated a large-scale attack on car controls by stopping a Jeep going at 70 mph from their couch.

Toyota's computer breach in 2019 exposed millions of sensitive data pieces. As a latest update, on March 1, 2022, Toyota has stopped their production after Russian hackers acquired access to highly sensitive data after Japan expressed its support for Ukraine during the Russian-Ukrainian war. It happened because, a Russian war submarine accidentally attacked a Japanese war submarine.

1.4.Apps for Hacking an Automobile

- **General Motors OnStar App**

  To use the OnStar features on an Android or iOS device, download the OnStar Remote app. By downloading the OnStar app, users can control their vehicle simply by using their mobile phones. Despite that, hackers now can access the app's features by pretending to be the victim[6].

Figure 5:Onstar App

2. Evolution of the topic

2.1. The CAN Bus Architecture

The Controller Area Network (CAN) bus is at the heart of today's vehicles' network of interconnected systems. All vehicle’s data is sent over the CAN bus, which is a single, centralized network bus. Every command from the driver, from "roll down the windows" to "apply the brakes", is carried on the CAN bus. The introduction of the CAN bus resulted in increased efficiency and reduced complexity, as well as lower wiring costs[7].

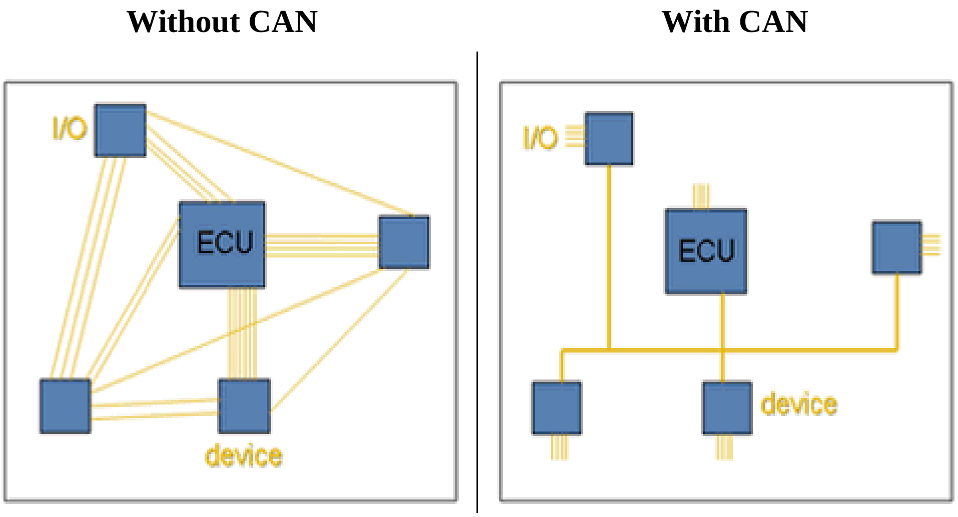
Without CAN **With CAN**

Figure 6

A specific point-to-point connection would have been necessary for any two car components that wanted to interact with one another prior to the advent of CAN bus technology. When CAN networks are used in automobiles, the old point-to-point topology is replaced with a more efficient, centralized approach, as depicted in the figure above. As in the pre-CAN diagram, the network bus is the focal point, removing point-to-point connections between devices and decreasing the ECU's role in the logical network.

Because most vehicle computerized components are connected via CAN, the bus gets a lot of use. "The CAN bus design is similar to a freeway system," says Ford technical specialist Eric Paton [8]. Each component or device is connected to the CAN bus via a "on-amp," referring to Eric Paton's freeway analogy.

CAN data flows whether or not requested. A tachometer shows the engine's RPM (RPM). A tachometer receives RPM data from the engine's ECU via the CAN bus without querying the engine. As soon as you see RPM messages, update the tachometer display. This procedure gives the driver a dynamic tachometer. CAN message size and broadcast frequency vary. It may send 1-byte RPM data every 100 ms over the CAN bus. It also has an 11-bit ID. Unpicking and handling messages is decided by the host controller's ID. So the tachometer's controller will look for RPM-identified CAN messages. This means that only those messages will be received. Another component sending data over CAN. The CAN bus also transmits vehicle speed and cabin temperature. The May bus can carry up to 2,000 signals per day [9]. CAN messages are 1 to 8 bytes long.

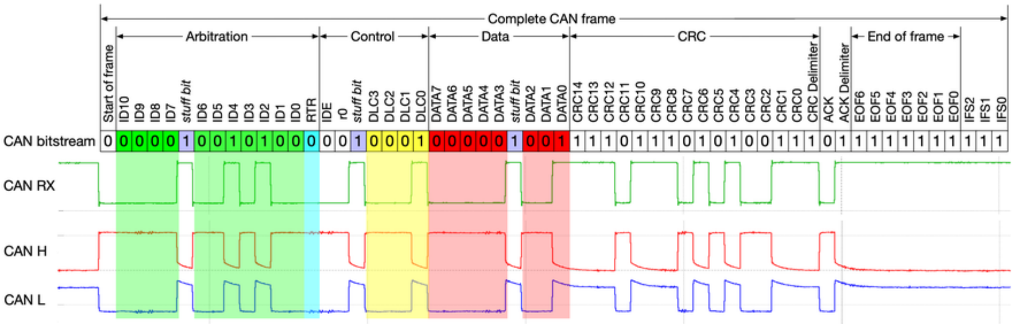

Figure 7:CAN Data Frame

Intuitive device networking over a high-integrity serial bus ISO 11898 is the global CAN standard (National Instruments, 2014). Small and robust, CAN allows new components to be added to the network without modifying existing ones. Message prioritization and error checking are supported by the CAN protocol via the message ID and CRC fields. CAN is the current standard for in-vehicle networking. Figure 7 shows a typical CAN data frame. The SOF bit begins a new data frame. The next 11 bits identify. The RTR bit is indicated in blue. However, a CAN controller can use the RTR bit to request data from another controller. A reserved bit surrounds the RTR bit. A 4-bit data length field (yellow) indicates the data length. The data part (red) ranges from 0 to 64 bits (8 bytes).

The message's integrity is ensured by a CRC field. The next two bits are ACK bits. Finally, EOF bits end CAN data transfer.

2.2. ECU Hacking

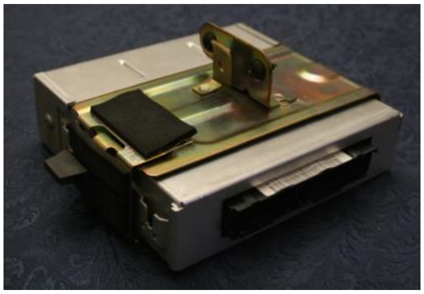

Figure 8:An ECU from a Geo Storm

Figure 9:An ECU from a Chevrolet Beretta

Many electronic controllers in a car are networked together and can communicate. These computerized systems are known by many names, including electronic control unit (ECU), transmission control unit (TCU), and transmission control module (TCM) (TCM).

Contrary to formal usage, these terms are frequently used interchangeably in practice. The electronic controllers are classified as TCUs or TCMs, and both perform the same or very similar functions. Electronic control units (ECUs) control the vehicle's braking system, cameras, engine, and gearbox. Today's electronic control systems come in all shapes and sizes. Some of the more common ones are a PCM, TCM, EBCM, BCM, SCM, Control Unit, or Control Module[10].

Three sorts of attack vectors exist for ECUs:

- **Front Door Attacks -** Taking control of the original equipment manufacturer's access method (OEM)
- **Back Door Attacks -** Making use of more standard hardware-hacking techniques
- **Exploits -** Exploring the possibility of unintentional access techniques

2.3. TCU Hacking

In order to connect to cloud services and other connected vehicles, a vehicle must have a telematic control unit (TCU). It collects and processes vehicle telemetry data and sends it to various sub-systems[11].

A Telematic Control Unit consists of[12],

- Tracking the vehicle's latitude and longitude values using a satellite navigation (GNSS) unit
- To provide the monitored values to a central geographic information system (GIS) database server through the use of an external mobile communication interface (GSM, GPRS, Wi-Fi, WiMax, LTE, or 5G)
- Unit of electronic processing
- A microprocessor or field programmable gate array (FPGA) may act on the GPS interface in some versions, while a microcontroller is used in others.
- A mobile communication Unit
- A small amount of memory for storing GPS values while the vehicle is in an area without cell service or for storing sensor data wisely

2.4. Various Techniques for Unlocking an Automobile

RF Transceiver Based on Arduino

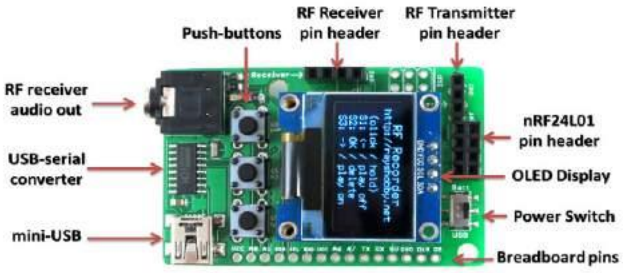

Figure 10:Arduino-based RF transceiver

In the first attack, a radio device costing just $27 with a radio receiver, a small control board, and the ability to spy and extract the code values used by keyless entry systems was used.

It is possible to encode code values in the signal that is sent every time a driver presses the key buttons, which may then be used in combination to duplicate a key that is unique for each car. Afterwards, applied reverse engineering to a single component within a car's network and were successful in extracting a cryptographic key from it. Then combined the two secret keys, which allowed to clone the key fob and get entry to the vehicle.

60 Second Hijack using HiTag2 and a Radio

This method uses an old cryptographic scheme called HiTag2, which is still used in millions of cars, including Lancia, Opel, Renault, Ford, Alfa Romeo, Chevrolet, and Peugeot.

To carry out this attack, a hacker will need a small radio setup, similar to the previous one. A radio device can read and intercept the coded signals from the car's key fob. Using rolling codes, flaws in the HiTag2 method can be used to quickly crack the cryptographic key. So these methods were only intended to unlock the car and make it available to hackers or criminals to steal. A digital method, rather than rolling codes, would be more secure. To hack an automobile, the hacker must first unlock it, allowing access to the CAN bus and the OBD port.

Using Roll Jam Devices

General vehicle remotes are the term used to describe these gadgets. The use of roll jam devices allows programmers to open any vehicle or carport door they come across. In order to jam the moving code end, a roll jam gadget is used to jam the codes. To put it simply, the roll Jam device determines the recurrence between the key and the automobile or electronic entryway, or whether the key is required. This is something that roll is capable of. The operation of this device is divided into three steps[13].

- Radio frequency
- Signal Transmitter
- R Signal Receiver

Using a USB Killer

USB Killer devices look and function similarly to ordinary thumb drives, but they are designed to cause harm to hardware components by injecting high-voltage surges into them during the use of the device. This type of equipment is frequently employed in the evaluation of the reliability of USB flash drives. By connecting this USB killer to the USB ports of the vehicle's electronic control unit (ECU), the vehicle's electronic control unit (ECU) will entirely fail. This device sends a high-voltage power surge into the device to which it is connected, which can cause hardware components to be damaged. Founded in Hong Kong, technology manufacturer USBkill.com manufactures the USB cable in its own country[14].

Figure 11:USBKill V4 Pro

2.5. History of Automobile Hacks in the Past Decade

Once the CAN bus was first developed in the 1980s, its creators had no idea that it might one day be used by criminals who wanted to take control or otherwise influence an automobile's functions. For the most part, automotive hacking was not even on the minds of most vehicle owners until about ten years ago. A very real danger, car hacking has just emerged in the previous decade and especially in the last few years. 78 percent of Kelley Blue Book's 2015 survey participants predicted that vehicle hacking "would be a frequent concern in the next three years or less," according to a press release. The public's opinion of automobile hacking is mostly based on previous high-profile incidents. Some of the most recent car hacks are outlined in the chronology below [15].

- **2010 - Disabling Vehicles at a Remote Using a Web App**

Onboard computer hacking and remote control of a vehicle were used in 2010 by a disgruntled ex-employee of an Austin, Texas, car dealership. No cars were hacked in this attack. A thief may still disable innocent people's cars without their knowledge.

Unknown former distribution center employee used stolen credentials to access a web service that allowed remote access to customer vehicles' functions like engine immobilizer and horn. This web application was designed to allow dealership employees to immobilize customers who had fallen behind on their loan payments. It was misused when motorists were locked out of their cars and their horns blared nonstop.

Pay Technologies, LLC's WebTeckPlus was utilized by the dealership in this instance. The WebTeckPlus program can access PayTeck electronic controllers in customers' cars. PayTeck hardware includes an electronic keypad and controller installed in the customer's vehicle. The controller connects the car's immobilizer and horn. Customers who pay on time receive a new code to enter the electronic keypad. If the right code is entered, the vehicle will run normally. If payment is late and no keypad code is entered, the engine immobilizer will be activated. A dealership employee can also use the WebTeckPlus application to remotely disable a customer's vehicle. Dealerships can use PayTeck hardware and WebTeckPlus software to avoid repossessions.

This attack involves unauthorized access to a web-based program. The perpetrator was charged with computer intrusion. However, in today's connected world, a malicious person could manipulate a vehicle's vital control systems.

- **2010 & 2011 – Experimental Analysis of CAESS**

As a result of this collaboration between UW and UCSB, the Center for Automotive Embedded Systems Security (CAESS) published an article in 2010 entitled "Experimental Security Analysis of Modern Automobiles" (Koscher et al., 2010). It was discovered that the CAN bus may be used to modify a vehicle's operations through a series of lab experiments and road tests. An attacker could easily disable the brakes, selectively deactivate each wheel, and more by demonstrating that he or she was able to do so successfully.

Even though the CAESS team's research revealed severe security problems in modern car systems, their findings were universally panned. Automakers and the media at the time said that it was impossible for an attacker to gain wired access to a vehicle's CAN bus in order to conduct this type of attack in the real world.

"Comprehensive Experimental Analyses of Automotive Attack Surfaces" was published by the CAESS team the following year, in 2011. The team's prior conclusions had been widely criticized by the media. An earlier threat model of an attacker having physical access to the vehicle's internal network had "justifiably been assessed as impractical" by the team, they admitted. Researchers set out to examine a modern vehicle's external assault surface in order to see if an attack might be launched from afar.

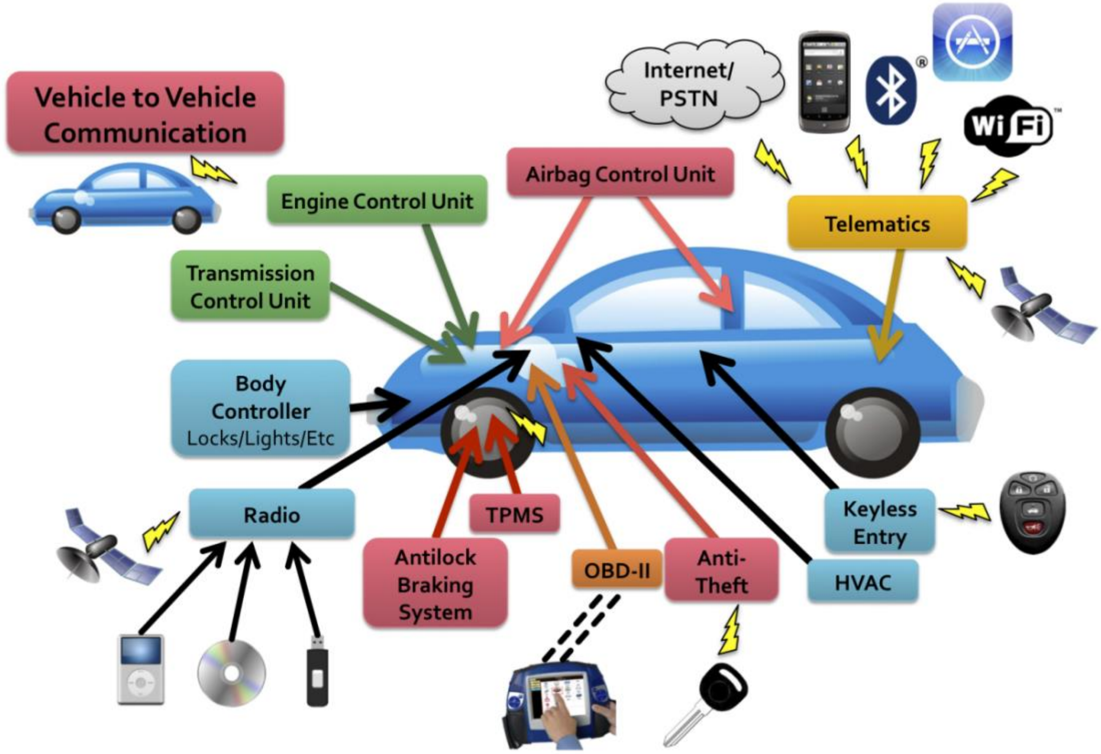

Figure 12:Modern Automobile Digital I/O channels

Above figure depicts the results of the CAESS team's investigation into the attack surface of a modern automobile. An attacker could gain access to a vehicle's I/O channels through the infographic, which depicts the various options available. In the "lightning bolts" symbols, you may see various sources of wireless access and control from outside of the building. The attack surface grows wider and wider as automakers continue to add connectivity to their automobiles. For a potential attacker, the vehicle's cellular, Bluetooth, and Wi-Fi networks present highly appealing access points.

The vehicle's MP3 parser, its Bluetooth system, and the cellular connection used for its telematic system all proved useful in remotely exploiting the CAESS team's test automobile, which was able to be controlled from afar. As previously proved in the group's research, CAN messages might be injected on the bus from there.

"It proved that automobiles were vulnerable to attacks from throughout the country, not just locally," said one researcher (Miller & Valasek). The CAESS team's results received little media attention or response from the auto industry, despite having countered their detractors. Among the reasons for this was that the researchers didn't divulge how their exploits could be replicated or what vehicle they tested on specifically. When the research team decided to keep its activities under wraps, it was understandable, but it also made the findings simpler for the car industry and the general public to dismiss.

- **2015 – Remote Hack of Miller & Valasek**

Charlie Miller and Chris Valasek used a 2014 Jeep Cherokee to demonstrate remote exploiting an untouched passenger vehicle. Unlike the 2013 Toyota Prius and Ford Escape hacks, it showed remote code execution. As a result of this year's hack, Fiat Chrysler had to recall 1.4 million cars for security upgrades, and Sprint had to beef up its. That the Jeep's onboard connectivity and the CAN bus were insecure. A flaw in the car's infotainment, navigation, apps, and cellular communications. Its microcontroller-equipped head unit can talk to other CAN bus modules. The hacker connected the car's telematics system via a Sprint network flaw.

With the telematics system, you can connect remotely. Uconnect had a D-Bus open (6667). D-Bus is a message bus. User input should not be sent via D-Bus. Previously, any Sprint 3G device could talk to any Uconnect-enabled vehicle's open D-Bus port. Attached with a laptop and Sprint 3G phone. The laptop could then connect to Uconnect-enabled cars. An Internet port scan of 6667 over IP ranges 21.0.0.0/8 and 25.0.0.0/8 returned responses from Uconnect devices in vehicles worldwide, the duo found.

Dodge, Ram, Jeep, and Chrysler models were found across the country. Their next focus was the Uconnect's CAN microcontroller. Malicious firmware could be flashed onto a controller. They could control various car components and systems using modified CAN firmware. Miller and Valasek showed the press how to control the air conditioner, radio, and wiper fluid. They may also disable transmission.

It's no secret that recent car hacking demonstrations raised public awareness of A recent Jeep Cherokee hack was known to 72% of car buyers, according to Kelley Blue Book (as cited in PR Newswire, 2015). Considering the recent vehicle hacking incident, 41% will "buy/lease their next car"? (PR Newswire, 2015)

No automotive hack has yet cost a major automaker million. The company decided to repair any faulty vehicles to avoid losing customers and reputation. In total, FCA incurred a labor cost of over $10 million for this. Miller and Valasek want to share their research with the auto industry and security community to improve future vehicle security. To hit an automaker's bottom line is one way.

3. Future developments in the area

3.1. Securing the Automobile from Hackers

The media attention given to Charlie Miller and Chris Valasek's Jeep Cherokee hack has prompted automakers to beef up vehicle security. “Security by obscurity” is no longer acceptable. Researchers have described how to access the CAN bus and alter CAN communications. As a result, manufacturers can no longer neglect automotive system security. All automakers will tackle vehicle system security in their own way, but there are some fundamental best practices that should be followed going ahead.

1. **Encryption**

   Non - secure CAN protocol lacks message confidentiality. Automakers use a proprietary message format unknown to the public for security. The ability to decode proprietary CAN messages and then modify or replay them is possible. Encrypting the protocol prevents CAN reconnaissance [16].

   The CAN protocol data field size is 8 bytes. As an old technology with limited data streams, CAN cannot use meaningful encryption, says Security Innovation's Gene Carter. Strong encryption algorithms require 128- or 256-bit blocks.

   Several researchers and security firms have proposed CAN encryption solutions. SecureCAN from Trillium promises to encrypt CAN messages. Encrypted payloads of 8 bytes or less are designed for SecureCAN. It uses three algorithms: substitution, transposition, and time-multiplexing.

   Trillium says this threshold is required for real-time automotive CAN bus applications. SecureCAN manages keys using “Dynamic Key-Lock Pairing”. Every time a car is started, a new shared master key is created. In addition, SecureCAN can change the ciphertext at random intervals. With SecureCAN, an attacker can't intercept or modify CAN messages.

2. **Device Authorization**

Authentication or authorization of devices is another critical step in preventing malicious CAN bus messages. It used devices that shouldn't have been on the CAN bus, like laptops. This allows receiving CAN controllers to verify the message's origin. This is done by preprogramming CAN controllers with known good CAN identifiers.

For example, the steering controller should only trust commands from the steering wheel controller. As a result, an attacker can send messages that appear to be legitimate. Device authorization requires encryption of the CAN identifier field. The CAN data field is encrypted to prevent message function decoding. A CAN device can no longer be spoof because the identifier field is encrypted.

CAN Device Authorization and Verification" by Patrick K. Richards was published in 2011. Unauthorized CAN bus nodes cannot communicate with authorized nodes due to a unique encryption code stored in each device. Instead of the identifier field, Richards' solution encrypts it. Changing a data frame's CAN identifier causes the recipient CAN controller to ignore the message.

A hardware-based encryption between sending and receiving CAN controllers is required. Richards' solution uses two KEELOQ devices to encrypt and decrypt CAN data. Microchip owns the KEELOQ hardware cipher. This solution may result in longer CAN transmission processing times, higher automaker costs, and heavier vehicles. Implementing a security solution always involves trade-offs.

3. **Two-Way Authentication Method**

The two-way authentication method improves the seed key protocol by allowing the client to control who can access the OBD-II port. After receiving the security access request, the tester is sent a seed S. A pager, a cell phone, or any device that allows the client to receive and send an acknowledgement completes the 2-way authentication process [17].

If the client denies access, the seed is dropped, and the response is not processed. On repeats this process until the client accepts the request and adds the global seed. Upon acknowledgement, the user is granted access. The security method combines the benefits of the seed key protocol and the proposed two-way authentication method.

3.2. Internet of Things and the Connected Vehicles

Integrity and authenticity are critical challenges for the connected automobile, as they are for the Internet of Things as a whole. Automobiles, on the other hand, are unusual in that they are quite valuable and have a lengthy useful life.

Vehicles are difficult to update since they may necessitate a workshop visit, and failure might have a considerably greater financial and human toll than is typical. 65 percent of respondents from the automobile industry agreed that customers' buying decisions for IoT goods will be influenced by security issues. Automotive respondents gave IoT products in their industry an average rating on cyber-attack resistance of just 35 percent [18].

Both on-board and off-board authentication and authorization are essential for ensuring the integrity of the system. However, despite its intimidating appearance, this problem can be solved by adapting well-established best practices from the software development industry (including mobile and IoT) to the specific needs of the automobile sector.

3.3. Performance Tuning

An engine's operating parameters can be altered to increase the vehicle's performance. Even for mechanical modifications, today's vehicles require modifying an engine computer.

Most auto racing requires performance tuning. The Performance Racing Industry estimates that nearly half a million people compete in auto races each year in the United States alone. And that doesn't include the thousands of modified cars that compete in amateur races worldwide [19].

Most performance tuning is simply changing an engine's operating conditions to achieve goals other than the original design. Most engines can be made to produce more power or use less fuel if you are willing to sacrifice safety or use a different fuel than the engine was designed for.

Here are some examples of performance tuning's uses and successes:

- In a 2008 Chevy Silverado, a different rear axle gear improved the truck's ability to tow heavy loads, but messed up the speedometer, the transmission shifted too late, and the antilock brakes failed. A new engine computer was required to correct the speedometer reading, and a new transmission controller to correct the truck's shifting. The truck worked properly after calibration.
- A 2005 Ford F350 needed to have its engine and transmission computers reprogrammed to ensure accurate speedometer readings and proper transmission shifting.
- A 1996 Nissan 240's factory computer was reprogrammed to match a new engine and transmission. Previously, the car could barely run. The car ran as if it had a new engine after the reprogramming.

4. Conclusion

Everything in the world is changing. The hacking of automobiles is currently a hot topic in Cyber Security. Because the number of people hacking into cars is on the rise. In today's environment, we have safeguards in place to keep us safe from both external and internal manipulation. Improve the safety, reliability, and dependability of the vehicular system.

At the present time, many people rely on cars. With so many substantial advancements in automobile system security in recent years, the public is finally holding automakers accountable. People are becoming more aware of the serious consequences of car security flaws, which may be the trigger for change. The solution is neither simple nor cheap. But automakers must stop repairing security weaknesses and start creating secure systems from scratch.

5. References

Texts	
[1]	J. Desjardins, “How many millions of lines of code does it take?,” *Visual Capitalist*, 10-Mar-2019. [Online]. Available: https://www.visualcapitalist.com/millions-lines-of-code/. [Accessed: 16-Apr-2022].
[2]	C. Cimpanu, “Volkswagen sued researchers for 2 years to prevent them from publishing a security flaw,” *softpedia*, 16-Aug-2015. [Online]. Available: https://news.softpedia.com/news/volkswagen-sued-researchers-for-2-years-to-prevent-them-from-publishing-a-security-flaw-489347.shtml. [Accessed: 16-Apr-2022].
[3]	“Automotive hacking,” *Wikipedia*, 15-Apr-2022. [Online]. Available: https://en.wikipedia.org/wiki/Automotive_hacking. [Accessed: 16-Apr-2022].
[4]	“Connected cars: What is it? features and benefits,” *Acko General Insurance*, 31-Mar-2022. [Online]. Available: https://www.acko.com/car-guide/connected-cars-features-benefits/. [Accessed: 16-Apr-2022].
[5]	D. P. H. of C. S. Engineer, “Car hacking is real. here's how manufacturers can combat it,” *Auth0*, 21-Dec-2020. [Online]. Available: https://auth0.com/blog/car-hacking-and-cybersecurity-in-automotive-industry/. [Accessed: 16-Apr-2022].
[6]	“An app above,” *OnStar*. [Online]. Available: https://www.onstar.com/us/en/mobile_app. [Accessed: 16-Apr-2022].
[7]	“Can bus,” *Wikipedia*, 07-Apr-2022. [Online]. Available: https://en.wikipedia.org/wiki/CAN_bus. [Accessed: 17-Apr-2022].
[8]	“Mymoto Nigeria,” *Go to MyMoto Nigeria.* [Online]. Available: https://mymoto.com.ng/how-it-works-the-computer-inside-your-car/. [Accessed: 17-Apr-2022].
[9]	“What is Can bus (controller area network),” *Dewesoft*. [Online]. Available: https://dewesoft.com/daq/what-is-can-bus. [Accessed: 17-Apr-2022].
[10]	P. D. Hasan Ibne Akram, “Car hacking: How to hack an ECU,” *LinkedIn*, 17-Jan-2022. [Online]. Available: https://www.linkedin.com/pulse/car-hacking-how-hack-ecu-hasan-ibne-akram-phd?trk=public_profile_article_view. [Accessed: 17-Apr-2022].
[11]	T. Upstream, “Protecting connected vehicles: From TCU to full control: Upstream,” *Upstream Security*, 17-Apr-2022. [Online]. Available: https://upstream.auto/blog/from-a-single-tcu-to-full-control/. [Accessed: 17-Apr-2022].
[12]	“Telematic Control Unit,” *Wikipedia*, 19-Feb-2021. [Online]. Available: https://en.wikipedia.org/wiki/Telematic_control_unit. [Accessed: 17-Apr-2022].
[13]	Caleb KraftCaleb KraftI get ridiculously excited seeing people make things. I just want to revel in the creativity I see in makers. My favorite thing in the world is sharing a maker's story. You can find me on twitter at @calebkraftView more articles by , C. Kraft, H. G. S. says: M. M. B. says: A. Says: and J. A. says: “Anatomy of the rolljam wireless car hack,” *Make*, 11-Aug-2015. [Online]. Available: https://makezine.com/2015/08/11/anatomy-of-the-rolljam-wireless-car-hack/. [Accessed: 17-Apr-2022].
[14]	M. 3, F. 21, F. 14, and J. 19, “USB Killer: What it is and how to protect your devices,” *Infosec Resources*, 12-Jun-2021. [Online]. Available: https://resources.infosecinstitute.com/topic/usb-killer-how-to-protect-your-devices/. [Accessed: 17-Apr-2022].

[15]	R. Ferguson, “A brief history of hacking internet-connected cars,” *Medium*, 13-Feb-2018. [Online]. Available: https://medium.com/s/new-world-crime/a-brief-history-of-hacking-internet-connected-cars-and-where-we-go-from-here-5c00f3c8825a. [Accessed: 19-Apr-2022].
[16]	B. R. Davis, “How to provide security for car controllers using encryption algorithms,” *Medium*, 22-Jun-2020. [Online]. Available: https://medium.com/@brianrusseldavis/how-to-provide-security-for-car-controllers-using-encryption-algorithms-76109bce725a. [Accessed: 19-Apr-2022].
[17]	L. Rosencrance, P. Loshin, and M. Cobb, “What is Two-factor authentication (2FA) and how does it work?,” *SearchSecurity*, 07-Jul-2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/two-factor-authentication. [Accessed: 19-Apr-2022].
[18]	“Connected vehicles & IOT,” *Internet of Things*, 14-Aug-2019. [Online]. Available: https://www.gsma.com/iot/knowledgebase/connected-vehicles/. [Accessed: 19-Apr-2022].
[19]	“Performance tuning,” *Wikipedia*, 30-Sep-2021. [Online]. Available: https://en.wikipedia.org/wiki/Performance_tuning. [Accessed: 19-Apr-2022].

Figures	
1	“Possible car hacking methods and prevention tips: Dubizzle,” *UAE's leading autos blog | dubizzle Cars*, 23-Dec-2021. [Online]. Available: https://www.dubizzle.com/blog/cars/car-hacking-prevention/. [Accessed: 16-Apr-2022].
2	“Computer History Museum,” *Real-Time Computing*. [Online]. Available: https://www.computerhistory.org/revolution/real-time-computing/6. [Accessed: 16-Apr-2022].
3	“Protrack GPS - apps on Google Play,” *Google*. [Online]. Available: https://play.google.com/store/apps/details?id=com.itrybrand.tracker&hl=en&gl=US. [Accessed: 16-Apr-2022].
4	L. Guangzhou SEEWORLD Technology Co., “ITrack-GPS Tracking System,” *App Store*, 28-Oct-2015. [Online]. Available: https://apps.apple.com/us/app/itrack-gps-tracking-system/id1041798568. [Accessed: 16-Apr-2022].
5	“OnStar App ,” *Ni.com is currently unavailable*. [Online]. Available: https://www.ni.com/en-us/innovations/white-papers/06/controller-area-network--can--overview.html. [Accessed: 16-Apr-2022].
6	“Can bus,” *Wikipedia*, 07-Apr-2022. [Online]. Available: https://en.wikipedia.org/wiki/CAN_bus. [Accessed: 17-Apr-2022].

7	"Electronic Control Unit," *Wikipedia*, 14-Feb-2022. [Online]. Available: https://en.wikipedia.org/wiki/Electronic_control_unit#/media/File:2008-04-17_ECU.jpg. [Accessed: 17-Apr-2022].
8	"Engine Control Unit," *Wikipedia*, 15-Mar-2022. [Online]. Available: https://en.wikipedia.org/wiki/Engine_control_unit#/media/File:An_ECM_from_a_1996_Chevrolet_Beretta-_2013-10-24_23-13.jpg. [Accessed: 17-Apr-2022].
9	G. Samara, W. Al-Salihy, and R. Sures, "Security analysis of vehicular ad hoc networks: Semantic scholar," *undefined*, 01-Jan-1970. [Online]. Available: https://www.semanticscholar.org/paper/Security-Analysis-of-Vehicular-Ad-Hoc-Networks-Samara-Al-Salihy/54a9b3bfc8e6a6f14fdf443e8fb870d2ff52b762. [Accessed: 17-Apr-2022].
10	"Arduino-based RF Transceiver," *Google search*. [Online]. Available: https://www.google.com/search?q=arduino%2Bbased%2BRF%2Bexplained%2Bdiagram&hl=en&sxsrf=APq- [Accessed: 17-Apr-2022].
11	"USBKILL v4 KitPro," *USBKill*. [Online]. Available: https://usbkill.com/products/usbkill-v4-kit?variant=32836116578386. [Accessed: 17-Apr-2022].
12	"Digital I/O channels appearing on a modern car. colors ..." [Online]. Available: https://www.researchgate.net/figure/Digital-I-O-channels-appearing-on-a-modern-car-Colors-indicate-rough-grouping-of-ECUs-by_fig1_259753269. [Accessed: 19-Apr-2022].