INFORMATION ASSURANCE

(ENPM686)

REPORT

V2X ENABLED VEHICLE HIGHJACKING

BY

HITI PARIKH (119198889)

DADHIJA PATEL (119186367)

ABSTRACT

In this digital day and age, the importance of information security has increased. With all the devices connecting to the internet and accessible by the whole network, it becomes a necessity to protect the web assets. The increased cyber threats and attacks have motivated us to take this security seriously.

The concept of self-driving cars has become extremely popular recently. With its popularity, comes more threats to the system and the safety of passengers and other components on the open road.

Our report takes an example of such an incident that caused harm to involved parties and aims to provide solutions to avoid such mishaps in the future. It will include the incident, the factors that led to the incident and the precautions that we should take to prevent future incidents. The contents of the report are inspired by the DRIDE and STRIDE model as well as the Biba model.

INDEX

INTRODUCTION

Vehicle To Everything (V2X) Technology

Vehicle to Everything or V2X is a vehicular communication system that enables the transmission of information from vehicles to any entity of the traffic system that may affect or may be affected by the vehicles. The main purpose of V2X is to enhance traffic efficiency, road safety and energy savings. V2X is a formation of mesh networks between vehicles and fixed infrastructure. In this system, every vehicle has multiple sensors that are part of the Advanced Driver Assistance System (ADAS), which helps the driver be more aware of things like approaching vehicles, the state of the road, blind intersections, and many more. It also includes in-vehicle networking (IVN) for sending signals between two vehicles.

Scope

The scope of this report is to educate people on the value of cybersecurity in the automotive industry, specifically in relation to V2X communication technology, and to highlight the potential consequences of a cyber-attack on a vehicle. The report also aims to emphasize the need to encourage businesses to take the initiative in recognizing and resolving vulnerabilities in their products' security and the importance of holding companies accountable for their products' safety and security. Additionally, it demonstrates how incidents like these can lead to increased security in automotive vehicles. So, the report also underscores the importance of collaboration among automakers, cybersecurity experts, and policymakers to develop comprehensive regulations and industry standards to prevent and mitigate cybersecurity risks in the automotive industry.

SCENARIO

There is an automotive company called Alpha Motors, which has been developing and implementing V2X communication technology in its vehicles. The company is proud of its transformative technology and has been widely recognized for its commitment to safety. However, one day, a group of hackers discovers a vulnerability in the V2X communication system of Alpha Motors' vehicles. The vulnerability allows the hackers to gain control of the vehicle remotely, including its braking system, steering, and acceleration. The group of hackers, known as "Black Hat," decides to take advantage of this vulnerability and launch a series of attacks on Alpha Motors' vehicles. They target a specific vehicle owned by a wealthy businessperson named Mr. Smith, who is on his way to an important meeting. The hackers can take control of Mr. Smith's vehicle, causing it to accelerate uncontrollably and collide with several other vehicles on the road. The accident ends up causing Mr. Smith serious injuries, and Mr. Smith's family sues Alpha Motors for negligence. The incident prompted Alpha Motors to launch an investigation into the security of its V2X communication system. The company discovers that the vulnerability was caused by a flaw in the encryption algorithm used to secure the wireless signals. Alpha Motors quickly develops a security patch and introduces intrusion detection system (IDS) to fix the flaw and releases it to all its customers. The incident also leads to greater scrutiny of the security of V2X communication systems, and Alpha Motors' rivals begin to invest heavily in securing their own systems. The competition becomes fierce, with each company trying to outdo the other in terms of security features. Meanwhile, Mr. Smith's family continues to pursue legal action against Alpha Motors, arguing that the company should have been more proactive in identifying and fixing the vulnerability.

CURRENT STATE

The attack on Mr. Smith's family happened because of a vulnerability and after an investigation, the company discovered a flaw in the encryption algorithm used to secure wireless signals. After finding the vulnerability they quickly developed a security patch and introduced IDS for releasing it to all its customers. However, there is still room for implementing additional security measures.

Assets

Physical Assets	**Human Assets**	**Digital Assets**
Car Components	Customers	Mobile app
Traffic Entities	Employees	Software
	Pedestrians/cars	sensors

PRESENT ARCHITECTURE

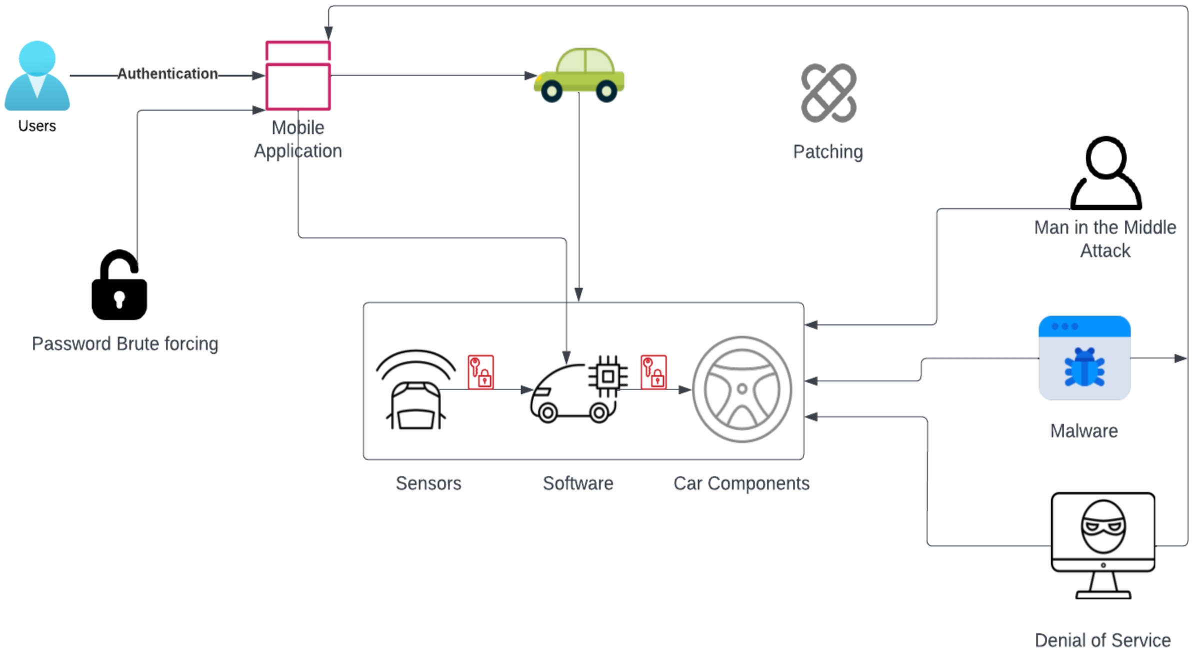

Figure 1 – Present Architecture

ISSUES WITH THE TECHNOLOGY

Weak Encryption Algorithm

The DES encryption algorithm was the main reason for the attack as it is outdated and has a shorter key length. Therefore, the attacker could give malicious commands to the components of the car and modify the pre-defined set of instructions.

Damage to physical devices

Presently, anyone can damage the outer physical devices of the car without any trouble. As these devices are important for sensory functions, any damage to them can be dangerous.

Lack of security testing and validation

The system does not have a proper testing and validation strategy. As a result, the components of the car are not properly checked before driving. Moreover, the clients cannot know whether a malicious actor is monitoring the location of the car.

Inadequate Authentication

Hackers can brute force through the password dictionary and get the password easily for the mobile application. Therefore, just a password does not suffice as a mode of authentication.

Flaws in design

Flaws in design like inadequate security measures and outdated software components can leave the car vulnerable to exploits targeting security weaknesses.

POSSIBLE THREATS

Attacks

GPS Spoofing	An attacker can use radio interference to jam the GPS signal being sent to the self-driving car and send fake GPS signals to trick the AI system of the car.
Man-in-the-middle	An attacker could intercept communication between the car and these sensors and manipulate the data being sent to the car.
Denial of Service	An attacker can interfere with the communication channels of the car and they can flood sensors with large volume of data overwhelming the car’s processing capability and cause it to shut down or malfunction.
Social Engineering	An attacker can attempt to divulge information from client as well as employees to find vulnerabilities in the software.
Malware Injection	The attacker can inject malware in three ways: by injecting malware in the new software update, by gaining physical access to the car and plugging a USB, or from the wireless network used for communication.

Attackers:

Nation-State Actors, Hackers, Insiders, Competitors.

PROPOSED PLAN

Multi-factor Authentication

The mobile application that serves as a connection between the user and the car is currently password protected which can be brute forced by an adversary. Therefore, we plan to introduce a two-factor authentication system using Duo mobile application.

Password Hashing

While storing the passwords in a database, we will use password hashing to prevent the attacker from accessing the password if any security breach occurs.

Automated Software Testing

We would introduce a software testing system that would carry out a thorough check of all the physical components of the automobile to make sure that all systems are working properly.

Firewalls

Firewalls will be built around the software system of the car aiming to protect car's components from threats. We will include three firewalls: the gateway firewall, the In-vehicle network wall, and the application firewall.

Intrusion Detection System

Intrusion detection system will be implemented with the car software and communication system to detect any threat before it becomes a calamity. An internal and an external system will be implemented to provide thorough protection from all malicious intents.

Honeypots

We will implement two honeypots in the system. One will act as the commanding interface for the accelerator and brake and the other will act as a sensor detecting objects on the street.

Security Audits

We will create an elaborate plan to perform periodic tests and security checks. These checks will include the mobile application, database, physical components, and network communications. The checks will be done through vulnerability scanning software and pen-testing.

REUSING CURRENT TECHNOLOGY

Patching

There is already a patching system in place. However, it is not regular or strategic. We plan to introduce a more systematic approach with different schemes and regular patching.

Encryption Algorithm

We will be switching the outdated DES encryption algorithm with AES. The algorithm will be implemented in the communication between the sensors, the car software, and the car components. The system uses TLS protocol to protect data in transit.

Mobile Application Authentication

The mobile app already had password protection. However, we plan to add a multi-factor authentication application.

PROPOSED ARCHITECTURE

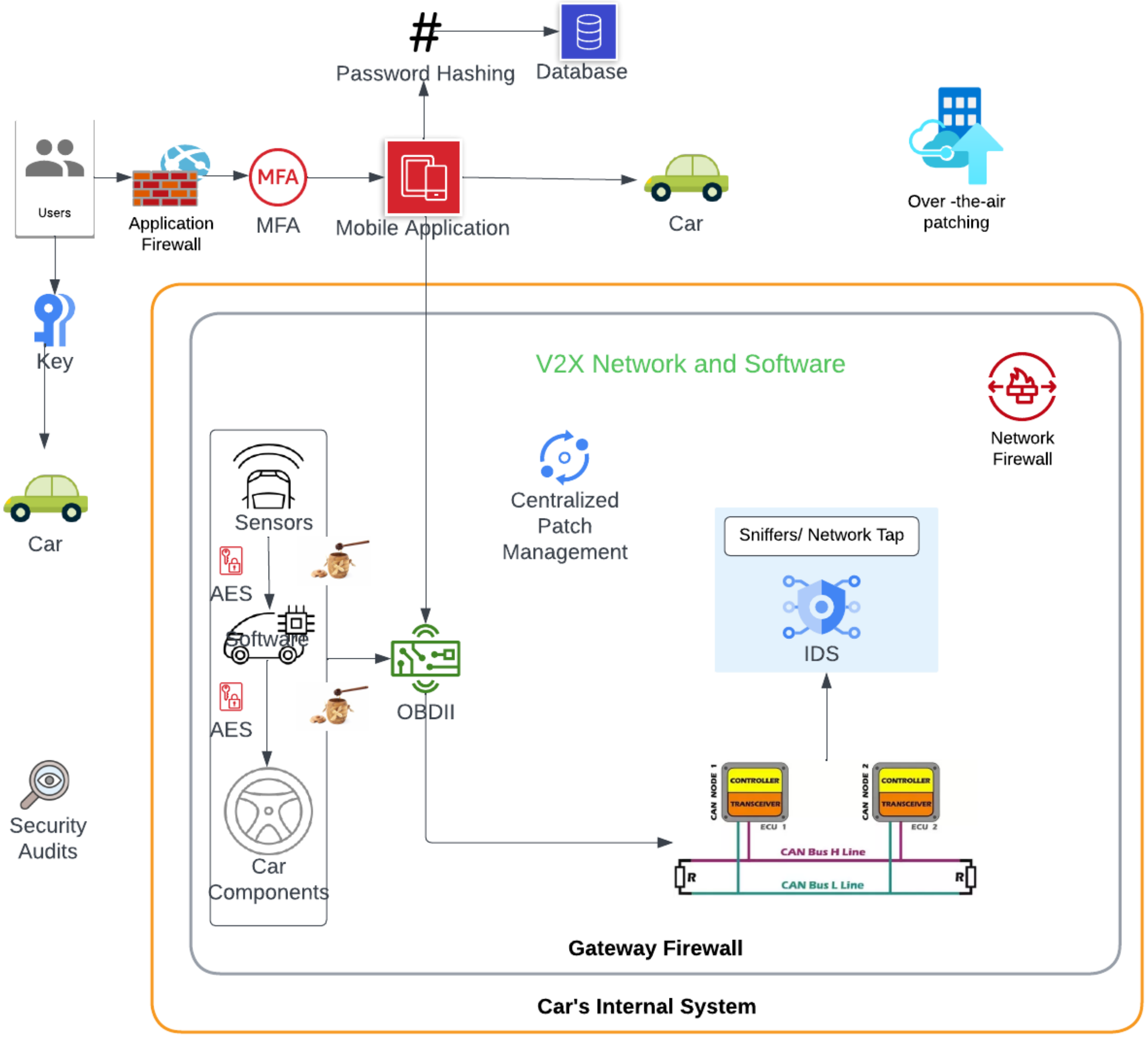

Figure 2

IMPROVED SECURITY

Application MFA

We have included the Push Notification based multi-factor authentication in the mobile application. For integrating MFA with the mobile application, we are using DUO API. This API will help in verifying MFA codes, push notifications and biometrics data. Furthermore, the MFA is also synchronized with the login process to make the user interface easy to use.

Automated Software Testing

For including automated software testing we have included on-board diagnostic system. So here the OBD-II hardware will be installed in the car and then the hardware will be connected to the V2X network. Once the OBD-II hardware is connected to the V2X network, we can connect it to the car’s centralized software and the mobile application which will provide vehicle's diagnostic data to provide real-time alerts, warnings, and other information to the user and other vehicles in the environment.

Intrusion Detection System

- **IDS used for external attackers**

  External attackers can launch cyberattacks through wireless interfaces like Wi-Fi, cellular network, mobile application and through hijacking the car’s software. So, to protect the vehicle from external cyberattacks we are putting IDS within the system gateways. Taps and Sniffers will monitor the network traffic and then forward them to the car software. So if any malicious packets are detected it will notify the car software as well as the mobile application.

- **IDS used for internal attackers**

  The intrusion detection system will be placed on the CAN-bus. Here, the system will detect harmful packets and analyze them to understand the threat from the packets.

Firewall

- **Gateway firewall**

  A gateway firewall can be placed at the point where the vehicle connects to the outside world, such as the internet or cellular network. The gateway firewall can monitor and filter traffic for suspicious patterns or behavior and block or alert them, as necessary.

- **In-vehicle network firewall**

  A firewall can be installed on the vehicle's internal network to protect communication between different electronic control units (ECUs) and other connected devices. This type of firewall can be placed between the IDS and the CAN-bus which helps to isolate vulnerable ECUs or devices from the rest of the network, preventing malicious traffic from spreading across the system.

- **Application firewall**

  An application firewall is included at the device layer which will provide protection against various cyber breaches and hijacking.

Patching

- **Over-the-Air (OTA) Patch Management**

  The most effective way to manage patches in V2X-enabled vehicles is through OTA updates. With OTA updates, vehicle manufacturers can send software updates wirelessly to vehicles, enabling the latest security patches and software fixes. OTA updates can also address any security vulnerabilities or bugs that are discovered in the system.

- **Centralized Patch Management**

  We have also used centralized patch management system to manage patches across all V2X-enabled vehicles. The system can monitor all vehicles and push patches as soon as they become available.

Honeypots

Once both the honeypots are set up, they will continuously monitor the activity. If any malicious actor tries to give commands to the brake or accelerator in the car, they would be giving commands to honeypots. Consequently, no actual harm will occur to the system and the activity would be detected by the security professionals. If any potential hacker wishes to gain information about the location of the car, they will encounter a honeypot that does not exactly display the correct information. This honeypot will be a decoy that protects the user's information.

Security Audit

We have included regular security audits in V2X-enabled vehicles which will involve defining the scope and objectives, performing a risk assessment, developing a security audit plan, conducting the audit, analyzing the results, developing a remediation plan, and monitoring and reviewing the system.

Password Hashing

Using a strong one-way hash algorithm and salting, the storage of user passwords will become a lot more secure. Even if any data is compromised, the attacker will not be able to retrieve the passwords.

Encryption Algorithm

AES has a larger key size and therefore it is more secure. It is much faster than DES while encrypting the data. It will maintain confidentiality of the data while the data is transmitted between two parties. So, all the wireless signals communicating to sensors and physical components will be strongly encrypted.

RELATION TO INFORMATION ASSURANCE

Confidentiality

Confidentiality comes into play as the driver's personal information is protected. No unauthorized user will not be able to get information like the location of the car, or the destination of the car. Moreover, many people store information like home addresses and office addresses and places that they often visit for convenience. This information is also protected from attackers.

Integrity

In a self-driving car, integrity includes protecting the integrity of the data generated by the car's sensors, such as location and speed, to prevent attackers from manipulating the data and causing the car to behave erratically. Using the technology mentioned above, the integrity of the commands given to the car is maintained.

Availability

In a self-driving car, availability includes ensuring that the car's sensors and computer systems are always available and functioning properly, even in the face of a cyber-attack or system failure.

ALTERNATE SOLUTIONS

Data backups and recovery system

The only place where this system would require a data backup and recovery system is the database that stores the passwords of the mobile application. This technology and development are not in our scope. Additionally, it is not a priority for us right now as there are many other databases with the company that stores the information of each client. We can use that information to recover data if any loss occurs.

Artificial intelligence for threat detection and prevention

Detection and Prevention of threats can be done by AI and machine learning. However, our system only deals with the software part of the car. Therefore, an elaborate system to detect threats is much work for a menial work. It would also require a hefty sum of money to implement the AI system.

Automatic Analyzing of security logs

The automatic analysis of security logs is also a big decision for a small amount of work. It would increase the sale price of the product. As a result, the sales could go down for the company and the company could function at a loss. Therefore, we decided not to include the above technologies in the system.

BUDGET

Components	Number of Implementations	Estimated Cost
Software		
Firewall	3	30,000-45,000
MFA	1	10,000-35,000
Hashing	1	5000-15,000
Database	1	40,000-60,000
Patching	3	45,000-75,000
Security Audits	1	20,000-40,000
Secure Encryption Algorithm	1	15,000-25,000
Honeypots	2	10,000-30,000
Intrusion Detection System	1	15,000-35,000
Sniffers	1	3000-7000
Hardware		
OBDII	1	2000-4000
Can Bus	1	2500-4000
People		
Employee Training		10,000-30,000
Employee Salary		60,000-80,000
Total		267,500-485,000

The budget was finalized based on a thorough security assessment of the cybersecurity needs required by the organization's V2X-enabled vehicle. The selected security measures, such as firewalls, MFA, hashing, patching, security audits, strong encryption algorithms, honeypots, and IDS, are intended to provide layered security to mitigate the major risks that the car faced. Additionally, the budget was planned in such a way that Alpha Motor's V2X-enabled vehicles are protected against cyber threats without overspending on unnecessary security measures. Overall, the budget is cost-effective and relevant to the organization's security needs.

REFERENCES

https://arxiv.org/pdf/2105.13289.pdf

https://arxiv.org/pdf/2111.02364.pdf

https://www.etas.com/en/company/news-intrusion-detection-as-a-distributed-system.php