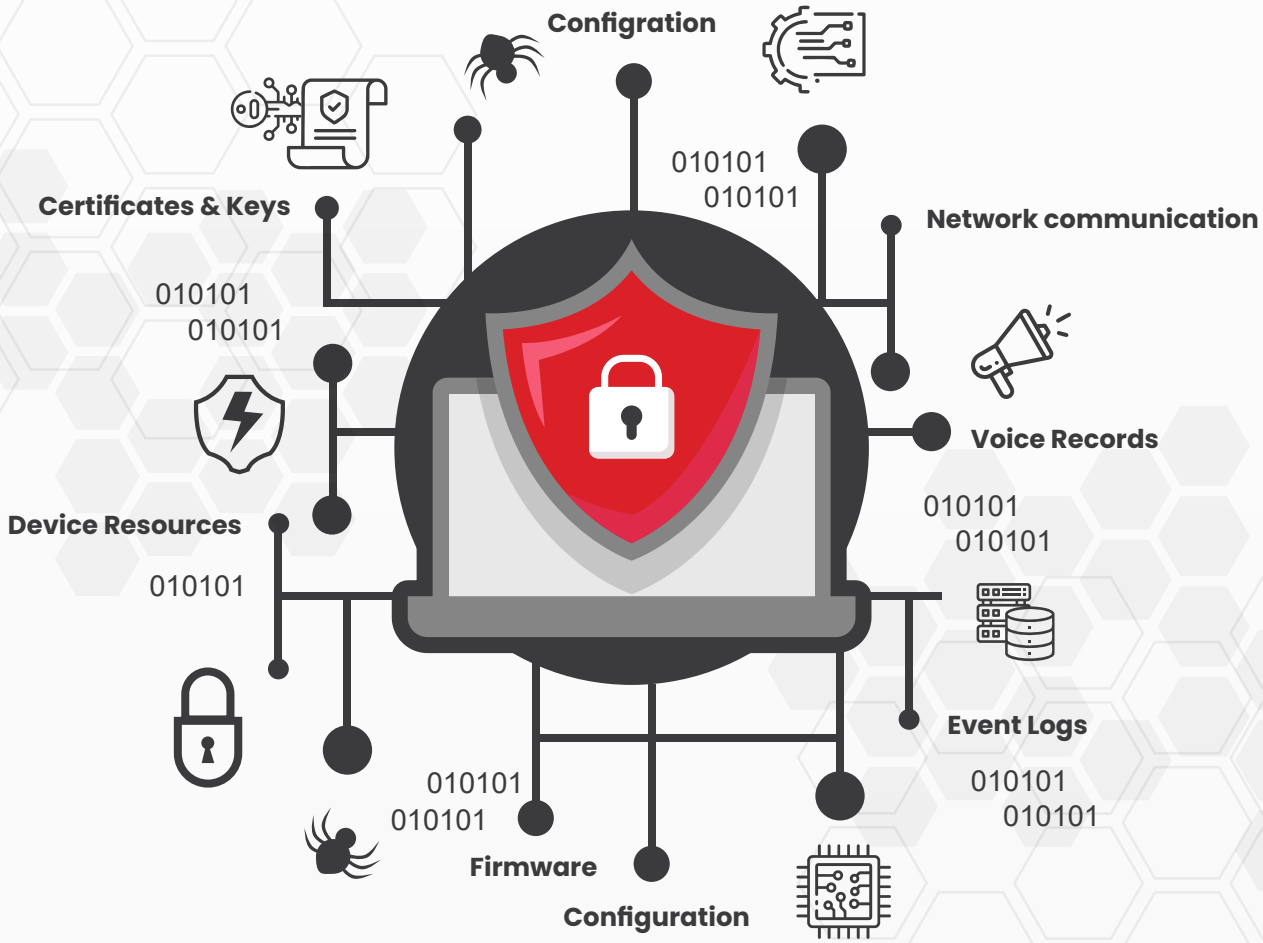
Whitepaper

Automotive System Threat Modeling

Understand the IoT and Automotive Security-related Threats in One Go!



THE AUTHORS

Yashodhan Vivek
IoT Security Researcher
& Compliance Manager

Yashodhan is an IoT Security Researcher and Compliance manager at Payatu. He has Research and Development experience in the IoT and AI domain of more than 10 years. Currently, he is pursuing a Ph.D. in Astro Photonics. His academic qualification involves M.Tech Satellite Communication, M.Tech Signal Processing, B.E (E&TC). He has developed and delivered Industrial IoT products with AI capabilities. He also has research experience in Signal Processing, RF and Electromagnetics, and cubesatellite.
At Payatu, he is responsible for security assessment and creating threat models for IoT products and is working on research focusing on Side-channel attacks and Fault injection.

Tanvi Tirthani
Content and Media Strategist

Tanvi is a Content and Media Strategist with a special foray into technology. She's been in the martech field ever since the beginning of her career. With an MBA in Marketing, Tanvi is well equipped to develop memorable content collaterals, where technology comes easy to her!
At Payatu, you will find her working with the tech team to help them enrich their copies and assets, before they are rolled out to the general public. A lot of her time here is spent understanding the cybersecurity arena and penning things down in a distinct reflective manner.

Table of Contents

1. EXECUTIVE SUMMARY

This document discusses Threat Model and Security Objectives for the basic automotive platform. The manufacturer can refer to this document as a minimalistic threat model and can develop the rest of the security objectives on top of it. it. Based on the description of the system, the document lists the assets that need protection and the threats that are considered in the scope. The threats have been considered on the basis of major security features in the system. The security problem has been defined with respect to Confidentiality, Integrity, and Availability, i.e., CIA Triad. The necessary security objectives have been discussed to mitigate the threats that have been identified.

Why should you read it?

This whitepaper will be ideal for IoT/automotive security researcher/ developer to get an understanding of overall threats for systems and the security objectives to be achieved. So, if you are in this field and looking for a detailed technical paper to help you understand things better, then this is the resource for you.

What is the problem that this paper aims at solving?

This paper will give you a deeper view of the identification and possible mitigation of threats in IoT/automotive systems. With this paper, we aim at making some contribution in the domain of IoT/automotive security, which in turn may be beneficial for professionals in protecting these systems.

How will we try to make this contribution?

This document has been created considering automotive security use cases. Here, we discuss the necessary components in automotive domain from embedded/IoT perspective as base architecture. Considering that the security objectives have been proposed.

2. INTRODUCTION

This section provides an overview of the Target of Evaluation (TOE)

The threat model and security objectives for the mentioned TOE have been evaluated based on Common Criteria (CC) and Platform Security Architecture (PSA).

CC is an ISO/IEC 15408 standard for computer security certification. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) in a Security Target (ST) and may be taken from Protection Profiles (PPs). Common Criteria maintains a list of certified products, including operating systems, access control systems, databases, and key management systems.

Platform Security Architecture (PSA) is an initiative from Arm that aims to address some of the shortcomings with IoT security. It has the goal to demystify implementation choices and bring coherence to the IoT ecosystem.

The basic and minimalistic automotive system architecture is shown in figure 1. Following are the components of reference architecture.

1. The telematics component includes GPS and cellular communication.
2. The touch screen, voice commands and audio are part of HMI component.
3. The communication component contains internal communication between ECU and other components.
4. Infotainment system is an extension of the HMI system. It includes audio video, entertainment system through Bluetooth and WiFi interface.
5. Sensors system includes all sensors in different components for various ECU. The actuator system component has an anti-braking system, fuel injection, window control, and steering control, etc.

6. The Diagnostics component includes fault diagnostic systems such as On Board Diagnostics (OBD-II) protocol. This also includes Controller Area Network (CAN) protocol and FlexRay protocol.
7. Firmware runs on the top of the Operating system.
8. The operating system either runs Linux OS or Android Open-Source OS (AOSP)

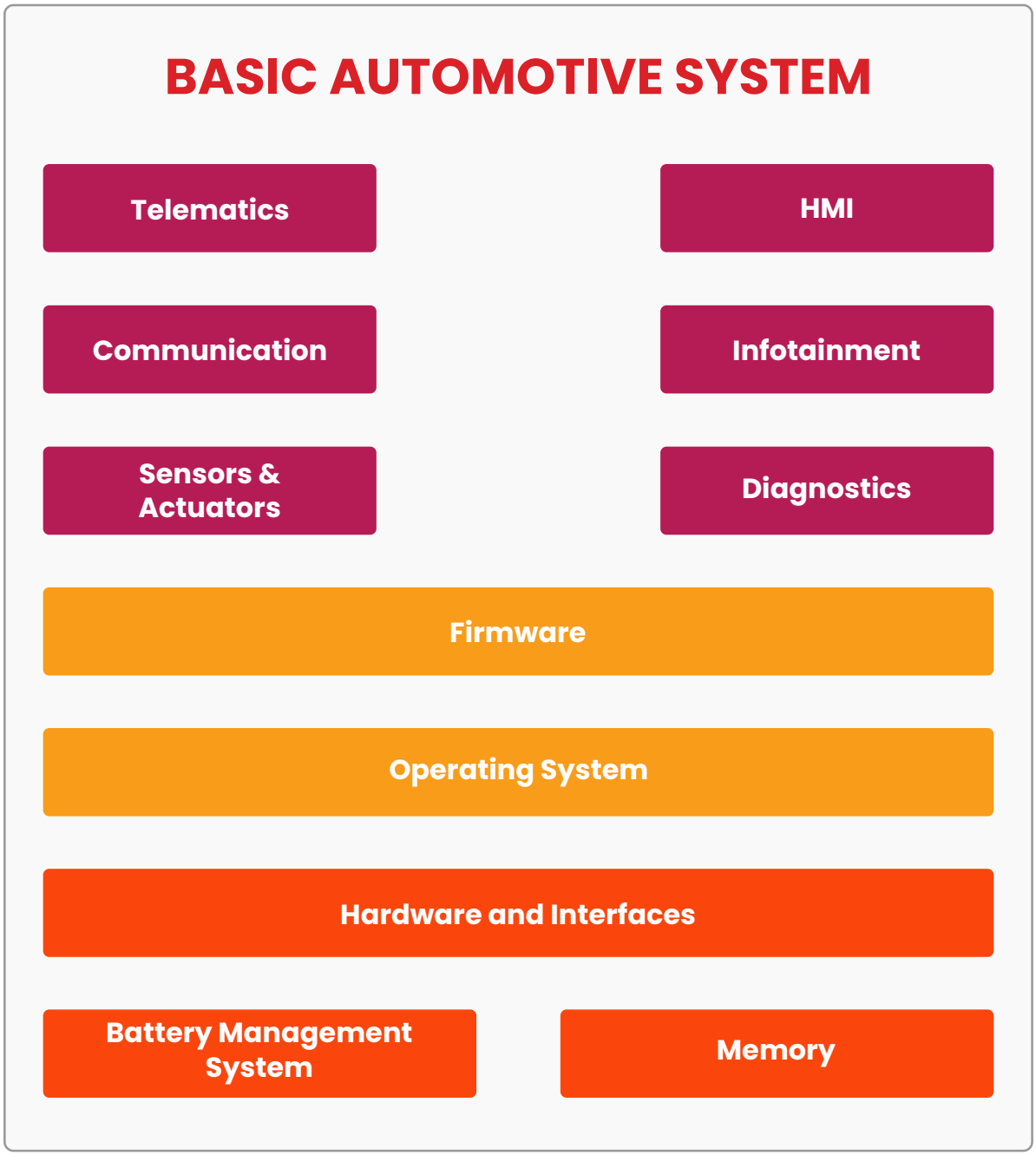


FIGURE 1

2.1 TARGET OF EVALUATION (TOE) OVERVIEW

2.1.1 TOE TYPE

1. The TOE of this protection profile (PP) is the basic embedded system for automotive.
2. The TOE is a platform composed of a hardware device and firmware implementing automotive functionalities such as vehicle health, infotainment system, and telematics. The firmware itself may include a generic purpose operating system.

2.1.2 TOE USAGE AND MAJOR SECURITY FEATURES

1. One of the security features includes communication that includes WiFi, Bluetooth/Bluetooth Low Energy (BLE), and cellular communication. Also, positioning technology GPS will be addressed. Cellular communication and GPS maps to the telematics component of the reference architecture.
2. The PP will focus on all communications to optimize location mapping that includes GPS and, if needed, triangulation from 4G cellular communications may be used to achieve precise location.
3. The TOE may include sensors such as temperature sensor, pressure sensor for Tyre Pressure Monitoring System (TPMS), accelerometer and gyroscope, ambient light sensor.
4. The PP has a capacitive touch screen and audio player as a part of the infotainment system.
5. The battery management system (BMS) of TOE also comes with security features.
6. The Onboard Diagnostics (OBD II) is one of the critical security features necessary for diagnostics.

2.2 TARGET OF EVALUATION (TOE) DESCRIPTION

The figure shown below illustrates the basic components for an automotive system, and TOE for this is PP.

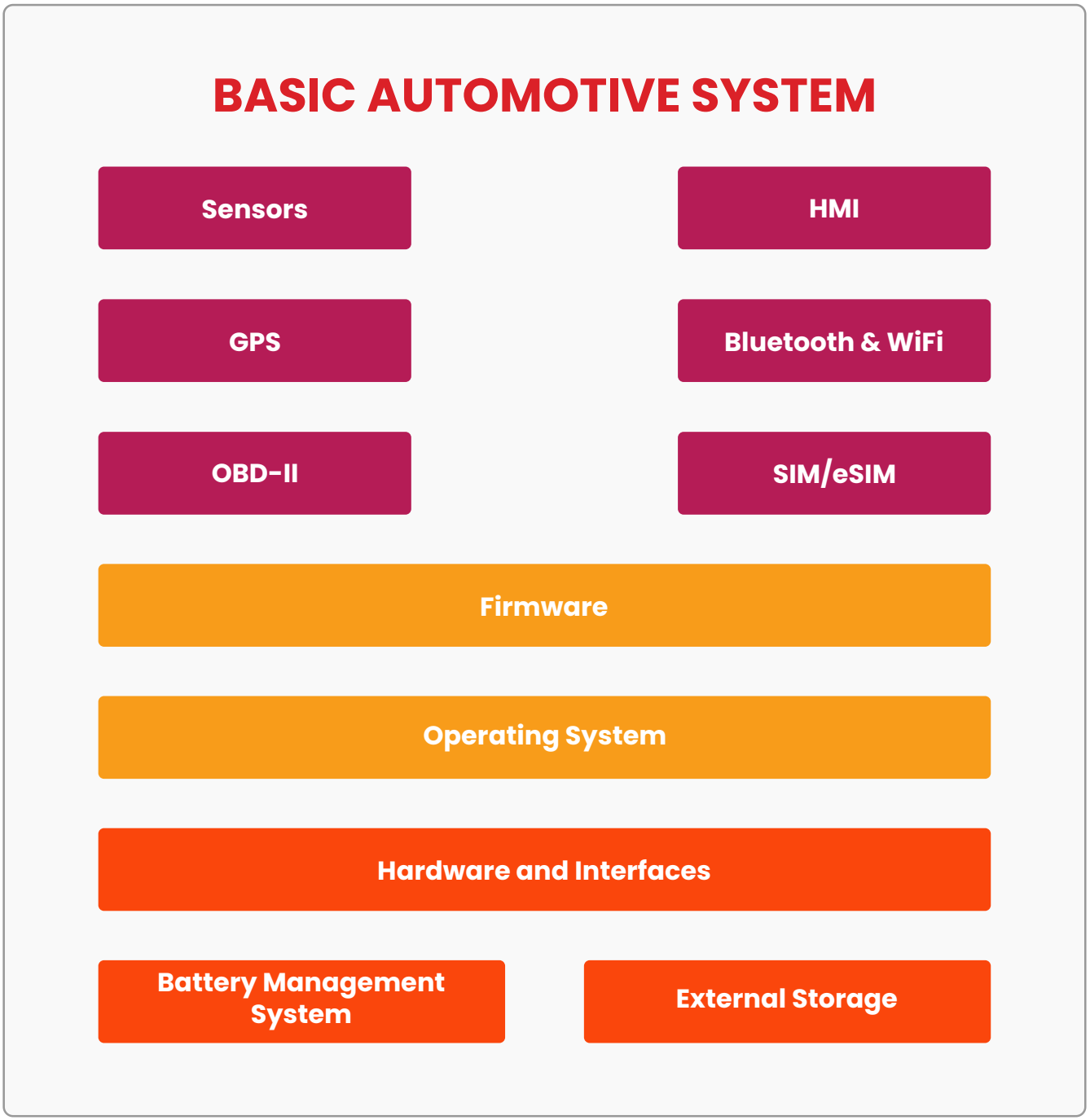


FIGURE 2

2.2.1 TARGET OF EVALUATION (TOE) FEATURES

1. Authentication: User must be authenticated prior to modifying configuration or updating system functionality. Also, the cellular network operated by a dedicated telecom operator requires authentication through SIM/eSIM.
2. Authorization: Some of the features such as BLE pairing, WiFi connectivity, and Google maps access should be limited to limited users.
3. Secure communication: Generally, any communication over the network is performed using a protocol that includes integrity and confidentiality protections. Also, the communication between peripherals and the main processor should be secure, e.g., communication between external storage and processor, OBD II and ECU.
4. Log of security events: Security events are logged locally on the device to be made available in the forensic analysis of an attack or after another suspicious event.
5. Firmware update: The firmware running on the TOE can be updated in order to fix vulnerabilities identified after the device's deployment. Also, it needs to verify that thdevice cannot be downgraded to known vulnerable versions i.e, anti-rollback for a firmware update.
6. Tampering detection: The device is likely to include a combination of hardware and software measures to detect attempts to tamper with the device.

2.2.1.1 HARDWARE

1. Basic hardware for an automotive embedded system typically consists of a processor with external flash memory and ECU for controlling automotive operations that includes OBD II protocol and TPMS.
2. Sensitive data such as the user's driving license and vehicle registration details may be stored on external storage devices.
3. The Human Machine Interface (HMI) component typically consists of a touch screen, multimedia system with communication that includes Bluetooth, WiFi

and telematic system that includes GPS and Cellular communication.

4. Battery Management System (BMS), its trickle charging, and battery status is stored in external flash memory.

2.2.1.2 FIRMWARE

1. Firmware for each individual subsystem of automotive typically consists of a bootloader, an OS for the processor and firmware running on top of the OS.
2. The firmware is responsible for implementing TOE functionalities.
3. Each ECU will have its own firmware and functionalities.
4. The HMI component of architecture typically consists of a touch screen and infotainment system firmware.
5. The communication component involves Bluetooth, WiFi and other short range RF communication between various sensor modules and ECU.
6. Firmware is usually stored on a flash memory to support upgrades.
7. Software for the TOE includes the SIM application, responsible for management of network authentication keys and for network authentication. Also, it adds the functionality of GPS navigation and positioning and managing calls over Bluetooth.

3. SECURITY PROBLEM DEFINITION

This section uses abbreviations for the following terms: Threat = T.
Assumptions = A
Organisational Security Policy = P
Objective for the Target of Evaluation (TOE) = OT
Objective for the Environment = OE

3.1 USERS AND EXTERNAL ENTITIES

1. The external entities that are considered in this PP are:
   i. Remote Admin: The remote admin here refers to automotive manufacturers. This entity operates from backend servers and can configure the automotive embedded system platform remotely.
   ii. Local Admin: Local admin here refers to the user. This entity operates locally and can configure the automotive embedded system platform and perform firmware updates.
   iii. Attacker: This user can target the automotive embedded system for financial or malevolent reasons. Attackers can operate remotely or locally.
2. Remote and Local Admin entities are not necessarily users but can be devices or systems controlled by trusted users.

3.2 ASSETS

3.2.1 TARGET OF EVALUATION SECURITY FUNCTIONALITY (TSF) DATA

The following assets contain data that belongs to TSF.

3.2.1.1 AUTOMOTIVE EMBEDDED SYSTEM PLATFORM ID

1. A unique ID to identify the device on a network, which may be the Media Access Control (MAC) address of the device or also the International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) in case of a cellular network.
2. Properties: Integrity

3.2.1.2 FIRMWARE

1. The automotive platform firmware
2. The firmware of ECU responsible for diagnostics and communication
3. The infotainment firmware
4. The HMI firmware
5. The communication firmware
6. The BMS firmware
7. Properties: Integrity, Authenticity

3.2.1.3 FIRMWARE CERTIFICATE

1. The cryptographic certificate is used to authenticate firmware and firmware updates.
2. Properties: Integrity

3.2.1.4 LOGS

1. The event logs that can be used to detect suspicious activities.
2. Properties: Integrity

3.2.2 USER DATA

3.2.2.1 LOCATION

1. The location of the automotive vehicle is calculated by the device. This location is recorded at regular intervals, according to the configuration.
2. Properties: Integrity, Confidentiality.

3.2.2.2 CONFIGURATION

1. The automotive platform's configuration is split into three major components
   i. The software configuration of the device, including the location measurement patterns, the aggregation method, and the alert trigger configuration
   ii. The network configuration of the device, including IP address of backend

servers and security settings

iii. The Bluetooth profile configuration of the device

iv. The WiFi configuration as access point mode or station mode

2. Properties: Integrity

3.2.2.3 CREDENTIALS

1. Authentication credentials, used for local and remote authentication, and for data protection during communication.
2. The secret keys shared during 4G communication viz. Evolved Packet System Authentication and Key Agreement (EPS AKA) protocol used for mutual authentication between devices and mobile core network must be pre-shared on the device and typically stored on a SIM or e-SIM.
3. The WiFi communication credentials
4. Properties: Integrity, Confidentiality

3.3 THREATS (T.)

An attacker is a threat agent (a person or a process acting on his/her behalf) trying to undermine the TOE security policy defined by the current security target (ST) and, hence, the Target of Evaluation Security Functionality (TSF). The attacker especially tries to change the properties of the assets defined in Section 3.2.

3.3.1 T.IMPERSONATION

1. An attacker impersonates a maintenance device on the local interface.
2. The credentials may be obtained through insecure communication protocols or exposed through data disclosure.
3. The attacker may then modify configuration, firmware, or logs.
4. Assets threatened directly: Credentials.

Assets threatened indirectly: Firmware, Configuration, Logs.

3.3.2 T.MITM

1. An attacker performs a Man-In-The-Middle attack on Bluetooth, WiFi, and 4G communication.
2. The attacker may perform MITM on OBD II and modify messages on CAN and FlexRay.
3. The attacker may alter or modify messages exchanged with the device.
4. The attacker may then disclose and modify Location Records, Logs, Credentials, Configuration data.
5. Assets threatened directly: Credentials (Server), Logs, Location Records, Configuration.

3.3.3 T.FIRMWARE_ABUSE

1. An attacker installs a flawed version of the firmware and obtains partial or total control of the tracker. The firmware may have been modified prior to the attack to include malware or consist of an outdated version of the original firmware.

2. The attacker may, for instance, modify on the device the value of the firmware certificate used to authenticate the installed firmware or firmware updates.
3. The attacker may also exploit functionalities of the TOE that are available as functional requirements of the device.
4. Such an attack can allow for disclosing or modifying Configuration Data, Credentials, Firmware, or Logs. Assets threatened directly: Firmware, Firmware Certificate. Assets threatened indirectly: All.

3.3.4 T.HARDWARE_ABUSE

1. An attacker performs sniffing over protocols such as UART, SPI, I2C, CAN, OBD II and get access to data.
2. An attacker can perform sim unlock by sniffing the SIM data.
3. An attacker does the reverse engineering of PCB and gets access to debugging headers of JTAG, SWD, and UART.
4. An attacker can bypass the secure boot stage by performing Electromagnetic Fault Injection (EMFI) attack.
5. An attacker can get access to cryptographic keys by performing side-channel analysis during operation.
6. An attacker can perform Direct Memory Access (DMA) attacks that can compromise firmware locally or remotely on peripheral hardware.
7. Assets threatened directly: All. Assets threatened indirectly: All.

3.3.5 T.IMPERSONATION

1. A User of the device denies action performed on the TOE on its behalf.
2. This can be the local or remote administrator for configuration or firmware update.
3. Assets threatened directly: Logs, Location Records, Firmware.

3.3.6 T.TAMPER

1. An attacker tampers with the tracker and tries to access or modify assets in persistent or volatile memory. The main targeted assets are Location Record, Logs, Credentials, Cryptographic keys, Configuration data.
2. To perform this attack, the attacker may use debug functionalities or direct memory access.
3. Such an attack can, for instance, allow for cloning the device, modifying the actual location records or logs of the device, getting access to non-authorized features of the device, getting unauthorized access to the Bluetooth and WiFi or also performing a denial-of-service.
4. Assets threatened directly: All.

3.4 ORGANIZATIONAL SECURITY POLICIES (P.)

The TOE and its environment shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operation.

3.4.1 P.KEYS_MANAGEMENT

The cryptographic keys, credentials, and certificates used in the TOE shall be securely generated, provisioned on the TOE.

3.5 ASSUMPTIONS (A.)

This section describes the assumptions about the operational environment of the TOE.

3.5.1 A.TRUSTED_ADMIN

Admin of the TOE is assumed to follow and apply administrative guidance in a trusted manner.

4. SECURITY OBJECTIVES

This section uses abbreviations for the following terms:
Threat = T. Assumptions = A
Organisational Security Policy = P
Objective for the Target of Evaluation (TOE) = OT. Objective for the Environment = OE

4.1 SECURITY OBJECTIVES FOR THE TARGET OF EVALUATION (OT.)

4.1.1 OT.ACCESS_CONTROL

The TOE shall authenticate Remote and Local Admin entities before granting access to the configuration and logs and before performing firmware updates.

4.1.2 OT.SECURE_STORAGE

The TOE shall protect the integrity and confidentiality of the Credentials when stored, and protect integrity of Firmware Certificate, Configuration, and Logs when stored.

4.1.3 OT.FIRMWARE_AUTHENTICITY

1. The TOE shall authenticate and verify the integrity of the firmware image during boot and of new firmware versions prior to the upgrade.
2. The TOE shall also reject attempts of firmware downgrade, especially with vulnerable versions.

4.1.4 OT.HARDWARE_INTEGRITY

1. The TOE shall protect the hardware from Side-channel attacks, fault injection, and glitching with tamper-proof casing.
2. The TOE shall disable debug ports during operation.

4.1.5 OT.COMMUNICATION

1. The TOE shall only accept remote connections from configured back-end servers and be able to authenticate these servers.
2. The TOE shall only accept Bluetooth pairing with the authenticated device,
3. The local WiFi access point shall only be connected to authorized devices.
4. The TOE shall also provide authenticity, confidentiality, and replay protection for export outside of the TOE.

4.1.6 OT.AUDIT

The TOE shall maintain log of all significant events and allow access and analysis of these logs to authorized users only.

4.1.7 OT.TAMPER

The TOE shall react to physical tampering attempts. The tampering event detection can be achieved by various means such as crypto chip protection, sensors outside TOE that senses the opening and closing of the device, PCB track connected to processor pin to detect event, etc.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT (OE.)

4.2.1 OE.CREDENTIALS_MANAGEMENT

Similar to point discussed 3.4.1 P.KEYS_MANAGEMENT

4.2.2 OE.TRUSTED_ADMIN

The Admin of the TOE is not careless, willfully negligent or hostile.

4.3 SECURITY OBJECTIVES RATIONALE

The following table provides an overview of security objectives coverage (TOE and its environment) and also gives evidence for the sufficiency and necessity of the defined objectives. It shows that all threats and Organizational Security Policies (OSPs) are addressed by the security objectives and it also shows that all assumptions are addressed by the security objectives for the TOE operational environment.

SECURITY OBJECTIVES RATIONALE MATRIX

	OT.ACCESS_CONTROL	OT.SECURE_STORAGE	OT.FIRMWARE_AUTHENTICITY	OT.HARDWARE_INTEGRITY	OT.COMMUNICATION	OT.AUDIT	OT.SECURE_STATE	OT.TAMPER	OE.CREDENTIALS_MANAGEMENT	OE.TRUSTED_ADMIN
T.IMPERSONATION	X					X			X	
T.MITM					X					
T.FIRMWARE_ABUSE	X		X				X			
T.HARDWARE_ABUSE	X	X		X				X		
T.REPUDIATION	X				X	X				
T.TAMPER		X		X			X	X		
P.KEYS_MANAGEMENT	X								X	

TABLE 1

4.3.1 SECURITY OBJECTIVE RATIONALES: THREATS

4.3.1.1 THREAT: T.IMPERSONATION

This threat assumes that the TOE can be attacked by impersonating a legitimate user. This threat is countered by the security objectives OT.ACCESS_CONTROL that ensures authentication of users to access TOE functionalities and OT.AUDIT allows for an audit of TOE users' activities and by the security objective on the operational environment OE.CREDENTIALS_MANAGEMENT ensures that no default password can be used on operational usage.

4.3.1.2 THREAT: T.MITM

This threat assumes that the TOE can be attacked by intercepting or spying communications with remote servers, local Bluetooth devices, and WiFi access. This threat is countered by the security objective OT.COMMUNICATION that ensures authentication of remote servers, local, low-power, low-range communication, and protection in confidentiality and integrity of exchanged data.

4.3.1.3 THREAT: T.FIRMWARE_ABUSE

This threat assumes that the TOE can be attacked by modifying the firmware or installing an outdated, vulnerable version. This threat is countered by the security objectives OT.ACCESS_CONTROL that ensures only Admin can initiate firmware upgrade, OT.FIRMWARE_AUTHENTICITY that ensures verification of firmware authenticity prior use and prior upgrade, and OT.SECURE_STATE that ensures that the TOE maintains a secure state even in case of failure of verification of firmware integrity.

4.3.1.4 THREAT: T.HARDWARE_ABUSE

1. This threat assumes that the TOE can be attacked via open debug ports, extraction of firmware from external flash. These can be encountered by OT.ACCESS_CONTROL and OT.HARDWARE_INTEGRITY that ensures the TOE has protection against physical attacks. Also T.HARDWARE_INTEGRITY ensures that the debug ports of hardware are disabled.

2. This threat also assumes that TOE can be attacked with Fault Injection mechanisms such as EMFI, Voltage Glitching. To mitigate this attack, the device needs tamper protection that has been addressed in OT.TAMPER.

4.3.1.5 THREAT: T.REPUDIATION

This threat assumes that TOE users can deny their actions on the TOE. This threat is countered by the security objectives OT.ACCESS_CONTROL that ensures authentication of users to access TOE functionalities, OT.COMMUNICATION that ensures protection in the authenticity of exported TOE data and OT.AUDIT that allows for an audit of the TOE users' activities.

4.3.1.6 THREAT: T.TAMPER

This threat assumes that the TOE can be attacked by physical tampering. This threat is countered by the security objectives OT.SECURE_STORAGE that ensures a secure storage for TOE assets, by OT.SECURE_STATE that ensures that the TOE maintains a secure state in case of failure, and by OT.TAMPER that ensures reaction to physical tampering attempts.

4.3.2 SECURITY OBJECTIVE RATIONALES: SECURITY POLICIES

Each identified security policy in this Security Target is addressed by at least one security objective for the TOE or security objective for the operational environment. This section provides a mapping from each security policy to the security objectives and provides a rationale for how the security policy is fulfilled.

4.3.2.1 POLICY: P.KEYS_MANAGEMENT

This security policy is directly upheld by the security objective on the operational environment OE.CREDENTIALS_MANAGEMENT.

4.3.2.1 POLICY: P.KEYS_MANAGEMENT

This security policy is directly upheld by the security objective on the operational environment OE.CREDENTIALS_MANAGEMENT.

4.3.3 SECURITY OBJECTIVE RATIONALES: ASSUMPTIONS

Each security assumption in this Security Target is addressed by at least one security objective for the operational environment. This section maps assumptions to environmental security objectives and provides a rationale for how the assumption is fulfilled.

4.3.3.1 ASSUMPTION: A.TRUSTED_ADMIN

This security policy is directly upheld by the security objective on the operational environment OE.TRUSTED_ADMIN.

CONCLUSION -

The Threat model and security objectives discussed in the document considers different components of the system architecture as an asset and evaluates the possible threat for each of them. To counter the threats, we have also discussed about the security objectives. The security rationale matrix mapped for security objectives against the listed threats in the document will help the IoT/Automotive developer to address security efficiently.

About Payatu

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

Our deep technical security training and state-of-the-art research methodologies and tools ensure the security of our client's assets.
At Payatu, we believe in following one's passion, and with that thought, we have created a world-class team of researchers and executors who are willing to go above and beyond to provide best-in-class security services. We are a passionate bunch of folks working on the latest and cutting-edge security technology.

One of the Payatu's brand, EXPLIoT is all set to launch its revolutionary IoT Security Assessment Platform – IoT Auditor.

Don't forget to sign up for its limited access community edition.

If you're only getting started with IoT Security, get your hands on the IoT Security Learning Kit.

Visit the EXPLIoT store here.

Want to know more about the distinct premium services security services offered by Payatu?

Tell us about your specific requirements here, and we will get back to you with a customized sample report.

Payatu Security Consulting Pvt. Ltd.

www.payatu.com
info@payatu.com
+91 20 41207726