An Industrial Internship Report

submitted by

Preeti Yadav

21BEC0815.

in partial fulfillment for the award of the degree of

B.TECH

in

ELECTRONICS AND COMMUNICATIONS ENGINEERING

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

ACKNOWLEDGEMENT

I would like to extend my sincerest gratitude to my mentor Swapnil Rane, Senior Subject matter expert at KPIT Technologies and all my teammates who have generously supported and guided me throughout my internship.
My mentor's patience, and unwavering support have been instrumental in shaping my professional growth during this internship. His mentorship has not only provided me with valuable insights into the industry but has also inspired me to strive for excellence in all my endeavors.

I would also like to express my heartfelt appreciation to Rakesh Kokoula for his invaluable assistance and encouragement throughout this journey. Whether it was offering advice, sharing knowledge, or providing a helping hand, her support has been truly invaluable.

Furthermore, I extend my gratitude to the entire Renault CYS Team for creating a conducive learning environment and for their willingness to share their expertise and experiences.

I am deeply grateful for the opportunity to have worked alongside such dedicated and talented individuals. Their guidance and encouragement have played a significant role in my personal and professional development.

I would also like to thank Vellore Institute of Technology for giving me this wonderful opportunity to explore and providing me with a dynamic and enriching platform for learning and growth.

CERTIFICATE ISSUED BY THE COMPANY

KPIT

Date: January 25, 2024

Traineeship Certificate

This is to certify that **Preeti Yadav** has done her Traineeship with us from **02-Aug-23** to **02-Jan-24**.

During her tenure with us, we found her to be sincere and hardworking.

We wish her the very best in all future endeavor.

For KPIT Technologies Limited

RK singh

Rajesh Kumar Singh
Global Head - HR

KPIT Technologies Ltd. (Formerly KPIT Engineering Ltd.)
Registered & Corporate Office: Plot 17, Rajiv Gandhi Infotech Park, MIDC-SEZ, Phase-III, Maan, Taluka-Mulshi, Hinjawadi, Pune-411057, India.
CIN: U74999PN2018PLC174192

O +91 20 6770 6000
E info@kpit.com
W kpit.com

TABLE OF CONTENTS

INTRODUCTION

Exploring Automotive Cybersecurity at KPIT Technologies

During my internship at KPIT Technologies, I embarked on an illuminating journey into the realm of automotive cybersecurity. This experience not only expanded my knowledge but also deepened my interest in the interplay between technology and security within the automotive industry.

Throughout the internship, I had the privilege of immersing myself in various facets of automotive cybersecurity, gaining invaluable insights, and honing practical skills essential for safeguarding modern vehicles against evolving cyber threats.

Objective of the Internship

The objective of the internship is to gain comprehensive knowledge and practical experience in automotive cybersecurity. Through hands-on learning, mentorship, and collaborative projects, the internship aims to deepen understanding of cybersecurity fundamentals specific to automotive systems, explore the threat landscape facing modern vehicles, develop proficiency in security assessment tools and methodologies, and contribute to innovative solutions for mitigating cyber threats in the automotive industry. Additionally, the internship seeks to foster critical thinking, problem-solving skills, and industry-relevant expertise essential for pursuing a successful career in cybersecurity within the automotive sector.

Organizational Structure

KPIT Technologies' organizational structure includes the following members:

- Board of Directors

  Ravi Pandit, co-founder and chairman; Kishor Patil, co-founder, CEO, and managing director; Sachin Tikekar, president and joint managing director; Chinmay Pandit, whole-time director; Anup Sable, chief technology officer and board member; Anant Talaulicar, independent director and chairman of the nomination and remuneration committee, and CSR committee; B V R Subbu, independent director and chairman of

the stakeholders relationship committee; Prof. Alberto Vincentelli, independent director; Bhavna Doshi, independent director and chairperson of the audit committee; Prof. Rajiv Lal, independent director; and Srinath Batni, independent director

- Other members
  Gabriel Seiberth, president and geography head, Europe, and member of the executive board; Priya Hardikar, SVP, head corporate finance and governance; Pankaj Sathe, member of executive board and president, Europe; Rajesh Singh, global head and HR; Mohit Kochar, global head, marketing and communications; Rohan Sohoni, geo head, Asia; Tony Gu, country head, China; Rajesh Janwadkar, member of executive board and head passenger cars vertical; and Chinmay Pandit, member of executive board and head commercial vehicles vertical; and Pushpahas Joshi, member of executive board and head of new mobility vertical.

Various domains in which KPIT Technologies Operates

Automobile is now software on the wheels. Electronics in the form of ECUs, sensors and advanced chipsets work with millions of lines of code and play a differentiating role in the automotive industry.

A partner for software defined vehicles, KPIT enables newer business models and disrupt technology across CASE (Connected, Autonomous, Shared, Electric) domains. However, as the role of software and data grows, so does its complexity, thus making it necessary for the automotive industry to build deep software competence.

EXPERTISE AND GLOBAL SCALE TO HELP YOU REIMAGINE MOBILITY IN THESE AREAS TO

1) Decoupling components for modularity; move towards centralized architecture; faster time to market; high performance computing
2) Increasing complexity; software from multiple parties; multicore optimization; performance engineering; AUTOSAR, FuSa, Cybersecurity compliance
3) Access to right set of competencies across the globe from within/outside mobility; upskilling and cross-skilling. Solve the problem in new areas
4) Only embedded software company with deep domain expertise across CASE (Connected, Autonomous, Shared, Electrified) domains.

KPIT Technologies is a global partner to the automotive and Mobility ecosystem for making software-defined vehicles a reality. It is a leading independent software development and integration partner helping mobility leapfrog towards a clean, smart, and safe future. With 12000+ automobelievers across the globe specializing in embedded software, AI, and digital solutions, KPIT accelerates its clients' implementation of next-generation

technologies for the future mobility roadmap. With engineering centers in Europe, the USA, Japan, China, Thailand, and India, KPIT works with leaders in automotive and Mobility and is present where the ecosystem is transforming.

KPIT Technologies operates across various domains, offering a wide range of technology solutions and services to its clients. While the company's focus areas may evolve over time, here are some of the key domains in which KPIT Technologies has been active:

1. Automotive:KPIT Technologies has a strong presence in the automotive sector, providing software solutions, engineering services, and consulting for automotive OEMs (Original Equipment Manufacturers) and suppliers. This includes areas such as connected vehicles, autonomous driving, electrification, vehicle diagnostics, and infotainment systems.

2. Mobility Solutions: The company offers mobility solutions aimed at transforming transportation and urban mobility. This includes solutions for electric vehicles (EVs), smart transportation systems, ride-sharing platforms, and mobility-as-a-service (MaaS) offerings.

3. Manufacturing and Industrial IoT (IIoT): KPIT Technologies provides digital transformation solutions for manufacturing industries, leveraging Industrial IoT (IIoT), Industry 4.0 principles, and advanced analytics to optimize operations, enhance productivity, and enable smart manufacturing.

4. Utilities and Smart Cities: KPIT Technologies provides technology solutions and services to utilities and municipalities for building smart cities and sustainable infrastructure. This includes solutions for smart metering, energy efficiency, water management, and public safety.

5. Telecommunications: KPIT Technologies offers software solutions and engineering services to telecommunications companies. This includes solutions for network management, OSS/BSS (Operations Support Systems/Business Support Systems), and next-generation telecommunications technologies.

These are just some of the domains in which KPIT Technologies operates, demonstrating the company's diverse portfolio and expertise in delivering technology solutions across various industries.

DOMAIN OF INTERNSHIP : AUTOMOTIVE CYBERSECURITY

Under the mentorship of industry experts, I delved into the following key areas:

1.Understanding Automotive Cybersecurity Fundamentals:

I began by developing a foundational understanding of automotive cybersecurity principles, exploring the unique challenges posed by connected and autonomous vehicles. Through comprehensive training sessions and hands-on exercises, I familiarized myself with the fundamentals of threat modeling, risk assessment, and security architecture design specific to automotive systems.

2. Exploring Threat Landscape and Vulnerabilities:

With a focus on practical application, I conducted in-depth analyses of the threat landscape facing automotive ecosystems. By studying real-world attack scenarios and dissecting vulnerabilities in automotive software and hardware components, I gained valuable insights into potential cyber threats and their implications for vehicle safety and functionality.

3. Hands-on Experience with Security Assessment Tools:

Leveraging security assessment tools and methodologies, I gained practical experience in conducting penetration testing, Denial of Service testing, Fuzz testing , and code analysis for automotive systems. This hands-on experience not only sharpened my technical skills but also equipped me with the proficiency to identify and mitigate security vulnerabilities effectively.

4. Collaborative Projects and Industry Engagement:

Throughout the internship, I had the opportunity to collaborate with cross-functional teams on industry-relevant projects aimed at addressing cybersecurity challenges in automotive environments. Additionally, engaging with industry experts and participating in workshops and seminars provided invaluable exposure to emerging trends, best practices, and real-world applications of automotive cybersecurity technologies.

Recent Ongoing Work Methodology and Challenges in Automotive Cybersecurity.

As vehicles become more connected and autonomous, the automotive industry is facing increasing cybersecurity challenges. The rise of connected cars has opened up new avenues for cyberattacks, raising concerns about the safety and security of vehicles. In this blog post, we'll explore the top seven trends driving innovation and growth in the **Automotive Cybersecurity Market**.

1. Rise of Connected and Autonomous Vehicles

Connected vehicles, equipped with internet connectivity and advanced sensors, are becoming increasingly popular. These vehicles offer a range of benefits, such as improved safety, efficiency, and convenience. However, they also present new cybersecurity challenges, as hackers can potentially exploit vulnerabilities in the vehicle's software and systems. As the adoption of connected and autonomous vehicles continues to grow, the demand for automotive cybersecurity solutions is expected to rise.

2. Increasing Regulatory Focus

Regulators around the world are paying increasing attention to automotive cybersecurity. In the United States, the National Highway Traffic Safety Administration (NHTSA) has issued guidelines for automotive cybersecurity, while the European Union has introduced the General Data Protection Regulation (GDPR) to protect consumer data. These regulations are driving automakers to prioritize cybersecurity in their vehicles and systems, leading to increased demand for cybersecurity solutions.

3. Growing Threat of Cyberattacks

The automotive industry is increasingly being targeted by cybercriminals looking to exploit vulnerabilities in connected vehicles. These attacks can range from theft of personal data to remote control of vehicle systems. As the threat landscape evolves, automakers are investing in cybersecurity solutions to protect their vehicles and customers from cyberattacks.

4. Adoption of Security-by-Design Principles

Security-by-design principles are gaining traction in the automotive industry, with automakers incorporating cybersecurity features into their vehicles and systems from the

design stage. By implementing security-by-design principles, automakers can identify and mitigate potential vulnerabilities early in the development process, reducing the risk of cyberattacks.

5. Emphasis on Secure Software Updates

Software updates are essential for keeping connected vehicles secure and up to date. However, ensuring the security of these updates can be challenging, as they can potentially introduce new vulnerabilities. Automakers are focusing on implementing secure software update mechanisms, such as over-the-air (OTA) updates, to protect vehicles from cyberattacks while keeping them updated with the latest features and security patches.

6. Adoption of Intrusion Detection Systems

Intrusion detection systems (IDS) are becoming an essential component of automotive cybersecurity. These systems monitor vehicle networks for suspicious activity and alert users or automakers of potential cyberattacks. By adopting IDS, automakers can detect and respond to cyber threats in real-time, enhancing the overall cybersecurity posture of their vehicles.

Conclusion

The automotive cybersecurity market is evolving rapidly, driven by trends such as the rise of connected and autonomous vehicles, increasing regulatory focus, growing threat of cyberattacks, adoption of security-by-design principles, collaboration and partnerships, emphasis on secure software updates, and adoption of intrusion detection systems. As automakers continue to innovate and introduce new technologies, cybersecurity will remain a top priority to ensure the safety and security of connected vehicles.

PEOPLE INTERACTED WITH AND MACHINERY/EQUIPMENT OBSERVED AND LEARNING.

During my Internship at KPIT I was working under the Mentorship of Swapnil Rane who himself is an alumni of Vellore Institute of Technology. He is the Senior Subject matter Expert in Renault CYS team at KPIT Technologies.

In the beginning of my internship I was told to first read and get more knowledge about the basic systems and parts of a vehicle and how cybersecurity is necessary in a BMS (Battery management system) and for an ECU (electronic control unit).
The first month included training sessions on AUTOSAR and BMS.

Later on Swapnil Rane alloted Rakesh Kokoula who is a senior developer at Renault CYS Team and KPIT to give me a brief knowledge about CSM, Cry-IF, and Crypto modules using C4K tool.

In this session I also learned about various types of attacks made on the ECU like Penetration Testing, Fuzz Testing, and Denial of Service Testing. The highlight about this session was I got to learn more about the C4K Tool which is an inbuilt KPIT Tool which is used to create safety keys and license certificates which is used in vehicles whenever a software update or any kind of changes are required to be made into the system, without these license certificates the system cannot be hacked by any outside attacks.

I was later introduced to VBA programing which is an Excel based programing language that makes woking in excel more easy and effective.

DETAILED DESCRIPTION OF INTERNSHIP WORK.

Training Overview

Automotive Software Development and Cybersecurity.

The training program provided a comprehensive exploration into automotive software development methodologies and cybersecurity practices essential for ensuring the safety, security, and reliability of modern vehicles. Participants were immersed in a series of interactive sessions, workshops, and hands-on exercises designed to deepen understanding and foster practical skills across key domains. Below is an overview of the topics covered during the training:

1. AUTOSAR (AUTomotive Open System ARchitecture):
Participants were introduced to the AUTOSAR standard, a globally recognized framework for automotive software architecture. The training delved into the basic principles of AUTOSAR, including its layered software architecture and standardized interfaces for seamless integration of software components across different automotive domains.

2. Basic Software Architecture (BSW):
A detailed examination of the Basic Software (BSW) layer within the AUTOSAR architecture was conducted, focusing on its role in providing essential services and functions for automotive applications. Participants gained insights into BSW modules, services, and their interactions within the software stack.

3. AUTOSAR Runtime Environment (RTE Layer):
The training provided an in-depth understanding of the AUTOSAR Runtime Environment (RTE) layer, which facilitates communication and interaction between software components in an AUTOSAR-compliant system. Participants learned about RTE configuration, communication mechanisms, and runtime behavior.

4. Fuzz Testing for Automotive Software:
A practical session on fuzz testing techniques for automotive software was conducted, emphasizing the importance of identifying and mitigating vulnerabilities through systematic testing methodologies. Participants gained hands-on experience in designing and executing fuzz tests to uncover potential security flaws and software bugs.

5. Denial of Service Test (DOS):
An exploration into denial-of-service (DoS) testing methodologies and strategies was undertaken, focusing on simulating and mitigating DoS attacks targeting automotive systems. Participants learned how to assess system resilience to DoS attacks and

implement countermeasures to enhance system robustness.

6. Penetration Testing:
The training included a comprehensive overview of penetration testing techniques tailored for automotive software environments. Participants gained practical skills in identifying security weaknesses, exploiting vulnerabilities, and recommending remediation measures to strengthen system defenses.

7. Secure Software Updates:
An examination of secure software update mechanisms for automotive systems was conducted, highlighting the importance of ensuring integrity, authenticity, and confidentiality throughout the update process. Participants learned about secure update protocols, cryptographic mechanisms, and best practices for maintaining software integrity.

8. Secure Debug and Diagnostics:
Participants were introduced to secure debug and diagnostics techniques for automotive systems, focusing on safeguarding sensitive information and preventing unauthorized access during debugging and diagnostic procedures. The training covered secure communication protocols, access control mechanisms, and encryption techniques.

9. Secure Communication:
A deep dive into secure communication protocols and mechanisms for automotive networks was conducted, emphasizing the need for confidentiality, integrity, and authenticity in data transmission. Participants learned about secure communication protocols such as TLS/SSL, IPSec, and CAN bus encryption, and their application in automotive environments.

10. Secure Boot:
The training concluded with an exploration of secure boot mechanisms for automotive ECUs (Electronic Control Units), highlighting their role in ensuring the integrity and authenticity of boot processes. Participants gained insights into secure boot architectures, cryptographic techniques, and secure boot sequence implementation.

Overall, the training program equipped participants with a comprehensive understanding of automotive software development principles and cybersecurity practices, empowering them to contribute effectively to the design, development, and deployment of secure and reliable automotive systems.

TASK-1

After my Training was completed and I gained some knowledge about system vulnerabilities such as the Child Attacks and Parent Attacks I was assigned with my first task which was to make a python script that read all the company Data that was generated about the various attacks conducted on a system, which will read this data and form a visual representation of these attacks made on the system by which the team working on to resolve these issues gets a clear and detailed representation of the various attacks made on a system.

Along with my team member Rohit Pandit I worked on making the script, which also included a lot of trial and error to get the right output. Once we got a functional code with tried it on the working model.

Code:

```
import openpyxl
import networkx as nx
import matplotlib.pyplot as plt
import textwrap

def create_graphs(excel_file):
    wb = openpyxl.load_workbook(excel_file)
    sheet = wb.active

    graphs = []
    current_graph = nx.DiGraph()
    current_tree = None

    for row in sheet.iter_rows(min_row=2):
        tree_id, parent, parent_desc, child, child_desc = [cell.value for cell in row]

        if tree_id and current_tree != tree_id:
            if current_tree is not None:
                graphs.append((current_tree, current_graph))
            current_graph = nx.DiGraph()
            current_tree = tree_id

        current_graph.add_node(parent, description=parent_desc)
        current_graph.add_node(child, description=child_desc)
        current_graph.add_edge(parent, child)

    if current_tree is not None:
        graphs.append((current_tree, current_graph))
```

```
    return graphs

def tree_layout(graph, root, width=0.5, vert_gap=0.2, vert_loc=0, xcenter=0.5):
    pos = {root: (xcenter, vert_loc)}

    if graph.out_degree(root) != 0:
        dx = width / 2
        nextx = xcenter - (dx * (graph.out_degree(root) - 1)) / 2

        for child in graph.neighbors(root):
            pos.update(tree_layout(graph, child, width=dx, vert_gap=vert_gap,
vert_loc=vert_loc-vert_gap, xcenter=nextx))
            nextx += dx

    return pos

def visualize_graphs(graphs):
    rows = (len(graphs) + 1) // 2
    cols = 2  # Display 2 trees per page

    for tree_number, ((tree_id, graph), page_start) in enumerate(zip(graphs, range(0,
len(graphs), cols)), start=1):
        page_graphs = graphs[page_start:page_start + cols]
        num_graphs = len(page_graphs)
        rows = 1

        fig, axs = plt.subplots(rows, num_graphs, figsize=(15, 6))

        if num_graphs == 1:
            axs = [axs]  # To handle a single subplot case

        for i, (ax, (tree_id, graph)) in enumerate(zip(axs, page_graphs)):
            root_nodes = [n for n, d in graph.in_degree() if d == 0]
            for root_node in root_nodes:
                pos = tree_layout(graph, root_node, xcenter=0.5)  # Center each root node
                last_parent = None

                node_labels = {}
                labels = {}
                for node, desc in graph.nodes(data='description'):
                    x, y = pos[node]
                    desc_wrapped = '\n'.join(textwrap.wrap(desc, width=20))
                    num_lines = len(desc_wrapped.split('\n'))
                    box_height = 0.015 * num_lines
```

```
                desc_x = x - (box_height / 2)  # Adjust this value to move descriptions
further to the side

                if graph.out_degree(node) == 0:
                    ax.text(x, y - 0.04 - 0.6 * box_height, desc_wrapped, fontsize=8,
ha='center', va='center', zorder=1)
                else:
                    ax.text(desc_x, y, desc_wrapped, fontsize=8, ha='left', va='center',
zorder=1)

                ax.add_patch(plt.Rectangle((desc_x, y - 0.04 - 0.6 * box_height), 0.16,
box_height, color='white', edgecolor='gray', linewidth=1, zorder=0))

                if last_parent and node != last_parent:
                    node_labels[last_parent] = "\n".join(labels.values())
                    labels = {}
                labels[node] = node  # Store node name in labels
                last_parent = node

            if labels:
                node_labels[last_parent] = "\n".join(labels.values())

            nx.draw(graph, pos, with_labels=False, node_size=1500,
node_color='lightblue', font_size=10, font_color='black', ax=ax)
            nx.draw_networkx_labels(graph, pos, labels=node_labels, font_size=8,
verticalalignment='center', ax=ax)

        ax.set_title(f"Tree {tree_id}")
        ax.axis('off')

    plt.tight_layout()
    plt.show()

if __name__ == '__main__':
    excel_file = 'excelsheet.xlsx'  # Provide the correct path to your Excel sheet
    graphs = create_graphs(excel_file)

    visualize_graphs(graphs)
```

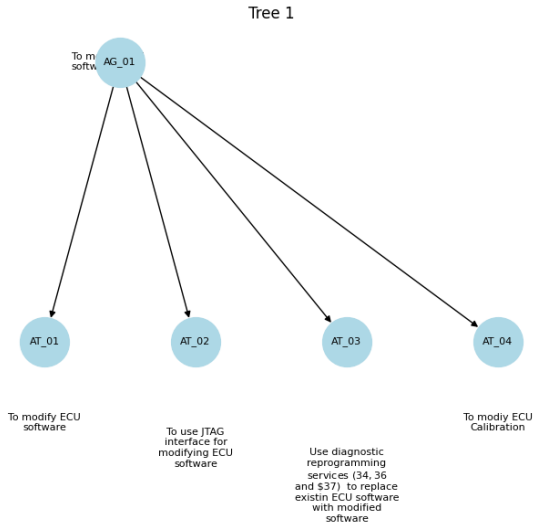
System vulnerabilities Data through Excel:

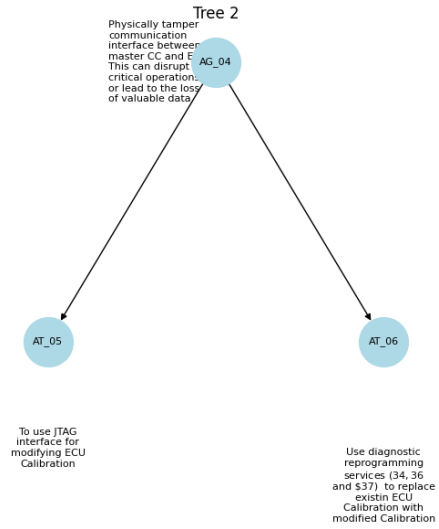
D	E	F	G	H	I	J	K	L	M	
CAPEC ID	**Threat Mechnaism**	**Attack ID**	**Attack Description**	**Parent Attack ID / Higher level Attack Goal**	**Parent Relation**	**Tree Level**	**Leaf level?**	**Attack vector**	**Attack complexity**	**Pr r**
184	Software integrity attack	AT_01	To modify ECU software	AG_01 AG_05 AG_08 AG_12 AG_15 AG_20 AG_23 AG_26 AG_29 AG_32 AG_35 AG_37	OR	2	No	Local	Low	N
		AT_02	To use JTAG interface for modifying ECU software	AT_01	OR	3	Yes	Local	Low	N
		AT_03	Use diagnostic reprogramming services ($34, $36 and $37) to replace existin ECU software with modified software	AT_01	OR	3	Yes	Local	Low	N
184	Software integrity attack	AT_04	To modiy ECU Calibration	AG_01 AG_05 AG_08 AG_12 AG_15 AG_20 AG_23 AG_26 AG_29 AG_32 AG_35 AG_37 AG_49	OR	2	No	Local	Low	N

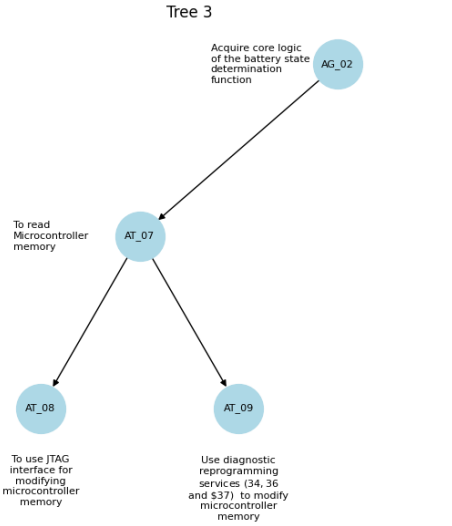
Attack Goal ID	Asset ID	Asset title	Property	Attack Description	CVSS	Attack Feasibility Rating
AG_01	AS_01	Battery State Estimation	Integrity	Manipulate member assets or associated assets of Battery State Determination	2.515145325	#REF!
AG_02			Confidentiality	Acquire core logic of the battery state determination function	1.4372259	#REF!
AG_03			Availability	Denial of service attack to make Battery State Determination unavailable	1.4372259	#REF!
AG_04				Physically tamper communication interface between master CC and ECU This can disrupt critical operations or lead to the loss of valuable data.	1.4372259	#REF!
AG_05	AS_02	Battery Monitoring	Integrity	Manipulate member assets or associated assets of monitor and transmit battery parameters function	2.515145325	#REF!
AG_06			Confidentiality	Acquire core logic of the battery monitoring function	1.4372259	#REF!
AG_07			Availability	Denial of service attack to make monitor and transmit battery parameters function unavailable	1.4372259	#REF!
AG_08	AS_03	Battery Data Management	Integrity	Manipulate member assets or associated assets of battery data storing and transmit function	2.515145325	#REF!
AG_09			Confidentiality	Acquire core logic of the battery data management function	1.4372259	#REF!
AG_10			Availability	Denial of service attack to make Battery State Determination unavailable	1.4372259	#REF!
AG_11				Attacker can physcially tamper communication interface between master CC and ECU This can disrupt critical operations or lead to the loss of valuable data.	1.4372259	#REF!
AG_12	AS_04	Cell Balancing	Integrity	Manipulate member assets or associated assets of cell balancing function	2.515145325	#REF!
AG_13			Confidentiality	Acquire core logic of the battery cell balancing function	1.4372259	#REF!
AG_14			Availability	Denial of service attack to make cell balancing function unavailable	1.4372259	#REF!
AG_15	AS_05	Battery Thermal Management	Integrity	Manipulate member assets or associated assets of Battery thermal management function	2.515145325	#REF!
AG_16			Confidentiality	Acquire core logic of the battery thermal management function	1.4372259	#REF!
AG_17			Availability	Denial of service attack to make Battery thermal management function unavailable	1.4372259	#REF!
AG_18				Attacker can physcially tamper communication interface between master CC and ECU This can disrupt critical operations or lead to the loss of valuable data.	1.4372259	#REF!
AG_19				Attackers may try to manipulate or spoof the data collected by sensors. By tampering with the sensor readings, they can provide inaccurate or false information, leading to erroneous decisions or actions based on that data.	1.4372259	#REF!
AG_20	AS_06	Battery Charge Management	Integrity	Manipulate member assets or associated assets of Battery Charge management	2.515145325	#REF!
AG_21			Confidentiality	Acquire core logic of the battery charge management function	1.4372259	#REF!
AG_22			Availability	Denial of service attack to make Battery Charge management function unavailable	1.4372259	#REF!
AG_23			Integrity	Manipulate member assets or associated assets of power relay management function	2.515145325	#REF!

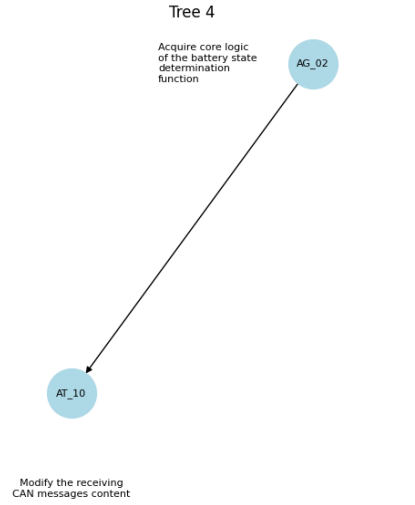
Primary Assets | Impact Analysis | Attack Tree | Primary Asset Attack Goals | Associate and Member Asset Goal

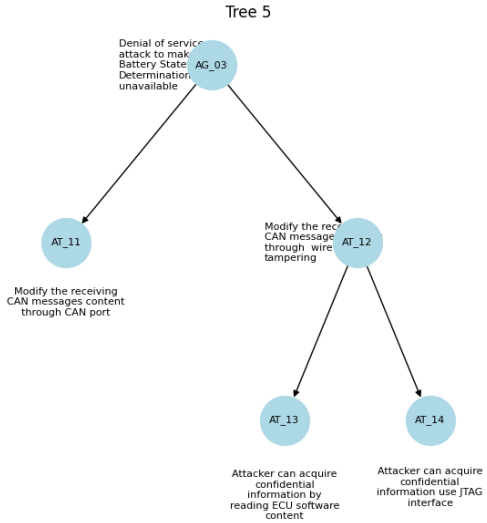
Output:

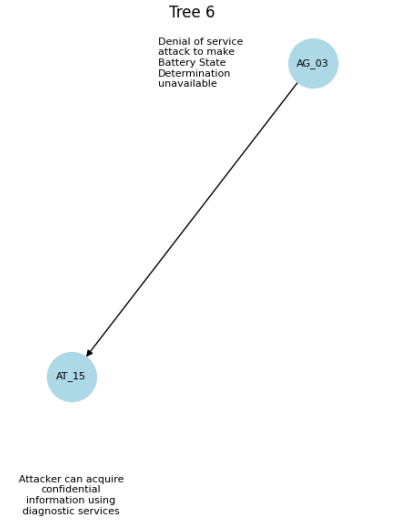

Tree 1
AG_01
AT_01
AT_02
AT_03
AT_04
To modify ECU software
To use JTAG interface for modifying ECU software
Use diagnostic reprogramming services (34, 36 and $37) to replace existin ECU software with modified software
To modiy ECU Calibration


Tree 2
AG_04
AT_05
AT_06
To use JTAG interface for modifying ECU Calibration
Use diagnostic reprogramming services (34, 36 and $37) to replace existin ECU Calibration with modified Calibration

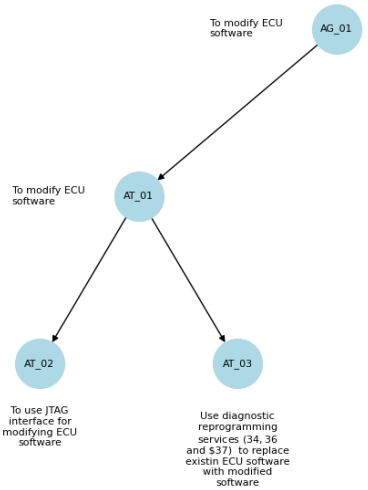

Tree 3
Acquire core logic of the battery state determination function
AG_02
To read Microcontroller memory
AT_07
AT_08
AT_09
To use JTAG interface for modifying microcontroller memory
Use diagnostic reprogramming services (34, 36 and $37) to modify microcontroller memory


Tree 4
Acquire core logic of the battery state determination function
AG_02
AT_10
Modify the receiving CAN messages content

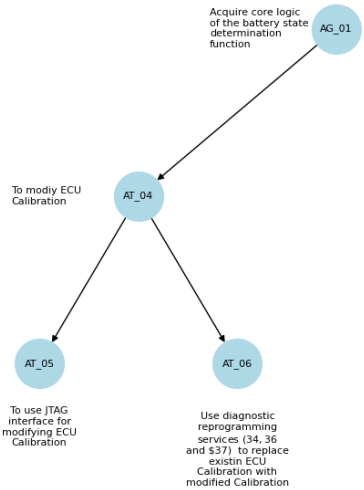

Tree 5
Denial of service attack to make Battery State Determination unavailable
AG_03
AT_11
AT_12
Modify the receiving CAN messages content through CAN port
AT_13
AT_14
Attacker can acquire confidential information by reading ECU software content
Attacker can acquire confidential information use JTAG interface


Tree 6
Denial of service attack to make Battery State Determination unavailable
AG_03
AT_15
Attacker can acquire confidential information using diagnostic services

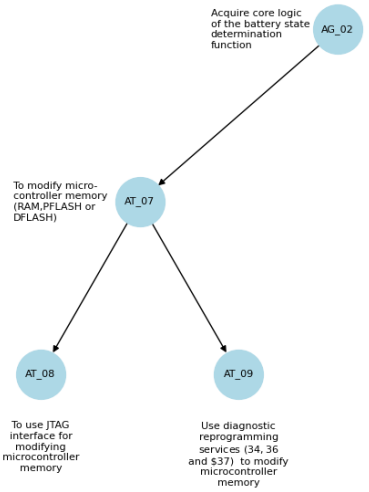
Tree 7



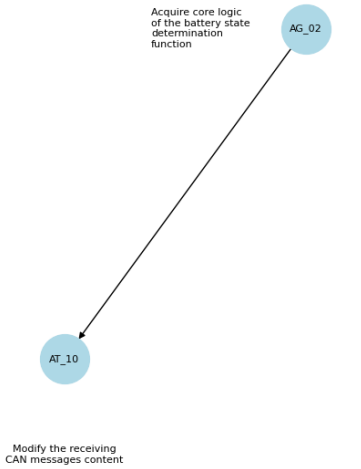
Tree 8



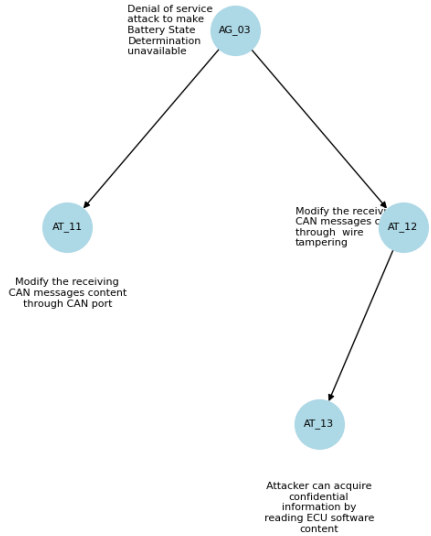
Tree 9



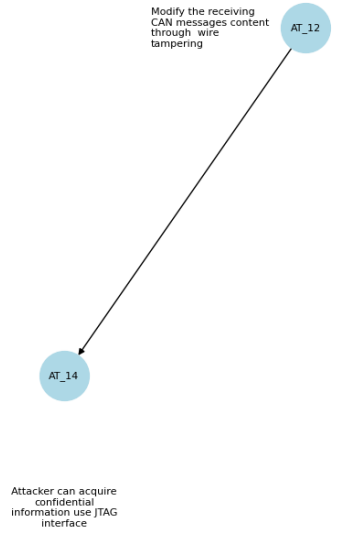
Tree 10



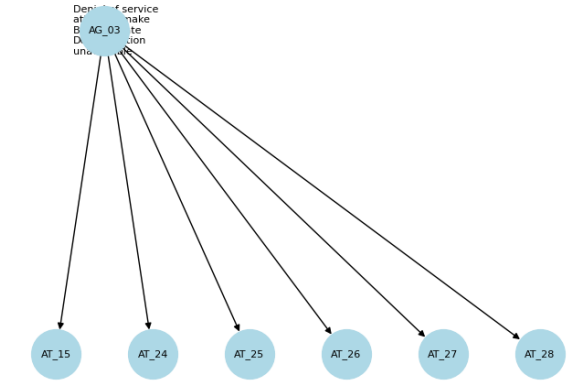
Tree 11



Tree 12



Tree 13



Attacker can acquire confidential information using diagnostic services

Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

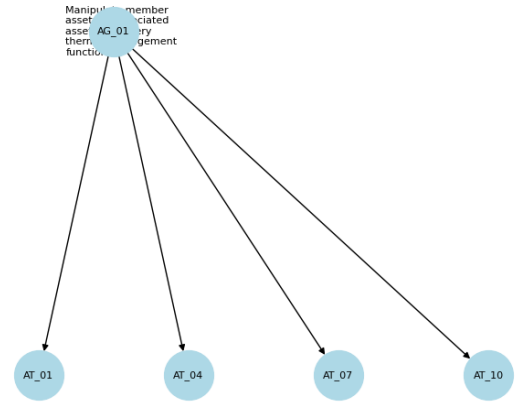
Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

Tree 14



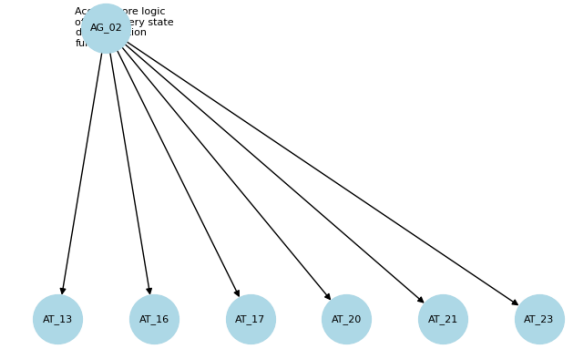
To modify ECU software

To modiy ECU Calibration

To modify micro-controller memory (RAM,PFLASH or DFLASH)

Modify the receiving CAN messages content

Tree 15



Attacker can acquire confidential information by reading ECU software content

Attacker can acquire confidential information by monitoring CAN communication messages

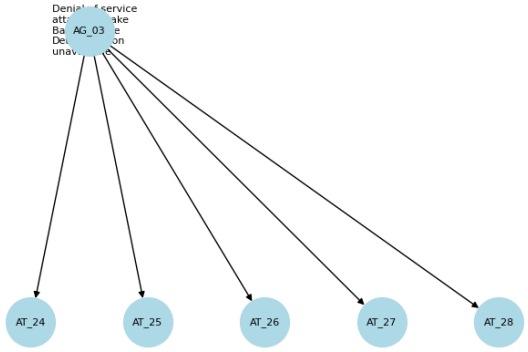
Attacker can acquire confidential information by reading ECU Calibration content

Attacker can acquire confidential information by monitoring CAN communication messages

Attacker can acquire confidential information by reading micro-controller memory

Attacker can acquire confidential information using diagnostic commands

Tree 16



Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

Attacker can send multiple requests to the ECU in small period of time which may lead the ECU to inresponsive state

TASK-2

Task two was about converting the Company data about the RAM and ROM data values of the ECUs that is received in a .map file to convert this data from the .map file to an Excel sheet in a systematic order having only the required information so that the Data can be viewed easily by the team member hence reducing the time and effort of collecting such huge data and manually copy pasting the data into an excel sheet.

Code:

```
import openpyxl
import re

def read_map_file(file_path):
    try:
        with open(file_path, 'r') as file:
            data = file.readlines()  # Read the lines
        return data
    except FileNotFoundError:
        print(f"Error opening file: {file_path}")
        return []

def update_excel(map_data, file_name, excel_path):
    # Create a regex pattern to match the file name in a case-insensitive manner
    pattern = re.compile(re.escape(file_name), re.IGNORECASE)

    # Initialize ROM and RAM values as strings
    rom_value = '0'
    ram_value = '0'

    # Flag to track if ".CODE" is found in the first line
    code_found = False

    # Iterate over each line in the map data
    for line in map_data:
        if re.search(pattern, line):
            if ".CODE" in line:
                # Extract 14th and 15th characters from the line and update ROM value
                rom_value = line[13:15].strip()
                code_found = True
            elif code_found and ".RAM" in line:
                # Extract 14th and 15th characters from the line and update RAM value
                ram_value = line[13:15].strip()
```

```
                break  # Stop searching after finding .RAM

    # Update the Excel sheet
    workbook = openpyxl.load_workbook(excel_path)
    sheet = workbook.active

    for row in sheet.iter_rows(min_row=2, max_row=sheet.max_row):
        if row[0].value and row[0].value.strip().lower() == file_name.strip().lower():
            # Update ROM and RAM columns with string values
            row[1].value = rom_value
            row[2].value = ram_value

    workbook.save(excel_path)

def main(map_file_path, excel_file_path):
    map_data = read_map_file(map_file_path)

    if not map_data:
        print("Error reading map file. Exiting.")
        return

    try:
        # Replace "file1" and "file2" with the actual file names in your Excel sheet
        update_excel(map_data, "file1", excel_file_path)
        update_excel(map_data, "file2", excel_file_path)
        # Add more calls to update_excel for each file in your Excel sheet

        print("Data updated successfully.")
    except Exception as e:
        print(f"An error occurred: {e}")

if __name__ == "__main__":
    map_file_path = 'path/to/your/map/file.map'
    excel_file_path = 'path/to/your/excel/sheet.xlsx'
    main(map_file_path, excel_file_path)
```

OVERALL SOFTWARE AND HARDWARE LEARNED:

Python Programming

VBA programing

KPIT C4K Tool

MIL,SIL,HIL

Cybersecurity Breakbox Functioning

ECU Electronic Control Unit

BMS battery management system of a vehicle

SUMMARY OF INTERNSHIP

During the internship focused on automotive cybersecurity at KPIT TECHNOLOGIES, I embarked on an enriching journey that deepened my understanding of the critical intersection between automotive technology and cybersecurity. Throughout this immersive experience, I gained invaluable insights and practical skills across various subject matters, contributing to a holistic understanding of automotive cybersecurity. Below is a summary of the key highlights and learnings from the internship:

1. Understanding of Battery Management System (BMS):
I acquired a comprehensive understanding of the Battery Management System (BMS) and its components, gaining insights into the role of BMS in managing and monitoring battery performance, health, and safety within electric vehicles.

2. Proficiency in Autosar CSM, Cry-IF, and Crypto Modules:
Through dedicated training sessions, I developed proficiency in Autosar Complex Device Driver (CDD) Security Module (CSM), Crytographic Interface (Cry-IF), and Crypto modules, essential components for ensuring the security and integrity of automotive systems. This knowledge enabled me to understand the implementation of cryptographic algorithms and secure communication protocols in automotive environments.

3. Identification of Attack Scenarios on BMS:
As part of hands-on exercises and cybersecurity assessments, I identified various attack scenarios targeting the Battery Management System (BMS). Leveraging penetration testing, fuzz testing, and denial-of-service testing techniques, I conducted comprehensive assessments to uncover vulnerabilities and assess the resilience of

BMS against cyber threats.

4. Case Study Report Preparation:
Drawing upon my findings from the cybersecurity assessments, I meticulously documented the identified attack scenarios, methodologies, and recommendations in a detailed case study report. This report served as a valuable resource for understanding the security implications and mitigation strategies for securing BMS in automotive systems.

5. Development of Attack Tree Representation Script:
Utilizing my programming skills, I developed a script to represent attack trees in graphical format, providing a systematic visualization of potential attack paths and their dependencies. This tool proved instrumental in analyzing and communicating complex cybersecurity scenarios effectively.

6. Overview Session by Renault CYS Team:
A highlight of the internship was the insightful overview session conducted by the Renault Cybersecurity (CYS) team, focusing on the configuration of CSM and Cry-IF modules in the C4K tool. This session provided practical insights and real-world applications of cybersecurity concepts in automotive systems, enriching my understanding of industry best practices and tools.

In conclusion, the internship provided a rich learning experience that equipped me with practical skills, theoretical knowledge, and a deeper appreciation for the importance of cybersecurity in the automotive industry. Armed with this expertise, I am confident in my ability to contribute to the development and implementation of secure automotive systems, ensuring the safety, security, and reliability of vehicles in the digital age.