STRIDE-BASED CYBER SECURITY THREAT MODELING AND TREATMENT OF AN INFOTAINMENT HIGH PERFORMANCE COMPUTING(HPC)

Popy Das

Roll: 17 CSE 019

Reg. Number: 110-019-17

Session: 2016-17

In Partial Fulfillment of the Requirements

For the Degree of

Bachelor of Science in Computer Science and Engineering

Department Of Computer Science and Engineering

University of Barisal

SUPERVISOR'S DECLARATION

I, hereby, declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor of Science in Computer Science and Engineering.

(Supervisor's Signature)

Full Name: Md. Rashid Al Asif

Designation: Assistant Professor

Department of Computer Science and Engineering

University of Barishal

Date: 2024-07-29

STUDENT'S DECLARATION

I, hereby, declare that the work in this research is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at University of Barishal or any other institution.

(Student's Signature)

Full Name: Popy Das

Roll: 17 CSE 019

Department of Computer Science and Engineering

University of Barishal

Date: 2024-07-29

ABSTRACT

Infotainment High-Performance Computing (HPC) plays a crucial role in modern automotive vehicles by providing advanced features and functionality to drivers and passengers. Infotainment systems in vehicles are designed to enhance the driving experience by providing a range of features such as music, navigation, climate control, communication, and entertainment. However, the increasing reliance on information technology in cars has led to cybersecurity threats, which can cause data breaches, loss of sensitive information, and damage to the security of the system. The objective of the research is to conduct a holistic threat modeling on component levels of infotainment HPC to identify common security issues for security betterment of the system. This research proposes an Infotainment HPC system, which includes various components and workflows. Using Microsoft's threat modeling method, STRIDE, the research identifies 34 potential security threats that need to be considered during the design and development of Infotainment HPC systems. These threats are presented systematically, and general mitigation suggestions are provided to enhance cybersecurity in Infotainment HPC systems of automotive vehicles. The future work involves risk assessment of each threat to determine the most suitable mitigation strategy that may upgrade cybersecurity within infotainment HPC.

Keywords: Cybersecurity, Infotainment, High-Performance Computing (HPC), Threat Analysis, Threat Mitigation, Cyber Attacks

ACKNOWLEDGEMENTS

I wish to express my sincere gratitude to my supervisor, **Md. Rashid Al Asif** for providing me with all the necessary facilities, giving undivided attention and fostering me all the way through the thesis. His useful comments, remarks and engagement helped me with the learning process throughout the thesis.

I want to express my heartiest gratitude and thanks to all teachers of department of Computer Science and Engineering for sharing their pearls of knowledge and thoughts about the research. I would like express gratitude to all of the departmental faculty members for their help and support. I am also grateful to my parents for their encouragement, support and attention and for being ravished patrons. I also place on record, my sense of gratitude to one and all, who directly or indirectly, have contributed to this venture. Their motivation created additional perseverance throughout the completion of this thesis.

Contents

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction

In recent times, the combination of information and communication technology with automotive technology has become increasingly popular to improve the safety and convenience of vehicles. This integration encompasses various aspects, including the occupant's nomadic device, surrounding vehicles, traffic infrastructure, driver and pedestrians, and the environment. Always-connected vehicles offer several benefits, such as access to a vast amount of information. However, the downside is the potential risk of being attacked by adversaries at any time.

As vehicles become more connected, they can provide a wider range of services due to links between cars, other vehicles, and infrastructure. Smart gadgets' interconnection with automobiles also creates new user connections, leading to increased security vulnerabilities. Reports of car hacking incidents are becoming more frequent, prompting a greater emphasis on vehicle security research [1].

Using information and communication technology with automotive technology is a natural progression in the quest for increased safety and convenience. To achieve this, it is essential to analyze the security risks of occupant devices, nearby vehicles, traffic infrastructure, drivers, pedestrians, and the environment. While always-connected vehicles offer many advantages, they also present a risk of hacker attacks. To improve the security of in-vehicle infotainment HPC, this research has focused on identifying security vulnerabilities and threats using the Microsoft threat modeling tool STRIDE. Through the threat modeling process, 34 threats were identified, and mitigation measures were proposed to counter these threats, ultimately leading to an overall improvement in the vehicle system's security.

1.1 Motivation

Cybersecurity is an increasingly important field due to the rise of cyber threats and the importance of protecting sensitive information. Threat modeling and treatment are critical components of cybersecurity, as they allow organizations to identify potential vulnerabilities and implement proactive measures to protect against cyber attacks [2].

In the case of infotainment high-performance computing (HPC), there is a particular need for cybersecurity measures due to the large amount of data that is processed and the potential impact of any breaches. By conducting research in this area, we could help identify potential threats to infotainment HPC systems and provide possible mitigation to those threats.

Furthermore, the field of cybersecurity is constantly evolving, with new threats and vulnerabilities emerging all the time. By conducting research in this field, we can help advance our understanding of cybersecurity and contribute to the development of new and more effective cybersecurity solutions.

In summary, conducting research in cybersecurity, specifically in threat modeling and treatment of infotainment HPC systems, is important because it can help protect sensitive information, identify potential vulnerabilities, and advance our understanding of cybersecurity.

1.2 Problem Statement

Infotainment HPC systems are increasingly being used in various industries, such as automotive, healthcare, and entertainment, to process large amounts of data and provide high-quality services to users. However, these systems are also vulnerable to cyber attacks, which can have serious consequences, such as loss of data, financial damage, and reputational harm [3]. Nowadays security become the most important issue. As the system becomes updated we lack security in our life. Information theft, lack of security and violation of privacy, etc.

The problem is that the existing cybersecurity measures for infotainment HPC

systems are often reactive, focusing on responding to known threats rather than identifying potential vulnerabilities and implementing proactive measures to prevent cyber attacks. Furthermore, the complex and interconnected nature of these systems makes it difficult to identify all potential threats and develop effective security measures.

Therefore, the goal of this research is to propose system components for infotainment HPC systems based on threat modeling and treatment. This research should identify potential threats to these systems and provide effective strategies to mitigate those threats, taking into account the unique characteristics of infotainment HPC systems. The research will also explore new and emerging threats to these systems and propose solutions to address these threats.

1.3 Research Questions

The main objective of this paper is to present a picture of the research work on threat analysis in the automotive context and provide treatment for the threats. In this thesis, the following thesis questions will be answered.

- How can threat modeling be used to identify potential vulnerabilities in infotainment HPC systems and prioritize them for remediation?
- Which mitigation strategies can be followed to treat the threats?
- How can the effectiveness of cyber security measures in infotainment HPC systems be measured and evaluated over time?

1.4 Contributions of this Research

Numerous countries, companies, and researchers are currently focused on improving system security by identifying potential threats. However, this is an ongoing and challenging task due to the constant updates and changes to systems. The unique contribution of the research is to drive the components of the infotainment

HPC of an automotive vehicle. Then the research focuses on finding the potential vulnerabilities and threats of the system that may compromise the system and create effective threat models to address them. It also assists in developing strategies to mitigate cyber attacks on infotainment HPC systems, thereby preventing security incidents and data compromise. Additionally, this research can improve the security protocols used in infotainment HPC systems, raise awareness of potential risks among stakeholders and decision-makers, and even lead to the development of new technologies. Overall, this research is critical in enhancing the cyber security of infotainment HPC systems and preventing data compromise and other cyber attacks.

1.5 Structure of the Thesis

The thesis contains six chapters in total. In order to evaluate the threat analysis and treatment of infotainment HPC of an automotive vehicle. The rest of the chapters of this thesis are designed as follows:

- Chapter 2: The chapter discusses the concepts and background of the thesis. It contains a discussion about threat, STRIDE threat modeling tool, and six elements of STRIDE.

- Chapter 3: The chapter discusses the literature review of the thesis. It contains a discussion about the vulnerability of an infotainment HPC and a summary of previous research that was implemented in this field.

- Chapter 4: The chapter discusses the proposed system components and methodology of the thesis. It contains a discussion about the components detail of an infotainment HPC and the way through which we implemented the thesis.

- Chapter 5: The chapter discusses the threat modeling and mitigation of threats to the system of the thesis. It contains different threat models such

as PASTA, DREAD, STRIDE, and so on. It also contains an implementation of threat modeling and identification of threats.

- Chapter 6: The chapter discusses the result and discussion of the thesis. It contains treatment for the threats which will mitigate the threats.

Chapter 2

Concepts and Background

2.1 What is Threat ?

The automotive industry is constantly coming up with innovative ways to connect cars, from the engine to the cockpit. These modern devices alter how people operate and perceive their vehicles. An automobile is no longer just for transportation from point A to point B, but cars are rolling data centers that transmit a wealth of actionable intelligence to the networks and systems around them. However, that same information is also a valuable commodity to hackers – who are looking to steal it at any cost. When a system is connected to a network, it becomes vulnerable to a cyber adversary.

Where automobiles were once driven by wheels and an engine, now are a sort of data network on wheels. Yet new technical developments also bring new network threats and vulnerabilities. Any situation or occurrence that has the potential to negatively affect a vehicle's operations, its assets, or a person's personal information through a system— including illegal access, the destruction, disclosure, alteration, and/or denial of service—is considered a threat in an automobile vehicle [4]. WiFi, Bluetooth, LTE and 5G, CAN bus, V2X, and the entire infotainment system are all entry points that pose serious security risks for automotive manufacturers. New technologies such as Voice-as-an-Interface may further expand the attack surface from the vehicle to the consumer through connected ecosystems such as Amazon, Apple, and Google.

2.2 Why Threat Modeling ?

Threat modeling is an essential process used in the field of cybersecurity to proactively identify potential security risks and vulnerabilities in a system, application, or process. This process involves analyzing and modeling the potential threats that a system or application may face, and identifying the most critical vulnerabilities that need to be addressed.

One of the common reasons why threat modeling is used in cybersecurity is to identify potential threats. Threat modeling helps organizations to examine their systems and applications from an attacker's perspective and identify potential vulnerabilities [5]. This allows organizations to understand where the most significant threats may come from and take steps to prevent them.

Another important benefit of threat modeling is that it helps organizations prioritize their security efforts. By identifying the most critical threats, organizations can focus their security efforts on addressing those threats first. This ensures that the most critical vulnerabilities are addressed promptly and reduces the risk of a security incident occurring.

Threat modeling also helps to reduce security risks. By identifying and mitigating potential security risks before they are exploited by attackers, organizations can significantly reduce the likelihood of a data breach or other security incident occurring. This can help to protect sensitive data, prevent financial losses, and maintain customer trust.

In addition to these benefits, many regulations and standards require organizations to conduct regular threat modeling as part of their compliance requirements. For example, PCI DSS, HIPAA, and ISO 27001 all require regular threat modeling to ensure that organizations are taking the necessary steps to protect sensitive data and comply with industry regulations.

The key steps of threat modeling process are:

- Set Objectives: The first step in threat modeling is to clearly define the objectives of the process. This involves understanding what the system

is intended to do, who will use it, and what assets need to be protected. Defining objectives also helps to prioritize the threat modeling effort and ensure that the team is focused on the most important aspects of the system.

- Visualization: The second step is to create a visual representation of the system. This can take the form of a data flow diagram, architectural diagram, or other graphical representation. Visualization helps to identify the components of the system, the data flows between them, and the points of interaction with external entities.

- Identify Threats: The third step is to identify potential threats to the system. This involves using a structured approach, such as STRIDE or PASTA, to systematically identify and categorize potential threats. Threats can come from both internal and external sources, and may include attacks such as social engineering, injection attacks, and denial of service.

- Mitigation: The fourth step is to identify and implement mitigation strategies to address the identified threats. Mitigation strategies can take the form of technical controls, such as firewalls and intrusion detection systems, or non-technical controls, such as policies and procedures. The goal is to reduce the likelihood and impact of the identified threats.

- Validation: The final step is to validate the threat model and ensure that the mitigation strategies are effective. This may involve testing the system using techniques such as penetration testing or vulnerability scanning. It is important to continually review and update the threat model as new threats emerge or the system evolves. Validation helps to ensure that the system is secure and that the threat modeling effort was effective.

In conclusion, threat modeling is a crucial part of any comprehensive cybersecurity strategy. By identifying potential threats, prioritizing security efforts, and reducing security risks, organizations can protect their sensitive data, prevent financial losses, and maintain customer trust.

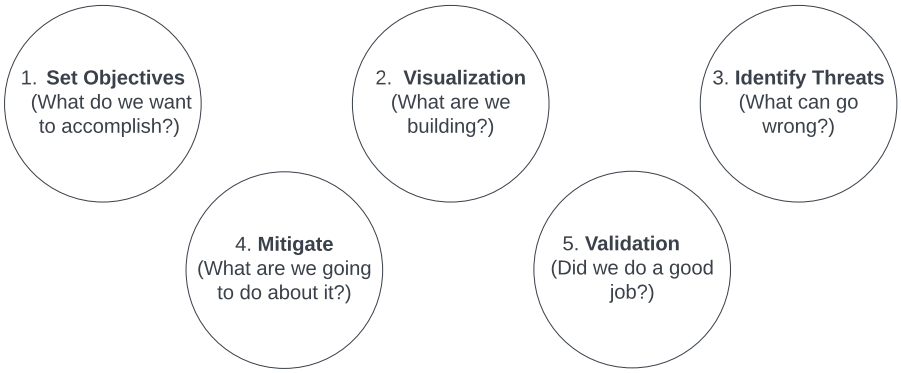

Figure 2.1: Steps of Threat Modeling

2.3 STRIDE Threat Model

The methods by which today's cyber attackers carry out big-bang cyber attacks are evolving at an ever-increasing rate. Some of these strategies include hacking suppliers in order to gain access to their customers or exploiting vulnerabilities in a piece of user information in order to attack an automobile. As a result, when developing an automotive vehicle, developers must be more alert to threats than ever before. But they can't be sure they've thought of everything because there are so many new threats. A framework like STRIDE threat modeling can assist in this regard. Developers and organizations can use STRIDE threat modeling to identify cybersecurity threats to their applications, prioritize them according to impact and likelihood, and develop mitigation strategies [6]. STRIDE stands for "spoofing," "tampering," "repudiation," "information disclosure," "denial of service," and "elevation of privilege," which are all types of security violations. The developer must consider his system and whether an attacker can use a threat from any of these classes to gain access to it in order to ensure that the application adheres to these security properties.

The Threat Modeling Tool helps one to answer certain questions, such as the ones below:

- How can an attacker change the authentication data?

- What is the impact if an attacker can read the user's personal information?
- What happens if access is denied to the user's personal profile?

STRIDE threat modeling is useful for developers on its own, but it is also part of a larger methodology that gives security teams a practical framework for identifying threats and dealing with them by defining security requirements, creating an application diagram, identifying threats, mitigating threats, and confirming that threats have been reduced. The six threat groups that are taken into consideration in the STRIDE threat modeling framework focus on various aspects of an application's security. This encourages developers to consider the threats that could affect every part of an application or system and the ways they can protect themselves from them from the beginning of the development process.

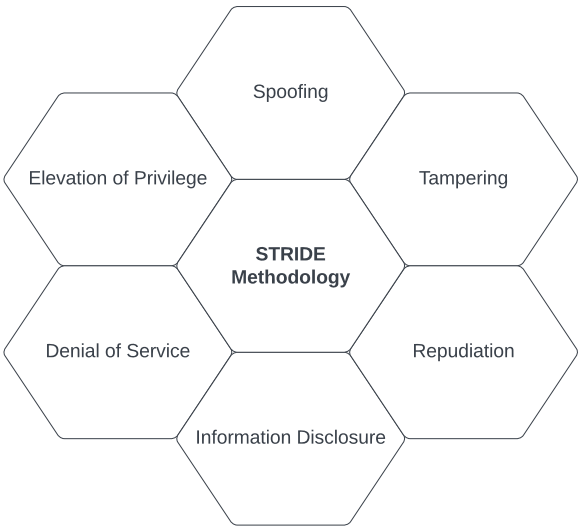

Figure 2.2: STRIDE Methodolody

The six elements of STRIDE threat modeling are:

2.3.1 Spoofing

When attackers successfully impersonate a trusted source and gain access to crucial user data or information, this is known as a spoofing attack. Social engineering is often used in spoofing to get users to give information like usernames

and passwords [7]. Attackers will use the information to access the application and then infect the network once they have it. In the automotive vehicle, an in-vehicle controller area network (CAN) bus is vulnerable because of increased sharing among modern autonomous vehicles and the weak protocol design principle [8]. Spoofing attacks on a CAN bus can be difficult to detect and have the potential to enable devastating attacks.

Spoofing attacks also include cookie replay attacks, session hijacking, and cross-site request forgery (CSRF) attacks. Examples of Spoofing:

- All activities that are typically carried out by the user may be carried out by an attacker by spoofing the processes running on the board computer of the infotainment HPC of an automotive vehicle. As a result, the attacker is able to perform actions that should not be possible.

- An attacker maliciously gains the credentials of a registered user the system and is able to log in as that user. As a result, the attacker is able to perform all actions that the registered user is able to perform.

Since spoofing is an attack on user authentication, the best form of prevention is to implement secure user authentication methods, including both secure password requirements and multi-factor authentication (MFA).

2.3.2 Tampering

The deliberate alteration of a system in order to alter its behavior is referred to as tampering. In order to alter system data such as user credentials and permissions or other crucial components, attackers will attempt to compromise applications by tampering with target parameters or code. In the automotive vehicle, tampering denotes deliberate and unauthorized manipulations of vehicle components, which alter vital vehicle functions aimed at gaining certain advantages [9]. The tamperer has physical access to the vehicle, and it performs persistent, long-term changes to components in order to gain particular advantages. As such, the tamperer

may integrate new components, alter existing ones, inject new communication frames, suppress trouble codes, reprogram ECUs, etc. A key problem, especially in the case of heavy-duty vehicles, is tampering with the vehicle's environmental protection system (EPS). Examples of Tampering:

- An attacker is able to access and modify board computer data of an automotive vehicle due to a lack of access privileges checks in a new feature that was recently developed. The new feature doesn't properly use the access privileges control method.
- An attacker is able to directly access a database that is exposed on the internet. By modifying the data in the database, the in-vehicle data is directly modified at the source.

Tampering attacks such as Cross-Site Scripting (XSS) and SQL injection damage the integrity of the system. In order to protect against tampering, the system should be designed to validate user inputs and encode outputs. Static code analysis should be used to identify vulnerabilities to tampering in the system both during the development stage and once the system is in production.

2.3.3 Repudiation

A repudiation attack is an attack on the validity and integrity of actions on the system. In an automotive vehicle, repudiation attacks take advantage of a lack of controls that properly track and log user actions, using this lack to manipulate or forge the identification of new, non-authorized actions, delete logs or log the wrong data to log files and deny actions or receipt of service. Examples of Repudiation:

- The Board computer of an automotive vehicle could be attacked by an attacker if the system lacks controls to properly track and log users' actions, allowing for malicious manipulation or faking the discovery of new actions.

Developers can build non-repudiation, or the assurance that someone can't deny the validity of an action, by incorporating digital signatures in the application which provide proof of actions, or by ensuring that there are full, tamper-proof logs in place.

2.3.4 Information Disclosure

Information disclosure is when the system unintentionally reveals information about the system that can be used by attackers to compromise the system. Information disclosure can come from developer comments that are left in the system, source code that provides parameter information, or error messages that contain too many details, revealing data about users, sensitive commercial or business data, and technical details about the application and its infrastructure. In the automotive vehicle, information disclosure can occur if the private information of the user gets exposed. This information can then be used by attackers to force access to the system gathering information about user, which can be used in further crime, or to gain privileges which in turn will give access to more sensitive areas of the system. Examples of Information Disclosure:

- An attacker accesses the system that should only show confidential information about the currently logged-in user. However, the attacker is also able to retrieve confidential information about other users who have previously used the vehicle.

- An attacker accesses a database through malicious access to the underlying operating system and discloses the confidential database information on the internet.

Developers are at the heart of preventing information disclosure vulnerabilities in the system. Error messages, response headers, and background information should be as generic as possible to avoid revealing clues about the application's behavior. Proper access controls and authorizations should be in place to prevent unauthorized access to information.

2.3.5 Denial of Service

Denial of service (DoS) attacks flood the target with traffic, triggering a crash, and shutting it down to legitimate traffic. DoS attacks typically cost time and money, but do not cause other damage to their victims. The most common form of DoS attack is a buffer overflow attack which simply sends too much traffic to the application. Other attacks exploit vulnerabilities to cause systems to crash. The Denial of Service (DoS) attack is one of the most common and popular attacks in the automotive vehicular system. In this attack, attackers try to make the resources and services unavailable to the vehicles. They do so by sending a large volume of messages through the network. Unable to handle the huge amounts of data, the board computer inside the vehicles and the Roadside Units (RSUs) shut down and critical systems and commands that ensure vehicle and driver safety cannot function as intended. In a DDoS (Distributed Denial of Service) attack, multiple malicious vehicles or devices target single or multiple network nodes. Thus making the attack much more dangerous. Examples of Denial of Service:

- An attacker sends many thousands of fake requests to the board computer of the automotive vehicle. As a result, the system is so busy responding to fake requests that no more resources are available to respond to valid requests from valid users.

DoS attacks can target both the network layer or the application layer. Applications can be protected against DoS attacks by configuring firewalls to block traffic from certain sources such as reserved, loopback, or private IP addresses, or introducing rate limiting to manage traffic.

2.3.6 Elevation of Privilege

Privilege escalation attacks exploit vulnerabilities and misconfigurations in the system to gain illicit access to elevated or privileged rights. Privilege escalation attacks may exploit credential and authentication processes, compromise vulnerabilities in code and design, take advantage of misconfigurations, or use malware

or social engineering to gain access. In the automotive vehicle, Without the required authorization, an attacker might obtain access to the board computer and carry out privileged operations.

- An attacker is registered as a normal user in the system but is able to maliciously perform administrative actions that only an administrator should be able to perform.
- An attacker does not have any access to an system at all. However, due to a configuration error the attacker is actually able to access the systemn.

Protection against escalation of privilege should be built into the system at the development stage. This includes managing the identity lifecycle, enforcing the principle of least privilege for all users, hardening systems and applications through configuration changes, removing unnecessary rights and access, closing ports, and more.

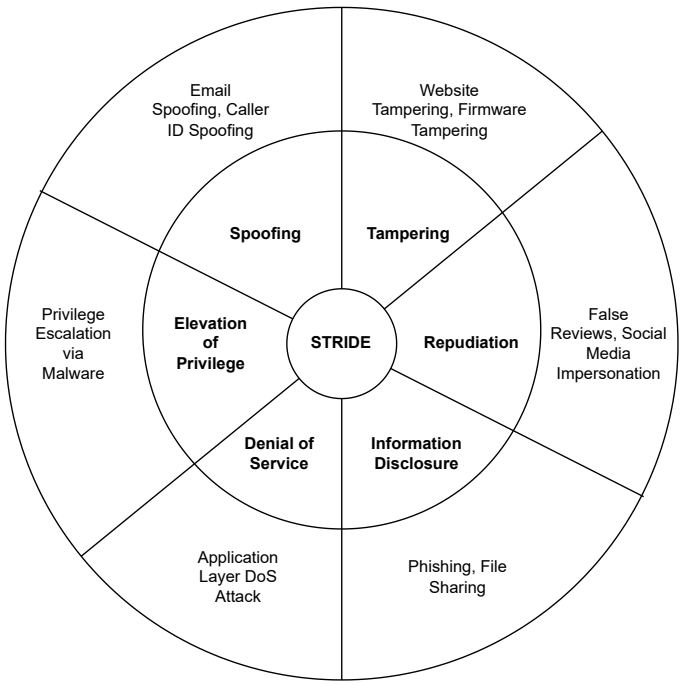

Figure 2.3: STRIDE Methodolody with Examples

2.4 Mitigation Strategies

Mitigation in cybersecurity refers to the process of reducing or minimizing the impact of a cyber threat or attack. Cybersecurity threats can include malware, phishing scams, ransomware attacks, and more. Mitigation techniques can help prevent these threats from compromising sensitive data, damaging systems, or disrupting business operations.

The goal of mitigation is to prevent or reduce the damage caused by a cyber attack. This can include actions such as implementing security controls to prevent unauthorized access, identifying and patching vulnerabilities in software and systems, and educating employees about safe browsing practices and cybersecurity risks [10].

Mitigation is an important part of a comprehensive cybersecurity strategy that also includes prevention, detection, and response. By implementing mitigation techniques, organizations can reduce the likelihood and impact of cyber attacks, and ensure the confidentiality, integrity, and availability of their data and systems. There are several mitigation techniques that can be employed to address threats in cyber security. Some of the most common techniques include:

- Firewall: A firewall is a security device that monitors and controls network traffic. It is placed between the organization's internal network and the internet to prevent unauthorized access to the organization's network. Firewalls can be hardware or software-based, and they use predefined security rules to block or allow traffic based on its source, destination, and type.

- Encryption: Encryption is the process of converting data into a code to prevent unauthorized access. It can be used to protect data in transit, such as email or online transactions, and data at rest, such as files stored on a computer or server. Encryption uses algorithms to scramble data, and it requires a key to unlock the data.

- Access control: Access control is the process of limiting access to a system or data based on predefined rules. It ensures that only authorized personnel can access sensitive data. Access control mechanisms include passwords, biometrics, and security tokens.

- Regular updates: Software and operating system updates often include security patches that address known vulnerabilities. Regular updates can help prevent exploits of known vulnerabilities by hackers. Organizations should ensure that all software, applications, and operating systems are updated regularly.

- Data Backup and Recovery: Regularly backing up data and testing data recovery procedures can help minimize the impact of security incidents, such as ransomware attacks or data breaches.

2.5 Summary

Nowadays, vehicles are becoming more and more connected. The links between cars and other vehicles as well as the connections between vehicles and infrastructure enable the provision of a wide range of services. Due to user connections made possible by the interconnection of smart gadgets and automobiles, security vulnerabilities are also growing. Any situation or occurrence that has the potential to negatively affect a vehicle's operations, its assets, or a person's personal information through a system— including illegal access, destruction, disclosure, alteration, and denial of service—is considered a threat in an automobile vehicle.

Threat modeling is a structured approach used in cybersecurity to identify, analyze, and mitigate potential threats to a system or application. It involves identifying potential attackers, their motivations, and the methods they may use to exploit vulnerabilities in the system or application. Threat modeling can help organizations understand the potential impact of a cyber attack and prioritize mitigation efforts. It can also help inform design and development decisions, en-

suring security is built into the system or application from the beginning. By using threat modeling, organizations can proactively address potential vulnerabilities and reduce the risk of a successful cyber attack, ultimately improving overall security posture.

STRIDE is the method that can be used to identify the threats that occur in an automotive vehicle. STRIDE is based on six common types of threats that we encounter today in applications, systems and so on. Spoofing relates to maliciously impersonating a user or a system. Effectively authenticating a user or system at the right time prevents a spoofing attack from being successful. Tampering relates to maliciously modifying (or creating, updating, deleting) data. Integrity is a security property that defines the importance of data being accurate. Repudiation relates to claiming that an action does or does not belong to a user, person or system. Non-repudiation is the ability to prove that an action was definitely performed by a user, person or system. Information Disclosure relates to having unauthorized access to confidential data. Confidentiality is a security property that defines the importance of data being kept secret. Denial of Service relates to overloading a system or service with fake requests so that it cannot respond to legitimate requests effectively or timely. Availability is a security property that defines the importance of being available. Elevation of Privilege relates to gaining higher acces privileges than intended. Authorization is the security mechanism to determine which rights a user, person or system should have. Mitigation is an important component of cybersecurity that involves reducing or minimizing the impact of a cyber attack. Cybersecurity threats such as malware, ransomware, and phishing attacks can cause significant damage to organizations, including the loss of sensitive data, damage to systems, and disruption to business operations. Mitigation techniques, such as implementing security controls, identifying and patching vulnerabilities, and educating employees about safe browsing practices, can help prevent these threats from compromising sensitive data and systems. By proactively implementing mitigation strategies, organizations can reduce the

likelihood and impact of cyber attacks, ensure business continuity, and protect their reputation and customer trust.

In the next chapter, the literature review will be discussed that was conducted as part of this research. This review opens with an overview of the research subject.

Chapter 3

Literature Review

The number of connected vehicles that connect to the Internet has greatly increased and by 2035 almost all new cars will be connected vehicles [11]. In-vehicle infotainment (IVI) systems are integrated into connected automobiles to deliver information and entertainment. Modern IVI systems include a remote service that permits control using a user smartphone connected to the Internet from outside the vehicle. In addition to standard navigation, radio listening, and playing multimedia material, it also achieves an in-vehicle network service (in-vehicle Wi-Fi service) that connects the automobile to the outside world.

Many remote interfaces that offer a range of connected services are available on the IVI system. As a result, an attacker may target these interfaces and use a system weakness to take anomalous remote control of the vehicle. In reality, prior research shown that a perpetrator can readily operate an automobile without a valid license [12]. Remote control services may implement countermeasures against these attacks such as encrypting all communications, adequately managing the secret key, and implementing authentication among the smartphone APP, back-end servers, and cars. However, this attacks - countermeasures cycle has been repeated many times and such countermeasures must be evaluated because the attack techniques evolve and become more sophisticated over time.

A vulnerability in services implemented in the IVI systems was looked into from the perspective of system intrusion, in [13]. In fact, it was demonstrated that a service vulnerability through the Wi-Fi interface may be used to obtain the root privilege of the IVI system. This implies that the hacker can access the system remotely. Once the attacker gains access to the system with root privileges, the

attacker is allowed to modify the system settings and extract significant user information [14]. There are papers that look into the potential for DoS assaults to halt system operation; such prior studies concentrate on how to get into IVI systems. The countermeasures in the IVI system against such attacks may be insufficient.

Investigating security issues with in-vehicle apps, particularly those involving inter-component communication (ICC) among these apps, has been done in [15]. With a communications object called intent, ICC enables programs to share data across or inside themselves. In the event of insecure communication, malicious apps may hijack or spoof intent, which could result in the leakage of sensitive user data to a hacker's database. It will be necessary to evaluate these apps for user privacy, safety, and security. In [8] , Since the CAN bus is a core component of in-vehicle communication, and the security weakness of the CAN bus design is intrinsic, adversaries can typically break the CAN bus to attack a vehicle or take full control of the ECUs by injecting spoofing messages. Diagnostic messages were sent when the victim vehicle was traveling at below 10 miles per hour, satisfying the safety constraints on electronic control units (ECU) that respond to such messages. Attacks can likely be made much more destructive if safety constraints on diagnostic messages become compromised.

In [16], Koscher et al. experimentally assess the security aspects of a contemporary car and show the brittleness of the underlying system structure. They demonstrate that an attacker who has gained access to virtually any ECU at a particular point in time can use this to completely bypass a variety of safety-critical systems and control a variety of automotive functions, such as disabling the brakes, selectively braking individual wheels on demand, stopping the engine and other similar actions. The method of exploiting security flaws affecting in-car communications to attack the infotainment system and get data about both the vehicle and driver is documented in [17].

In this study, it is identified that opportunities for adversaries to take con-

trol of the in-vehicle network, which can compromise the safety, privacy, reliability, efficiency and security of the transportation system. Numerous studies have demonstrated the deteriorating impact of an attacker on various driving performance measures. Actually, cyber-security threats take advantage of flaws brought on by the widespread use of ICT equipment installed in vehicles. For instance, by taking advantage of security flaws in infotainment HPC, it is possible to get sensitive information like the list of contacts, phone numbers, messages, and so on. Leveraging on these issues, we focus on the security threats related to in-vehicle infotainment HPC and provide treatment to the threats. There are different threat modeling tools available to identify threats; however, we adopted STRIDE, a Microsoft corporation product, in our modeling. We have also performed treatment to the threats.

This chapter presents security threats to IVI systems installed in recent connected automotive vehicles. We present a security analysis on (a) the automotive vehicle control services from the outside to the car, (b) the in-vehicle network services that connect from inside the car to the outside, (c) the leakage of user information due to security adversaries, and so on. Furthermore, in the next chapter about the proposed system components of the in- vehicle infotainment HPC and the details of the components.

Chapter 4

Proposed System Components and Methodology

4.1 Methodology

Methodology refers to the overall approach or set of principles and procedures used to conduct a particular activity or field of study. The purpose of the methodology is to ensure the reliability, validity, and accuracy of the results obtained through research or problem-solving.

This research aims to perform threat modeling and provide treatment to the threats of in-vehicle infotainment HPC by following the approach displayed in Figure [18].

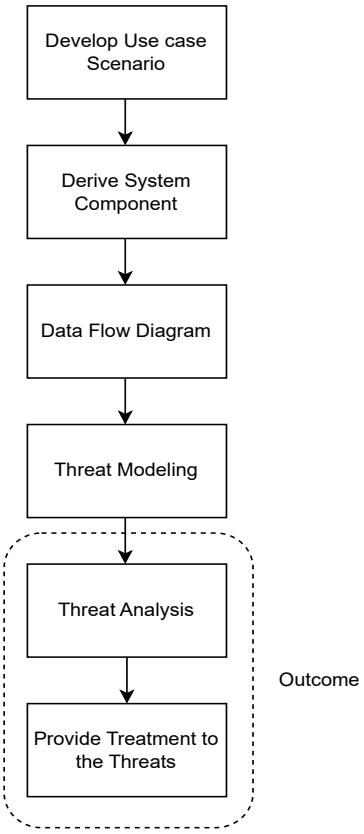

Figure 4.1: The Approached Methodology

The use case scenario intends to explain infotainment HPC from the perspective of the proposed system components of the infotainment system of an automotive vehicle. Simply, the board computer is controlling all the operations that are happening in the infotainment system of the automotive vehicle. The drive uses NFC, bluetooth, wifi and cellular network to transfer data and information. The CAN network is used by the board computer to communicate with the sub-sections of the automotive vehicle. While communicating with the outside world or transferring data, the data paths can be attacked by the attacker. An attacker is any person, including an insider, group, or entity that engages in hostile acts in order to damage, expose, disable, steal, obtain unauthorized access to, or otherwise misuse a resource [19].

In the research, at first, we derived the system components and generated a data flow diagram from the derived components. Then we performed threat modeling with the help of STRIDE, a Microsoft corporation product. The name STRIDE is constructed from the first character from the six threat categories namely Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Each threat category is a violation of Authenticity, Integrity, Non-repudiation, Confidentiality, Availability, and Authorization respectively. From the threat modeling tool, the threat report has been generated. We have listed the threats and on the basis of the threats we have provided treatments for the threats.

4.2 Driving System Components

Infotainment HPC (High-Performance Computing) in automotive vehicles refers to the advanced computing capabilities that power the multimedia and communication systems within a vehicle. Infotainment systems provide a range of features and functions, including music and video playback, navigation, hands-free calling, and internet connectivity.

HPC, in particular, refers to the use of powerful processors and graphics cards

to support these functions. This allows for faster and more efficient processing of large amounts of data, which is essential for delivering a high-quality user experience in modern vehicles.

In addition to providing entertainment and communication features, infotainment HPC systems can also support advanced driver assistance systems (ADAS) and other safety features, such as collision detection and lane departure warnings. These systems rely on the same high-performance computing capabilities to analyze sensor data and make split-second decisions to help prevent accidents.

The components of infotainment HPC (High-Performance Computing) in automotive vehicles can vary depends on the specific system and the features it supports. In [20], below architectre is described of infotainment HPC. But from all the components, we taken the marked components which are car audio system, speaker, ADC and GPS.

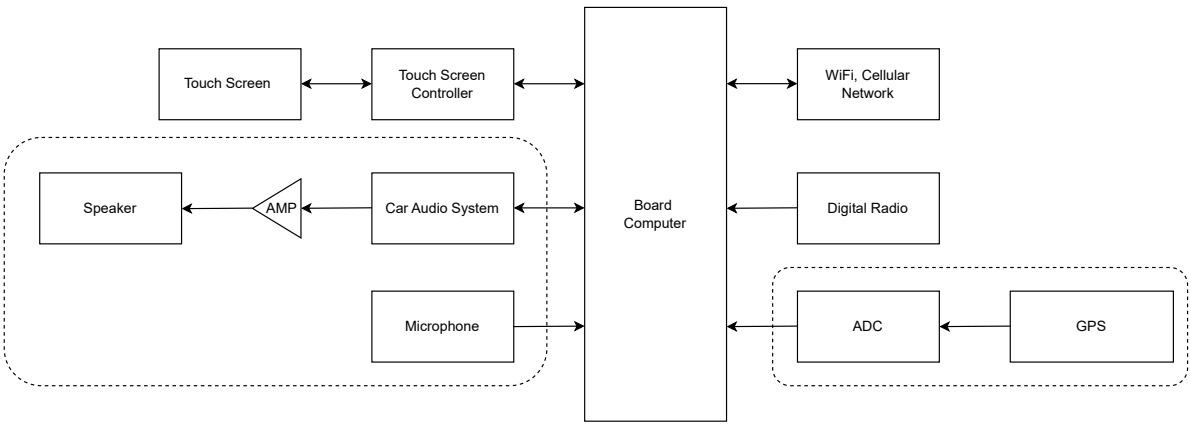

Figure 4.2: Derived System Components (1)

In [21], below architectre is described of infotainment HPC. But from all the components, we taken the marked components which are video buffer, touch screen controller, rear screen, touch screen, USB interface, portable media player and temperature sensor.

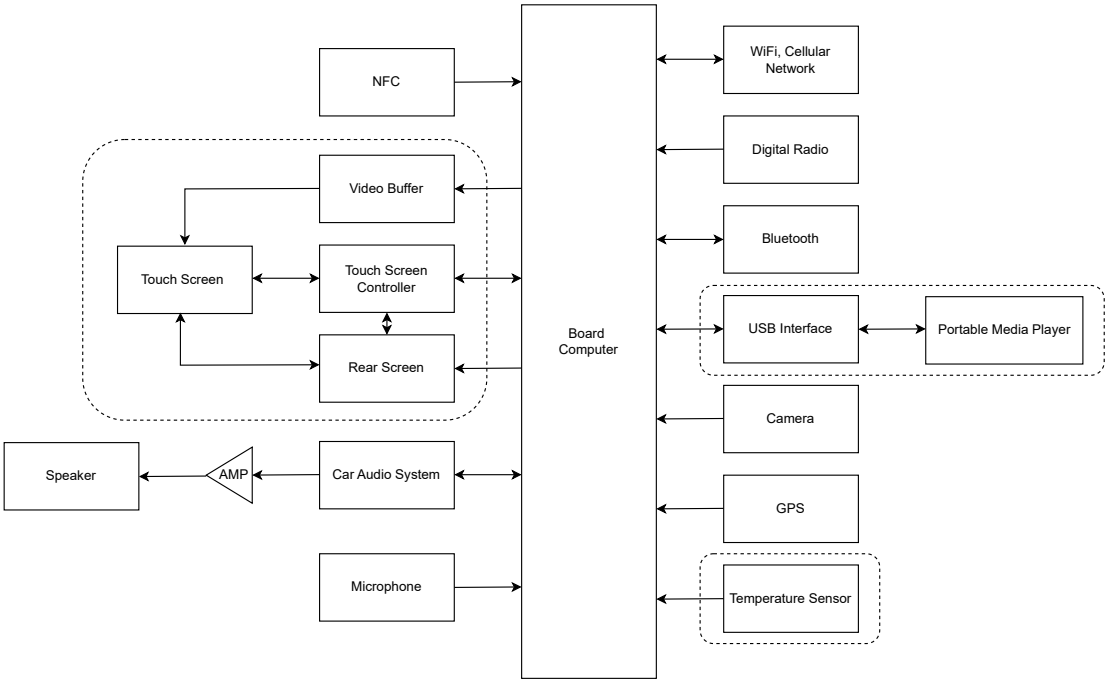

Figure 4.3: Derived System Components (2)

In [22], numerous components are described of infotainment HPC. But from all the components, we have taken the marked components which are NFC, bluetooth, wifi and cellular network.

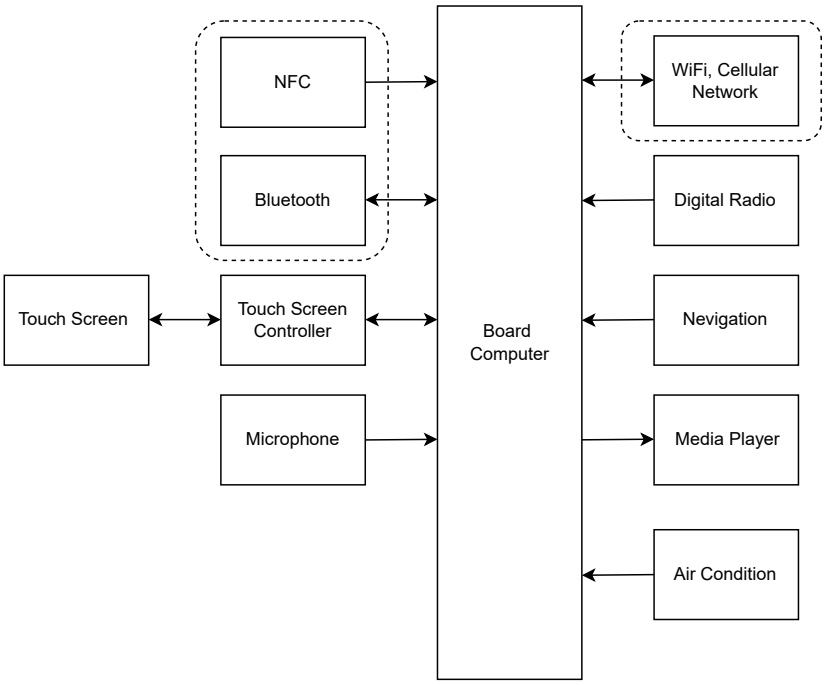

Figure 4.4: Derived System Components (3)

In [23], numerous components are described of infotainment HPC. But from all the components, we have taken the marked components which are camera, digital radio, CAN network and car automation network.

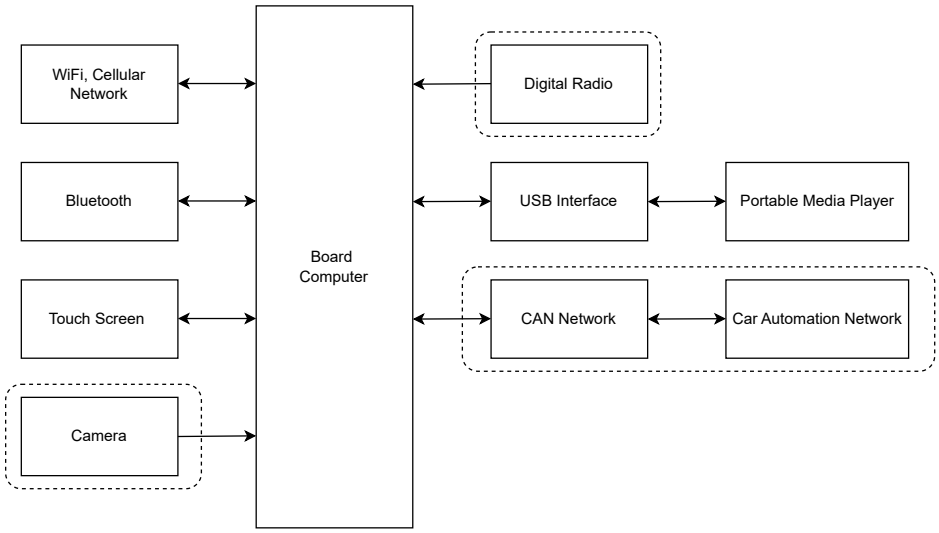

Figure 4.5: Derived System Components (4)

In the final proposed data flow diagram for the in-car infotainment HPC, we did not use all the components from previous references. Instead, we took partial components from previous references and integrated them with new components to develop the proposed data flow diagram. The diagram includes several key components to ensure the efficient and reliable operation of the system.

The final proposed data flow diagram includes a range of components that enable the various features of the infotainment system. These components include Near Field Communication (NFC) for secure communication between devices, a video buffer for smooth video playback, a touch screen controller and touch screen for user input, a rear screen for displaying information to passengers in the back seats, a car audio system with microphone and speaker for audio output and input, a camera for recording video and capturing images, wifi and cellular network capabilities for internet connectivity, digital radio for audio playback, bluetooth for wireless communication with other devices, a USB interface for connecting external devices such as flash drives, a portable media player for playing audio and video files, a Controller Area Network (CAN) network for communication with

other devices in the car, a car automation network for integrating with other systems in the car, an Analog-to-Digital Converter (ADC) for converting analog signals to digital signals, GPS for navigation and location-based services, and a temperature sensor for monitoring the temperature inside the car.

Overall, the proposed data flow diagram includes a wide range of components that work together to provide a comprehensive infotainment experience for users in the car.

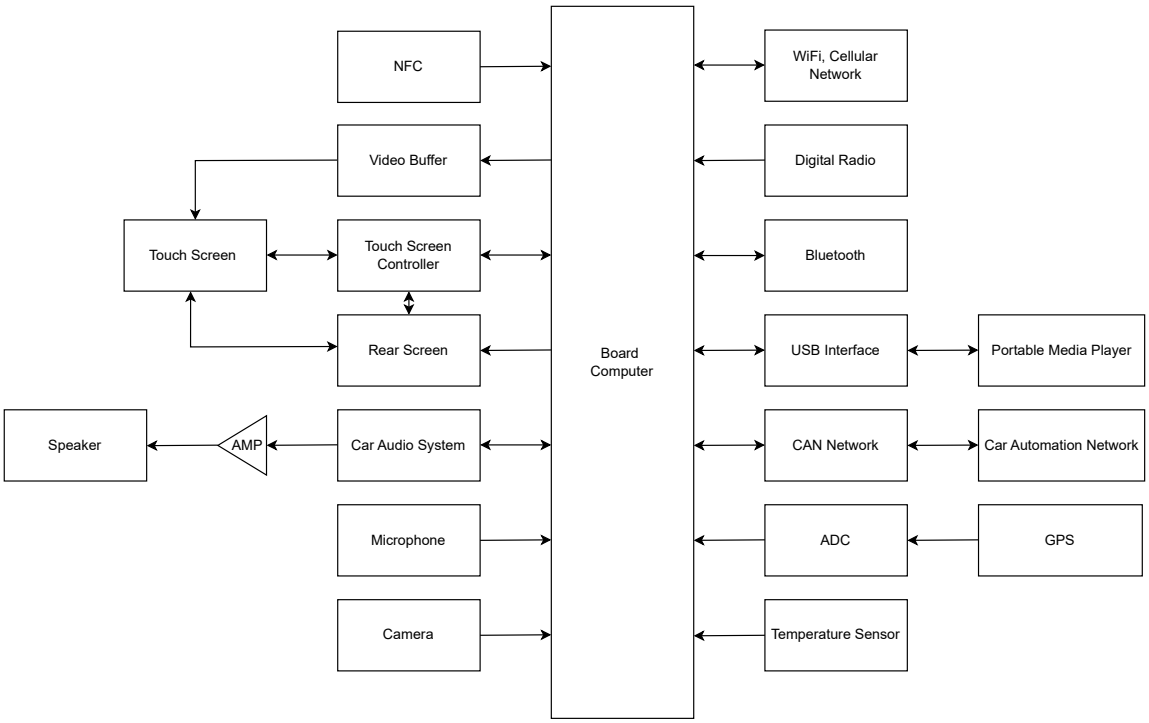

Figure 4.6: Proposed System Components of In-Car Infotainment HPC

4.3 Description of System Components

The typical architecture of an infotainment hpc is described below. The input/output devices for communication with the driver are:

- NFC (Near field communication): NFC lets devices communicate wirelessly. Near Field Communication (NFC) technology allows users to make secure transactions, exchange digital content, and connect electronic devices with a touch. NFC transmissions are short range (from a touch to a few centimetres) and require the devices to be in close proximity.

- Video Buffer: Video buffering is pre-loading data segments for streaming video content. The data is preloaded into a reserved section of memory.

- Touch Screen Controller: A touchscreen controller is a circuit (or multiple circuits) that connects the touchscreen sensor to the touchscreen device itself.

- Rear Screen: If the vehicle has a rear seat infotainment system from general motors accessories, the passengers can play media from various sources on two monitors located behind the front-seat headrests. These monitors work much like a smart TV.

- Touch Screen: Every new vehicle has an in-dashboard touch screen to control the air conditioning, radio, navigation, external camera, and other applications.

- Car Audio System: The fundamental component of a car audio system is a device that collects and transmits sound waves in order to generate music through speakers. Before being output from the speakers, these sound waves are first sent to filters. The car stereo, which is in charge of carrying out all crucial tasks for a car system, is the brain of the apparatus.

- Speaker: In order to produce sound, speakers transform an electrical signal into mechanical energy by moving the speaker cone back and forth. The vibrations in the air that we perceive as sound are actually caused by a speaker cone.

- Microphone: Due to the safety issue of driving, the traditional hand-operated interface has been replaced gradually by voice control. This technology uses the microphone to receive the driver's voice commands and translate them to interface commands to control the system.

- Camera: A car dashboard camera is mounted on the front windscreen, that is behind the interior rearview mirror. This position gives a clear vision

for the camera to capture what's going on ahead. A car recording camera is connected in such a way that it automatically switches on, and starts recording as soon as the driver switches on the car's ignition. So, one will never miss out on a recording while driving his car with a dashboard camera.

- WiFi, Cellular Network: It connects the computer and smart devices such as cameras or thermostats to the Internet. This means one can access web content, stream favorite TV shows, check email, etc., all while driving.

- Digital Radio: Digital radios automatically tune to all available digital stations, making it easy to flick through. It provides entertainment to the user of the car.

- Bluetooth: One should be able to navigate using his app of choice; receive, listen to, and send text messages using voice controls; make phone calls; and listen to audio streamed from phone. The goal of Bluetooth in cars is to enable hands-free connectivity, so one don't have to hold his phone to call a friend.

- USB Interface: The majority of gadgets in automobiles use USB ports. They serve as a means of data and information sharing between devices like smartphones and in-car multimedia systems in addition to serving as a means of device charging.

- Portable Media Player: A portable media player is a portable consumer electronics device capable of storing and playing digital media such as audio, images, and video files. The user can store their favourite songs, audio or video in it.

- CAN Network: The Controller Area Network (CAN) bus protocol is used for communication between sub-systems in motor vehicles when the use

of micro-controllers in engine control, window motors, airbags, anti-lock braking and so on.

- Car Automation Network: The car automation network involves the use of mechanisms, artificial intelligence, and multi-agent systems to assist the operator of a vehicle. In automated vehicles in which at least some aspect of a safety-critical control function (e.g., steering, throttle, or braking) occurs without direct driver input, car automation network is used for that.

- GPS: GPS receivers track the exact location of the GPS device and compute the time and the velocity the driver is traveling at.

- Temperature Sensor: The temperature sensor measures the coolant temperature sends information to the ECU. The water temperature sensor enables the control unit to identify engine overheating or an unusual rise in temperature.

4.4 Summary

In the chapter, the components description of the infotainment HPC of an automotive vehicle and the methodology, how we are performing the research. Where NFC is used to make secure transactions or connect to electronic devices with a touch, a video buffer is used to pre-load video data, the touch screen controller is connecting the touch screen sensors, the rear screen is used for rear seat entertainment and touch screen controls air conditioning, radio and so on. Car audio system and speaker are used for collecting and transmitting sound waves in order to generate music through the speaker. The microphone is usually used for voice control and the camera is used to capture the front view of the car. Digital camera provides entertainment to the passengers of the car and bluetooth and wifi, cellular network is used for data transfer or search information. USB interface is used to transfer music, audio, or video file from portable media players. CAN network communicates with the subsection of the system where car automation

network is also involved. GPS and temperature sensors are used to track the exact location and measure the temperature of the engine of the car respectively. The threats that may occur in the infotainment system of an automotive vehicle, we will use STRIDE, a threat modeling tool to measure those threats and provide treatments for those threats in the research.

Chapter 5

Threat Modeling and Possible Mitigation

5.1 Threat Models

Threat modeling is a method of optimizing cyber security by locating vulnerabilities, identifying objectives, and developing countermeasures to either prevent or mitigate the effects of cyber-attacks against the system. A threat model is an organized representation of all the data that influences an application's security. It essentially involves looking at the program and its surroundings via a security lens. A wide range of objects, including software, applications, systems, networks, distributed systems, Internet of Things (IoT) devices, and business processes, can be subject to threat modeling. Typically, a threat model contains a description of the subject to be modeled, assumptions that can be tested or contested in the future as the threat landscape evolves, potential threats to the system, actions that can be taken to mitigate each threat, a way of validating the model and threats, and verification of success of actions taken.

There are as many ways to fight cybercrime as there are types of cyber-attacks. For instance, some threat modeling methodologies are:

5.1.1 PASTA

PASTA stands for Process for Attack Simulation and Threat Analysis (PASTA). It is a risk-centric threat modeling method, meaning that risk plays a central role and the focus is on the highest and most relevant risks that can affect the system [24]. It offers a dynamic threat identification, enumeration, and scoring process. Once experts create a detailed analysis of identified threats, developers

can develop an asset-centric mitigation strategy by analyzing the application through an attacker-centric view.

PASTA has seven distinct stages. Each stage feeds information into the next stage. Each stage adds to the information known about the object in scope, its environment, potential threats involved, and its risks and feeds into the overall threat model [25].

The seven stages of PASTA threat modeling:

- Define the application: The first step in the PASTA threat model is to define the application or system being analyzed, including its purpose, architecture, and intended use.

- Identify security objectives: The next step is to identify the security objectives of the application or system, including confidentiality, integrity, availability, and accountability.

- Define the attack surface: The attack surface is the set of all potential attack vectors that could be used to compromise the system. This step involves identifying and analyzing the various components and interfaces of the application or system.

- Decompose the application: This step involves breaking down the application or system into smaller components and analyzing each component for potential vulnerabilities.

- Identify threats: Based on the information gathered in the previous steps, potential threats to the application or system are identified and analyzed.

- Rate and prioritize threats: Once potential threats are identified, they are rated and prioritized based on their likelihood and impact on the security objectives of the system.

- Mitigation planning: Finally, a plan is developed to mitigate or eliminate the identified threats, including the implementation of security controls and

the development of security requirements.

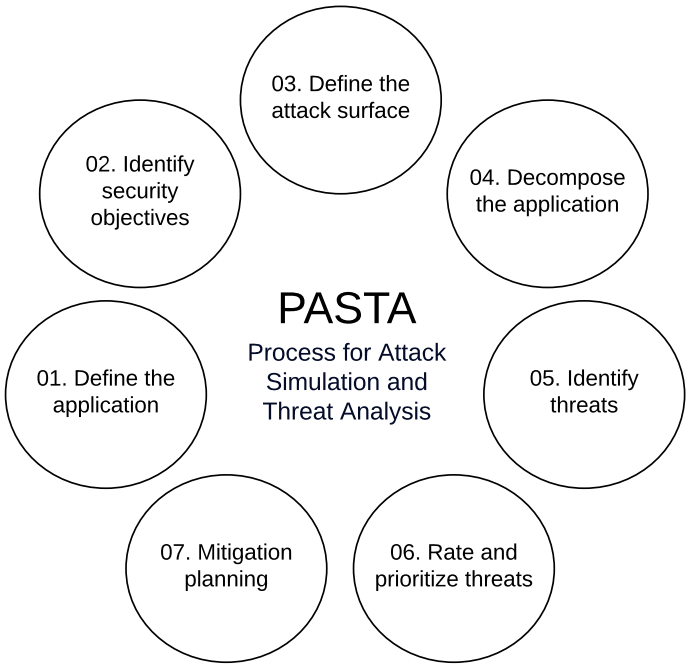

Figure 5.1: PASTA Threat Model

5.1.2 DREAD

The DREAD model quantitatively assesses the severity of a cyberthreat using a scaled rating system that assigns numerical values to risk categories [26]. The DREAD model enables analysts to rate, compare, and prioritize the severity of threats by assigning a given issue a rating between 0 and 10 in each of the above categories. The final rating, calculated as the average of these category ratings, indicates the overall severity of the risk. The DREAD model has five categories:

- Damage: Understand the potential damage a particular threat is capable of causing.
- Reproducibility: Identify how easy it is to replicate an attack.
- Exploitability: Analyze the system's vulnerabilities to ascertain susceptibility to cyberattacks.

- Affected Users: Calculate how many users would be affected by a cyberattack.

- Discoverability: Determine how easy it is to discover vulnerable points in the system infrastructure.

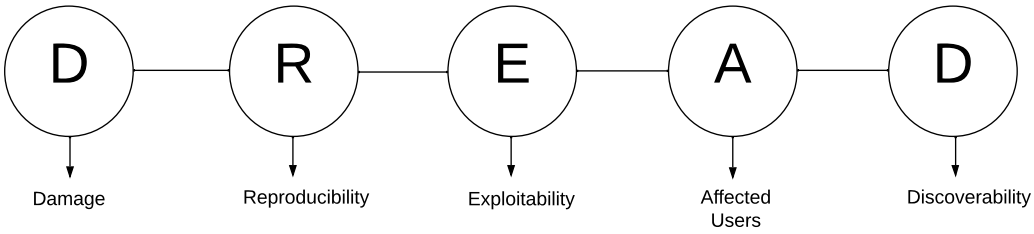

Figure 5.2: DREAD Threat Model

5.1.3 STRIDE

STRIDE is a popular threat modeling methodology that provides a framework for identifying potential threats to a system or network [6]. A methodology developed by Microsoft for threat modeling, it offers a mnemonic for identifying security threats in six categories:

- Spoofing: An intruder posing as another user, component, or other system feature that contains an identity in the modeled system.

- Tampering: The altering of data within a system to achieve a malicious goal.

- Repudiation: The ability of an intruder to deny that they performed some malicious activity, due to the absence of enough proof.

- Information Disclosure: Exposing protected data to a user that isn't authorized to see it.

- Denial of Service: An adversary uses illegitimate means to exhaust services needed to provide service to users.

- Elevation of Privilege: Allowing an intruder to execute commands and functions that they aren't allowed to.

Table 5.1: STRIDE Security Property

Threat	Desired Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

5.1.4 Attack Tree

An Attack Tree is a graphical tool used in cybersecurity to model and analyze potential attacks on a system or network. It is a type of threat modeling technique that is commonly used to identify and evaluate the different attack vectors that an attacker could use to compromise the security of a system.

An attack tree starts with the goal of the attacker, which is usually to gain access to sensitive information or to perform a specific action. The tree is then built by identifying the various steps or actions that an attacker could take to achieve the goal. Each node on the tree represents a possible attack vector, and the branches represent the different ways that an attacker could carry out the attack [27].

The attack tree is typically divided into different levels, with the top level representing the attacker's overall goal, and the lower levels representing the different ways that the goal could be achieved. At each level, the attack tree can be expanded further to include more specific details about the attack, such as the tools or techniques that an attacker might use.

Once the attack tree has been constructed, it can be used to assess the overall security of a system by evaluating the likelihood and impact of each attack vector. This can help organizations to prioritize their security efforts and allo-

Table 5.2: Goal of Attack Tree

Attack Tree Goal	Description
Gain access to sensitive data	The attacker's goal is to access confidential or sensitive information, such as customer data, financial records, or intellectual property.
Take control of a system	The attacker's goal is to gain control of a system or network, allowing them to execute commands, modify data, or launch further attacks.
Disrupt business operations	The attacker's goal is to disrupt the normal operations of a business or organization, such as by causing system outages, stealing data, or spreading malware.
Sabotage or damage systems	The attacker's goal is to intentionally damage or destroy systems or equipment, either for financial gain or to cause harm to the organization.
Extort money or resources	The attacker's goal is to demand payment or resources from the target organization, often through the use of ransomware or other extortion tactics.

cate resources more effectively to protect against the most likely and damaging attacks.

Overall, the use of attack trees can be a valuable tool in the field of cybersecurity, allowing organizations to proactively identify and mitigate potential security risks and vulnerabilities in their systems. Note that this table provides a high-level overview of some common attack tree goals, but there can be many variations depending on the specific threat landscape and the goals of the attackers.

5.1.5 VAST

The VAST threat model (Visual, Agile, and Simple Threat modeling) is a methodology used in cybersecurity to identify and assess potential security threats and vulnerabilities in an organization's information systems. The VAST model focuses on creating visual representations of system architecture and identifying potential attack vectors that can be exploited by adversaries [28].

The VAST threat model is based on four key components: data, users, tasks, and tools. These components are used to create a visual representation of the system and the potential threats that exist within it. The model is then used to

identify potential threats and develop strategies for mitigating them.

Data refers to the information that is processed and stored within the system. This includes user data, system logs, and other types of data that may be used to identify potential threats.

Users refer to the individuals who interact with the system, including employees, customers, and other stakeholders. The VAST model considers the actions and motivations of these users, as well as their level of access to the system.

Tasks refer to the specific actions that users perform within the system. This includes tasks such as data entry, data analysis, and system maintenance.

Tools refer to the software and hardware that is used to support the system. This includes firewalls, intrusion detection systems, and other security tools.

The VAST threat model is used to identify potential threats that may exist within each of these four components. For example, a potential threat may be identified in the data component if sensitive information is not properly encrypted or protected from unauthorized access. Similarly, a potential threat may be identified in the users component if an employee with privileged access to the system engages in malicious activity.

Once potential threats have been identified, the VAST model can be used to develop strategies for mitigating them. This may involve implementing new security measures, training users on proper security protocols, or updating system software to address vulnerabilities.

Overall, the VAST threat model is a useful tool for identifying potential cyber threats and developing strategies for mitigating them. By considering the four key components of the system, the VAST model provides a comprehensive framework for addressing potential threats and vulnerabilities in a holistic manner.

5.1.6 CVSS

The Common Vulnerability Scoring System (CVSS) is a widely-used framework for assessing the severity of vulnerabilities in computer systems and networks. It

provides a standardized method for rating the impact and exploitability of a vulnerability, allowing organizations to prioritize their response efforts and allocate resources more effectively [29].

The CVSS threat model is based on three main components: Base Metrics, Temporal Metrics, and Environmental Metrics. Each of these components provides a different aspect of the vulnerability and allows for a more comprehensive assessment of its impact and severity.

The Base Metrics include a set of measures that provide an initial assessment of the vulnerability, such as the level of access required to exploit it, the impact of a successful exploit, and the complexity of the attack vector. The Base Metrics are divided into three subcategories: Exploitability, Impact, and Scope.

Exploitability measures the level of difficulty required to exploit the vulnerability, including the required privileges, user interaction, and attack complexity. Impact measures the consequences of a successful attack, including data loss, system availability, and confidentiality breaches. Scope measures the extent to which a successful attack can impact the system or network.

The Temporal Metrics provide information about the vulnerability over time, including the likelihood of the vulnerability being exploited and the availability of a patch or other mitigation. These metrics are also divided into three subcategories: Exploit Code Maturity, Remediation Level, and Report Confidence.

Exploit Code Maturity measures the level of maturity of any known exploit code for the vulnerability, with higher values indicating more advanced exploit code. Remediation Level measures the availability of a patch or other mitigation for the vulnerability, with higher values indicating a higher likelihood of a patch being available. Report Confidence measures the level of confidence in the existence of the vulnerability, with higher values indicating greater confidence.

The Environmental Metrics allow organizations to assess the impact of a vulnerability within their specific environment, taking into account factors such as the asset value, the security posture, and the business impact. These metrics are

also divided into three subcategories: Confidentiality, Integrity, and Availability.

Confidentiality measures the impact of a successful attack on the confidentiality of the data or information. Integrity measures the impact on the accuracy or completeness of the data or information. Availability measures the impact on the availability of the system or network.

By using the CVSS threat model, organizations can better understand the severity and impact of a vulnerability and prioritize their response efforts accordingly. The model provides a common language for assessing vulnerabilities across different systems and networks, enabling better communication and collaboration between security teams and other stakeholders.

Despite the fact that there are numerous models that may be used to identify threats, we have chosen the STRIDE threat modeling tool because it is a well-accepted method accepted by academia and industry and it is used to identify threats at the component level. It is an open-source (free of cost) tool available from Microsoft called "Microsoft Threat Modeling Tool". It will concentrate on avoiding flaws and vulnerabilities in application security. Following the threat analysis, the necessary treatment and mitigation measures will be offered.

5.2 Threat Modeling Using STRIDE

Threat modeling is the process of identifying and mitigating potential threats to a system or network. The implementation of threat modeling involves a structured approach to identify, prioritize, and mitigate risks. The steps involved in the implementation of threat modeling include scoping the system or network to be modeled, defining the threat model, identifying potential vulnerabilities, prioritizing risks, developing mitigation strategies, testing and validating the model, and reviewing and updating the model on an ongoing basis.

As threat modeling is a proactive method of identifying, cataloging and prioritizing dangers, assisting in the development of effective defenses against threats. Simply, it is formed to answer the questions like "Where are the potential dan-

gers to the system?", "What are the most important threats?", and "Where the system most vulnerable?" [19]. A threat model simulates the attack and defense sides of a logical item, such as a piece of data, an application, a host, a system, or an environment, according to a NIST special publication [30].

NFC, Bluetooth, WiFi, and cellular networks are typically used to send information and commands. So, any compromise might cause information to leak or allow someone to seize control of the entire system. So, we cannot dismiss the possibility of security problems, particularly in terms of cyber security, in an automotive vehicle's infotainment HPC.

In this work, we have performed threat modeling on major data flows, and processes of DFD. We assume that the two sides that are marked in the red boundary are safe. Beside that, we have not performed threat analysis on all components in the DFD. We have not performed threat analysis on video buffer, touch screen controller, rear screen, touch screen, car audio system, speaker, camera, microphone, digital radio, GPS, and temperature sensor because there is no function of data or file transmission. We also have not performed threat analysis on USB interface and portable media player, because they have to be physically inserted into the system.

We considered only the threats which cross the trust boundary, which means, Board Computer, NFC to Board Computer (NFC to BC), Board Computer to WiFi, Cellular Network (BC to WiFi), WiFi, Cellular Network to Board Computer (WiFi to BC), Board Computer to Bluetooth (BC to Bluetooth), Bluetooth to Board Computer (Bluetooth to BC), Board Computer to CAN Network (BC to CN) and CAN Network to Board Computer (CN to BC). k. In the DFD, the circle denotes a process and the arrow represents data flow.

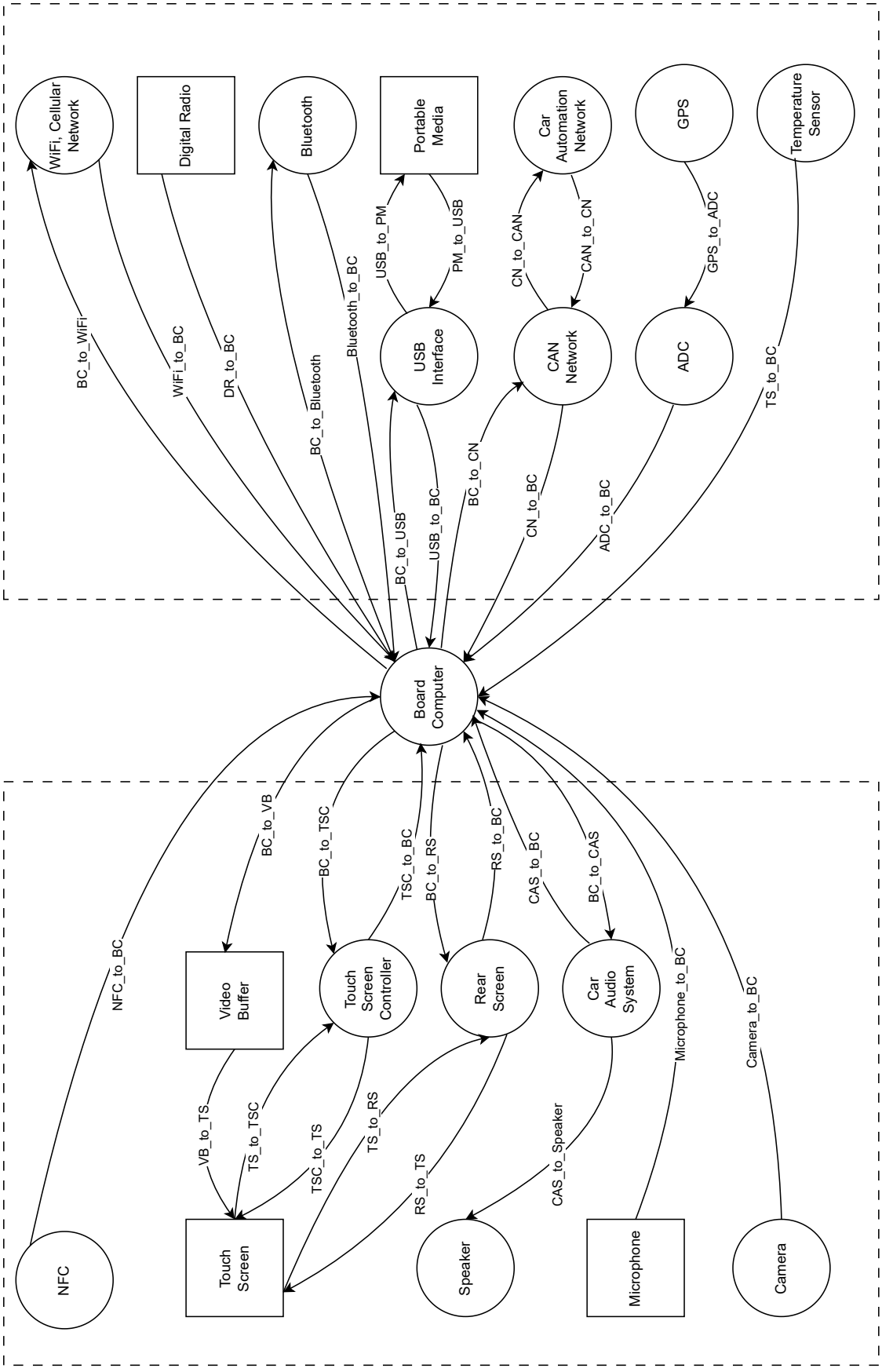

Figure 5.3: Data Flow Diagram

5.3 Identified Threats

Using STRIDE, organizations can identify potential threats by analyzing each of these categories and assessing the likelihood and impact of attacks within each category. This helps organizations prioritize their security efforts and develop effective mitigation strategies to protect their systems and networks from a wide range of potential threats.

Cyber security threats are identified here using Microsoft STRIDE. The name STRIDE is constructed from the first character from the six threat categories namely Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Each threat category is a violation of Authenticity, Integrity, Non-repudiation, Confidentiality, Availability, and Authorization respectively. Table 5.3 listed the identified threats with further details where we have used the term adversary frequently. We can explain the term as a person or organization that is not permitted to access or edit information, or that attempts to circumvent any security measures put in place to safeguard the system [31].

Table 5.3: Listing of Threats

Components or interaction	Threat No	Threat	Threat category
Board Computer	1	All activities that are typically carried out by the user may be carried out by an adversary by spoofing the processes running on the board computer.	Spoofing
Board Computer	2	An adversary may modify any given command and any instruction resulting in the modification of the system.	Tampering
Board Computer	3	The Board computer could be attacked by an adversary if the system lacks controls to properly track and log users' actions, allowing for malicious manipulation or faking the discovery of new actions.	Repudiation

Components or interaction	Threat No	Threat	Threat category
Board Computer	4	An adversary may steal or share any personal information with anyone, which may violate user's privacy.	Information Disclosure
Board Computer	5	In order to deny users of the board computer's services, an adversary may overwhelm or flood it with requests until normal traffic cannot be processed.	Denial of Service
Board Computer	6	Without the required authorization, an adversary might obtain access to the board computer and carry out privileged operations.	Elevation of Privilege
NFC to BC	7	Board Computer may crash, halt, stop or run slowly because of the fake requests sent by the adversary.	Denial of Service
NFC to BC	8	An adversary may interrupt data flowing across NFC to board computer with a snipping device and send a massive volume of data over the communication channel.	Denial of Service
NFC to BC	9	Data flowing from NFC may be sniffed by an adversary and depending on the type of data, the attacker may attack other parts of the system.	Information Disclosure
NFC to BC	10	An adversary may tamper the dataflow from NFC to board computer in order to gain particular advantage.	Tampering
BC to WiFi	11	WiFi, Cellular Network may crash or halt due to the overflow of traffic.	Denial of Service
BC to WiFi	12	An adversary may interrupt data flowing across board computer to wifi, cellular network with a snipping device and send a massive volume of data over the communication channel.	Denial of Service
BC to WiFi	13	The data passing from board computer to wifi, cellular network may sniffed by the adversary.	Information Disclosure
BC to WiFi	14	An adversary may tamper the dataflow from board computer to wifi, cellular network and modify information to gain additional privilege.	Tampering
WiFi to BC	15	Board Computer may crash, halt, stop or run slowly due to the adversary make the resources and services unavailable.	Denial of Service
WiFi to BC	16	An adversary may interrupt data flowing across wifi, cellular network to board computer by sending a massive volume of data over the communication channel.	Denial of Service
WiFi to BC	17	The data passing from wifi, cellular network to board computer may sniffed by the adversary. This may lead to compliance violation.	Information Disclosure
WiFi to BC	18	An adversary may tamper the dataflow from wifi, cellular network to board computer and alter information.	Tampering

Components or interaction	Threat No	Threat	Threat category
BC to Bluetooth	19	Bluetooth may crash, halt, stop or run slowly due to the adversary make the resources and services unavailable.	Denial of Service
BC to Bluetooth	20	An external adversary may interrupt data flowing across a trust boundary by sending a large amount of data over communication channel.	Denial of Service
BC to Bluetooth	21	The data passing from board computer to bluetooth may sniffed by the adversary. Based on the type of information disclosure, this may lead to compliance violation.	Information Disclosure
BC to Bluetooth	22	An adversary may tamper the dataflow from board computer to bluetooth and alter information.	Tampering
Bluetooth to BC	23	Board Computer may crash, halt, stop or run slowly because of the fake requests sent by the adversary.	Denial of Service
Bluetooth to BC	24	An external adversary may interrupt data flowing and keep the system busy to respond to fake requests.	Denial of Service
Bluetooth to BC	25	The data passing from board computer to bluetooth may sniffed by the adversary. Based on the type of information disclosure, this may lead to attack other parts of the system.	Information Disclosure
Bluetooth to BC	26	An adversary may tamper the dataflow from bluetooth to board computer and make unauthorized manipulation to the system.	Tampering
BC to CN	27	CAN network may stop and deny to provide authorized service.	Denial of Service
BC to CN	28	An adversary may interrupt data flowing across board computer to CAN network in either direction.	Denial of Service
BC to CN	29	An adversary may tamper the dataflow from board computer to CAN network and alter information.	Information Disclosure
BC to CN	30	An adversary may tamper the dataflow from Bluetooth to board computer and lead to a denial of service or an elevation of privilege attack against CAN network and an information disclosure attack by CAN network.	Tampering
CN to BC	31	Board Computer may crash, halt, stop or run slowly due to the adversary make the resources and services unavailable.	Denial of Service
CN to BC	32	An adversary may interrupt data flowing across CAN network to board computer in either direction.	Denial of Service
CN to BC	33	The data passing from CAN network to board computer may sniffed by the adversary. Based on the type of information disclosure, this may lead to attack other parts of the system.	Information Disclosure
CN to BC	34	An adversary may tamper the dataflow from CAN network to board computer and alter information.	Tampering

5.4 Summary

In the chapter, different types of threat models have been discussed. PASTA focuses on the highest risks that can affect the system. DREAD calculates the average risks and indicates the overall severity of the risk. An attack tree is a methodical way of describing the security of systems, based on varying attacks. VAST is an automated threat modeling process applied to either application threats or operational threats. CVSS provides a way to capture a vulnerability's principal characteristics and assign a numerical score showing its severity. But besides all of those, we chose STRIDE because it is good for the component level and widely accepted by academia and industry level. We implemented DFD based on the component architecture of the infotainment HPC and also performed threat modeling using the Microsoft threat modeling tool, STRIDE. We listed thirty-four threats that may impersonate the infotainment HPC.

Chapter 6

Result and Discussion

6.1 Generalized Defense Mechanisms against STRIDE

This part presented the resulting threat information with various defense mechanisms against threat categories after taking processes, data flows, and threat modeling approaches into account. In order to identify cyber security threats, we applied the Microsoft STRIDE approach to DFD for the selected processes and data flows (without implementing any mitigating measures). As a result, in Table 5.3 six STRIDE categories have thirty-four threats. To prevent any system compromise, we shall now put in place various defenses. we can provide defence mechanism to the threats by following below methods:

Spoofing:

- Implement user authentication mechanisms, such as usernames and passwords, two-factor authentication, or biometric authentication.
- Use encryption to protect sensitive data, both in transit and at rest.
- Implement mechanisms to detect and prevent impersonation, such as digital certificates and IP address filtering.

Tampering:

- Implement digital signatures and checksums to verify the integrity of data and software.
- Use encryption to protect data in transit and at rest.
- Implement runtime code integrity checks to detect tampering attempts.

Repudiation:

- Implement audit trails and logging mechanisms to track user actions.
- Use digital signatures and timestamps to verify the authenticity of transactions.
- Implement secure and verifiable communication protocols, such as message signing and encryption.

Information Disclosure:

- Implement access controls and permissions to limit access to sensitive data.
- Use encryption to protect data in transit and at rest.
- Implement data masking techniques to prevent the disclosure of sensitive information.

Denial of Service:

- Implement rate limiting and traffic shaping mechanisms to prevent resource exhaustion attacks.
- Use load balancing to distribute traffic across multiple servers.
- Implement intrusion detection and prevention systems to detect and block malicious traffic.

Elevation of Privilege:

- Implement least privilege access controls to limit the permissions of users and applications.
- Use secure coding practices to prevent buffer overflows and other types of privilege escalation attacks.

- Implement user activity monitoring and logging to detect potential privilege escalation attempts.

In this section, we have provided generalized defense mechanisms against STRIDE threat categories presented in Table 6.1.

Table 6.1: Cyber Security Defense Mechanisms against STRIDE Category

STRIDE Category	Threat	Threat Details	Mitigation
Spoofing	Identity Spoofing	Adversary pretend to be a legitimate user or system	Multifactor authentication [32], Biometric authentication
Tampering	Data Tampering	Adversary modify data or software without authorization	Encryption [33], Digital signature
Repudiation	Non-Repudiation	Adversary deny responsibility for actions they have taken	Logging and auditing mechanisms to track and trace user actions [34]
Information Disclosure	Data Disclosure	Adversary gain access to sensitive information	Access controls and permissions to limit access to sensitive data [35]
Denial of Service	Resource Exhaustion	Adversary prevent legitimate users from accessing a system or service	Rate limiting and load balancing to distribute traffic across multiple servers [36]
Elevation of Privilege	Privilege Escalation	Adversary gain higher levels of access than they are authorized to have	Secure coding practices, User activity monitoring and logging to detect potential privilege escalation attempts [37]

By following this method, it will be possible to mitigate threats. Moreover, we suggest following NIST guidelines for standard cryptographic algorithms and key length used to secure data or communication in each threat category [38, 39]. These methods will be helpful for a developer to build possible mitigation and secure environment for the user.

6.2 Risk Assessment

Risk assessment is a critical process in cybersecurity that involves identifying, analyzing, and evaluating the potential threats and vulnerabilities in an organi-

zation's information systems. The primary goal of a risk assessment is to identify potential cybersecurity risks and prioritize them based on their potential impact and likelihood of occurrence [40].

In a risk assessment of threats in cybersecurity, organizations evaluate the risks associated with potential cyber attacks, malware, viruses, social engineering, phishing, insider threats, and other potential threats. This involves identifying the assets that need protection, evaluating their value to the organization, and analyzing the risks associated with them. Organizations also identify the potential threats that could target their information systems and evaluate the likelihood and impact of each threat. They analyze the vulnerabilities in their systems that could be exploited by identified threats and evaluate the risks associated with each threat [5].

There are several risk assessment models that organizations can use to assess the threats in cybersecurity. Here are some of the most commonly used models:

- NIST Cybersecurity Framework: This framework is a widely recognized risk management model developed by the National Institute of Standards and Technology (NIST). It provides a structured approach to managing cybersecurity risks, including identifying, protecting, detecting, responding to, and recovering from cyber incidents.

- ISO/IEC 27001: This is an international standard for information security management systems (ISMS) that provides a systematic approach to managing and protecting sensitive information. It involves conducting a risk assessment and implementing appropriate security controls to mitigate identified risks.

- FAIR (Factor Analysis of Information Risk): This model is a quantitative risk assessment framework that uses a probabilistic approach to assess cybersecurity risks. It involves evaluating the frequency and impact of potential cyber incidents and assigning values to each to determine the level

of risk.

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): This is a risk assessment model developed by Carnegie Mellon University. It is a holistic approach to cybersecurity risk management that focuses on identifying and prioritizing critical assets, evaluating the threats and vulnerabilities associated with them, and developing risk mitigation strategies.

- CRAMM (CCTA Risk Analysis and Management Method): This model is a comprehensive risk assessment methodology that involves identifying, analyzing, evaluating, and managing risks associated with an organization's information systems. It provides a structured approach to risk management and helps organizations prioritize their cybersecurity efforts.

Selecting the appropriate risk assessment model(s) depends on the organization's specific needs, goals, and resources. Combining multiple models may provide a more comprehensive understanding of an organization's cybersecurity risks and help prioritize its efforts accordingly. In the research, the risk assessment of threats is not performed. We will perform risk assessment using ISO/SAE 21434:2021 [41] standard for road vehicles in future.

Table 6.2: Sample Outcomes of Risk Treatment Decisions

Threat Scenario	Risk Value	Risk Treatment Option
Spoofing is a signal leads to loss of integrity of the data communication of "Lamp Request" signal for power switch actuator ECU	S: 5	Reducing the risk
Denial of service	O: 2	Reducing the risk

By performing risk assessment, it will be more effective to provide treatment for the threats. In future, based on listed threats we will perform risk assessment to the threats.

6.3 Outcome

In the research, we have implemented threat modeling on the infotainment HPC of an automotive vehicle. We have used the Microsoft threat modeling tool, STRIDE to perform threat modeling. By performing threat modeling, we got thirty-four threats that may lead the infotainment system to compromisation. these threats are the violation of Authenticity, Integrity, Non-repudiation, Confidentiality, Availability, and Authorization respectively. We also have kept some components out of scope. Based on the threats we have provided some defense mechanisms that can be used to protect the system from compromise. Before deploying an infotainment system in an automotive vehicle, it is necessary to investigate whether proper mitigations of these threats are present to avoid any potential harm to the user by the adversary. In future, we will perform risk assessment to the threats based on the listed threats.

Chapter 7

Conclusion and Future Work

Threats can occur to infotainment HPC, according to the strong interplay between security and safety considerations in the automotive area. Specific methods to identify anomalies in the automobile system and recovery from them are required to defend against cyber security and privacy assaults. The issues must be tackled before deploying the system in the real world. We contributed towards this issue in this work where we identified, categorized, and enumerated thirty-four cyber security threats of an infotainment HPC using the well threat modeling tool. Using the threat modeling program STRIDE, which is based on Microsoft, we first detect and categorize the threats. Then based on the category of the threats, we provided the required mitigation methods. This might improve the trade-off between security and safety issues in the automobile industry as well as the security of the infotainment HPC in cars.

In the future, based on the listed threat, we will lead this research to assist risks. So that we can provide most appropriate mitigation and treatment for the threats.

REFERENCES

[1] J. Choi and S.-i. Jin, "Security threats in connected car environment and proposal of in-vehicle infotainment-based access control mechanism," in *Advanced Multimedia and Ubiquitous Engineering: MUE/FutureTech 2018 12*. Springer, 2019, pp. 383–388.

[2] F. Luo, Y. Jiang, Z. Zhang, Y. Ren, and S. Hou, "Threat analysis and risk assessment for connected vehicles: A survey," *Security and Communication Networks*, vol. 2021, pp. 1–19, 2021.

[3] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[4] M. Nieles, K. Dempsey, V. Y. Pillitteri *et al.*, "An introduction to information security," *NIST special publication*, vol. 800, no. 12, p. 101, 2017.

[5] W. Xiong and R. Lagerström, "Threat modeling–a systematic literature review," *Computers & security*, vol. 84, pp. 53–69, 2019.

[6] D. Van Landuyt and W. Joosen, "A descriptive study of assumptions in stride security threat modeling," *Software and Systems Modeling*, pp. 1–18, 2021.

[7] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Stride-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, pp. 1–6.

[8] Y. Yang, Z. Duan, and M. Tehranipoor, "Identify a spoofing attack on an in-vehicle can bus based on the deep features of an ecu fingerprint signal," *Smart Cities*, vol. 3, no. 1, pp. 17–30, 2020.

[9] P. Haller, B. Genge, F. Forloni, G. Baldini, M. Carriero, and G. Fontaras, "Vetadetect: Vehicle tampering detection with closed-loop model ensemble," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100525, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548222000154

[10] A. M. Albalawi and M. A. Almaiah, "Assessing and reviewing of cybersecurity threats, attacks, mitigation techniques in iot environment," *J. Theor. Appl. Inf. Technol*, vol. 100, pp. 2988–3011, 2022.

[11] H. WATABE and H. YAMADA, "Efforts toward realization of connected car society," *Denso Ten technical review*, vol. 1, pp. 3–11, 2019.

[12] J. Takahashi, M. Iwamura, and M. Tanaka, "Security threat analysis of automotive infotainment systems," in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*. IEEE, 2020, pp. 1–7.

[13] G. Kornaros, O. Tomoutzoglou, D. Mbakoyiannis, N. Karadimitriou, M. Coppola, E. Montanari, I. Deligiannis, and G. Gherardi, "Towards holistic secure networking in connected vehicles through securing can-bus communication and firmware-over-the-air updating," *Journal of Systems Architecture*, vol. 109, p. 101761, 2020.

[14] C. Smith, *The car hacker's handbook: a guide for the penetration tester*. no starch press, 2018.

[15] A. Moiz and M. H. Alalfi, "An approach for the identification of information leakage in automotive infotainment systems," in *2020 IEEE 20th International Working Conference on Source Code Analysis and Manipulation (SCAM)*. IEEE, 2020, pp. 110–114.

[16] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE symposium on security and privacy*. IEEE, 2020, pp. 447–462.

[17] G. Costantino, A. La Marra, F. Martinelli, and I. Matteucci, "Candy: A social engineering attack to leak information from infotainment system," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. IEEE, 2018, pp. 1–5.

[18] M. R. Al Asif, K. F. Hasan, M. Z. Islam, and R. Khondoker, "Stride-based cyber security threat modeling for iot-enabled precision agriculture systems," in *2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)*. IEEE, 2021, pp. 1–6.

[19] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[20] G. Sen and B. Sener, "Design for luxury front-seat passenger infotainment systems with experience prototyping through vr," *International Journal of Human–Computer Interaction*, vol. 36, no. 18, pp. 1714–1733, 2020.

[21] M. Claassen, "Designing infotainment systems that are interactive not distractive," in *Automotive - Technical articles - TI E2E support forums*, 2019-06. [Online]. Available: https://e2e.ti.com/blogs_/b/behind_the_wheel/posts/designing-infotainment-systems-that-are-interactive-not-distractive

[22] F. Quintal and M. Lima, "Hapwheel: in-car infotainment system feedback using haptic and hovering techniques," *IEEE Transactions on Haptics*, vol. 15, no. 1, pp. 121–130, 2021.

[23] J. Alarcón, I. Balcázar, C. A. Collazos, H. Luna, and F. Moreira, "User interface design patterns for infotainment systems based on driver distraction: A colombian case study," *Sustainability*, vol. 14, no. 13, p. 8186, 2022.

[24] L. O. Nweke and S. Wolthusen, "A review of asset-centric threat modelling approaches," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 2, pp. 1–7, 2020.

[25] A. Wolf, D. Simopoulos, L. D'Avino, and P. Schwaiger, "The pasta threat model implementation in the iot development life cycle," *INFORMATIK 2020*, 2021.

[26] A. Omotosho, B. Ayemlo Haruna, and O. Mikail Olaniyi, "Threat modeling of internet of things health devices," *Journal of Applied Security Research*, vol. 14, no. 1, pp. 106–121, 2019.

[27] H. S. Lallie, K. Debattista, and J. Bal, "A review of attack graph and attack tree visual syntax in cyber security," *Computer Science Review*, vol. 35, p. 100219, 2020.

[28] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: a summary of available methods," Carnegie Mellon University Software Engineering Institute Pittsburgh United ..., Tech. Rep., 2018.

[29] S. Figueroa-Lorenzo, J. Añorga, and S. Arrizabalaga, "A survey of iiot protocols: A measure of vulnerability risk analysis based on cvss," *ACM Computing Surveys (CSUR)*, vol. 53, no. 2, pp. 1–53, 2020.

[30] M. Souppaya, K. Scarfone *et al.*, "Guide to enterprise telework, remote access, and bring your own device (byod) security," *NIST Special Publication*, vol. 800, p. 46, 2016.

[31] Q. Dang *et al.*, *Recommendation for applications using approved hash algorithms*. Citeseer, 2008.

[32] A. A. Ahmed and W. A. Ahmed, "An effective multifactor authentication mechanism based on combiners of hash function over internet of things," *Sensors*, vol. 19, no. 17, p. 3663, 2019.

[33] M. Al-Shabi, "A survey on symmetric and asymmetric cryptography algorithms in information security," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, no. 3, pp. 576–589, 2019.

[34] N. F. Syed, S. W. Shah, R. Trujillo-Rasua, and R. Doss, "Traceability in supply chains: A cyber security analysis," *Computers & Security*, vol. 112, p. 102536, 2022.

[35] M. A. Almaiah, A. Al-Zahrani, O. Almomani, and A. K. Alhwaitat, "Classification of cyber security threats on mobile devices and applications," in *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*. Springer, 2021, pp. 107–123.

[36] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in iot: a survey," *The Journal of Supercomputing*, vol. 76, pp. 5320–5363, 2020.

[37] E. A. AbuEmera, H. A. ElZouka, and A. A. Saad, "Security framework for identifying threats in smart manufacturing systems using stride approach," in *2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*. IEEE, 2022, pp. 605–612.

[38] W. Barker, W. Polk, and M. Souppaya, "Getting ready for post-quantum cryptography: explore challenges associated with adoption and use of post-quantum cryptographic algorithms," *The Publications of NIST Cyber Security White Paper (DRAFT), CSRC, NIST, GOV*, vol. 26, 2020.

[39] M. Fagan, J. Marron, K. G. Brady Jr, B. B. Cuthill, K. N. Megas, R. Herold, D. Lemire, and B. Hoehn, "Iot device cybersecurity guidance for the federal government," *NIST Special Publication*, vol. 800, p. 213, 2021.

[40] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Intelligent transportation system security: impact-oriented risk assessment of in-vehicle networks," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 2, pp. 91–104, 2019.

[41] I. S. . Electrical, electronic components, and general system aspects, "Iso/sae 21434:2021 road vehicles — cybersecurity engineering," in *43.040.15 Car informatics. On board computer systems*, 2021-08.