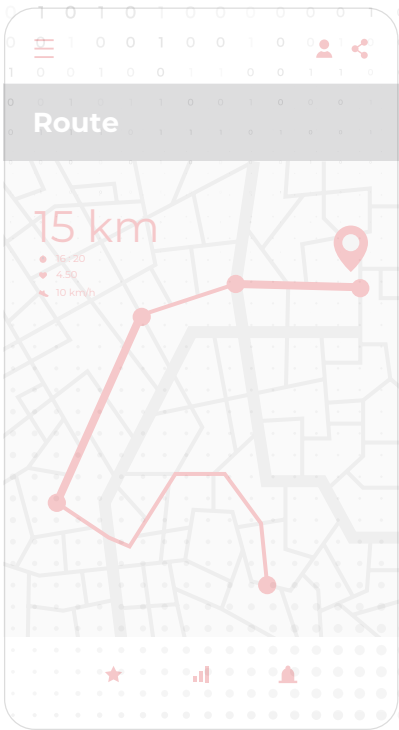




Payatu Case Study

# Bridging Security: Pentesting an Automotive ECU



# Project Overview

In today's automotive landscape, cybersecurity is no longer an afterthought, it is a fundamental necessity, especially for manufacturers developing vehicle-integrated devices. A leading global telematics company, specializing in Electronic Control Units (ECUs) and vehicle trackers, recently engineered an advanced intelligent solution designed to deliver a safe, seamless, and connected driving experience. This solution enables users to monitor vehicle health and location in real-time, complete with alerts, notifications, and detailed driving pattern analytics.

Before launching this innovative device to market, the company prioritized a comprehensive security assessment. Their goal was clear: to **identify vulnerabilities, understand the associated risks, and develop a prioritized roadmap for remediation** to ensure a resilient and trustworthy product.

Given the criticality of the device's function and its exposure to complex attack surfaces, the assessment encompassed a detailed examination of its hardware components, decryption of the encrypted Firmware Over-The-Air (FOTA) image, and analysis of the Bluetooth Low Energy (BLE) radio protocol.

Let's take a closer look at how this security evaluation unfolded.

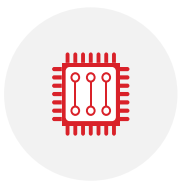
# The Scope

The engagement involved a comprehensive security assessment of the ECU, covering multiple critical areas:



## **Hardware Assessment:**

In-depth analysis of the device's physical components and attack surfaces.



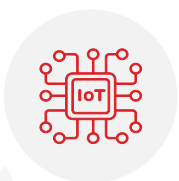
## **Firmware Assessment:**

Decryption and detailed examination of the encrypted firmware.



## **Radio Protocol Assessment (BLE):**

Evaluation of the Bluetooth Low Energy Communication.



## **IoT Protocol Analysis (MQTT):**

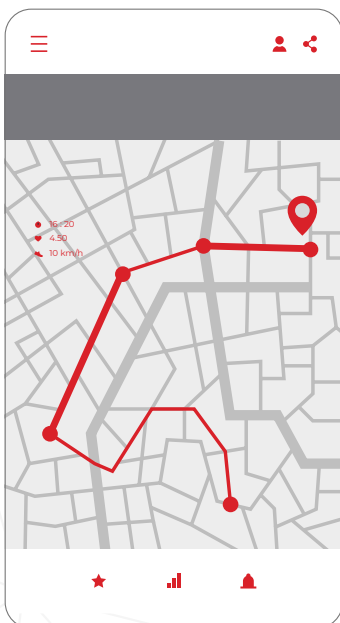
Review of the MQTT messaging protocol to identify security gaps in device-to-cloud communication.

# Process

The ECU under assessment is an intelligent in-vehicle solution designed to deliver a safe, convenient, and connected driving experience.

It enables users to monitor vehicle health and location in real time, with instant alerts and notifications. Additional features include detailed analysis of driving patterns and trip history, offering deeper insights into vehicle usage and performance.

All data and features are accessible via the user's smartphone, laptop, tablet, or PC, ensuring seamless connectivity across platforms.



# Hardware Assessment

The hardware assessment of the ECU was conducted at the [Payatu Laboratory](#). Given the potentially destructive nature of hardware testing, three identical units were provided for analysis to ensure continuity in case of physical damage.

This was a **black-box assessment**, with the only supporting document being the device's user manual. Initial interactions with the client's development team were essential to gain a foundational understanding of the device architecture and its intended functionalities.

Below is the structured process followed during the hardware assessment:



**External Reconnaissance:** Identified all external interfaces (e.g., USB, CAN) and analyzed their intended functions.



**Interface Fuzzing:** Conducted fuzzing on the CAN and USB ports to identify any unhandled or insecure input behaviors.



**Sniffing and Replay Attacks:** Captured CAN bus traffic and attempted replay attacks to evaluate message validation and bus-level security.



**Internal Reconnaissance:** Inspected the PCB to identify critical components and locate potential debug interfaces.



**Debug Port Scanning:** Probed for active UART and JTAG ports to assess the level of access available.



**Debug Port Exploitation:** Captured boot logs and obtained shell access via UART. Leveraged JTAG to dump and patch firmware from the microcontroller's internal memory. The firmware was encrypted at rest, making access to the initial bootloader essential for decryption efforts.



**Readout Protection Bypass:** Applied fault injection (power glitching) techniques on the power rail to bypass microcontroller readout protections and gain access to protected memory.



**External Memory Extraction:** Retrieved firmware and data from external flash memory components present on the board.



**Firmware Decryption and Analysis:** Extracted firmware was handed over to the firmware analysis team. Despite being encrypted at rest, appropriate decryption strategies were successfully applied to analyze the firmware contents.



**Reporting:** All identified weaknesses, including insecure debug configurations, protection bypasses, and firmware-level flaws, were thoroughly documented and included in the final assessment report.

# Wireless Assessment

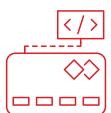
The ECU under assessment communicates with the user's mobile device via Bluetooth Low Energy (BLE), which was included within the scope of the evaluation.

The device uses a Realtek System-on-Chip (SoC) with BLE 5.0 stack support. BLE pairing was secured using a 6-digit PIN/passkey mechanism, intended to prevent unauthorized devices from accessing or modifying characteristic values.

Following an initial review of the configuration, the team initiated the BLE security assessment using the process outlined below:



**Reconnaissance:** Collected technical details about the BLE implementation and confirmed that it was built on a Realtek SoC with BLE 5.0 capabilities.



**Service and Characteristic Enumeration:** Attempted to enumerate available BLE services and characteristics without pairing, to test exposure prior to authentication.



**CVE Exploration:** Investigated known vulnerabilities associated with the Realtek chipset and BLE 5.0 stack. Publicly available exploits were tested to determine if the device was susceptible to these issues.



**Attack Execution:** Successfully performed certain enumeration techniques and denial-of-service (DoS) attacks, demonstrating potential weaknesses in the device's BLE handling and resilience.



**Reporting:** All findings, including unauthorized access attempts and successful DoS scenarios, were documented in detail as part of the final assessment report.

# Protocol Assessment

As this was a black-box assessment, no prior information about the MQTT implementation was shared by the client.

However, during BLE traffic analysis, the team identified a broker endpoint being used by the device for communication. This discovery enabled further evaluation of the MQTT protocol's security posture.

The assessment flow was as follows:



**MQTT Client Setup:** A custom client script was written to interact with the broker.



**Connection Attempt:** The broker accepted unauthenticated connections.



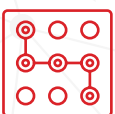
**Topic Enumeration:** Subscription to the wildcard topic (#) was successful, revealing access to system-level topics.



**Topic Analysis:** Additional sensitive endpoints were identified and subscribed to.



**Data Exposure:** Unencrypted firmware and other critical data were accessible through these topics.



**Data Manipulation:** Successfully published data to topics, confirming the absence of proper authorization controls.

# Challenges



Tight deadlines and client pressure to complete the assessment quickly.



Limited documentation made it a little complex.

# Findings

The most prominent findings were -

Vulnerability ID	Finding OWASP Top 10 Category	Severity
PY-TM-001	<b>Insecure Ecosystem Interfaces:</b> Exposed MQTT endpoint and credentials in the firmware present on HTTP server	<b>CRITICAL</b>
PY-TM-002	<b>Insufficient Privacy Protection:</b> Writing to the services and characteristics	<b>MEDIUM</b>
PY-TM-003	<b>Lack of Physical Hardening:</b> Open SWD port for Realtek BLE SoC with no authentication	<b>LOW</b>

The biggest finding was that

The IoT ecosystem extends beyond just the device. Using the device as an entry point, the Bandits were able to infiltrate the client's production server, gaining access to sensitive information, including customer data and other client details. They also succeeded in obtaining the client's firmware in an unencrypted, plain-text form, further exposing critical intellectual property and system functionality.

# Business Impact



The biggest business impact was that the MQTT protocol vulnerabilities uncovered could have led to a serious data breach, exposing sensitive customer and client information. Such a breach would have critical consequences, including loss of customer trust, regulatory sanctions, and substantial financial and reputational damage.








Unauthorized access to sensitive customer data could severely damage brand reputation and erode user confidence.





Compromise of production servers or ECU functionality could lead to service outages or vehicle malfunctions, impacting business continuity.

# Remediation

-  Authentication on the HTTP file server should be implemented.
-  To write any value to the handles, the BLE should ask the Passkeys.
-  The size check should be implemented to avoid length overflow scenarios.
-  Disable the SWD port.
-  Implement authentication on SWD access.

# Before Vs After

<b>BEFORE</b> 	<b>AFTER</b> 
Open hardware debug ports	Secure hardware debug ports
Potential exposure of sensitive information via BLE communication	No sensitive information leakage via BLE communications
<ul style="list-style-type: none"><li>- Lack of authentication and authorization on the MQTT endpoints</li><li>- Access to unencrypted firmware on the MQTT server</li></ul>	Authentication on the MQTT server

# 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.



## IoT Security Testing [↗](#)

IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.



## Web Security Testing [↗](#)

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.



## DevSecOps Consulting [↗](#)

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.



## Product Security [↗](#)

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components “fit” together in your mega-product.



## Cloud Security Assessment [↗](#)

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared. As long as cloud servers live on, the need to protect them will not diminish.

Both cloud providers and users have a shared responsibility to secure the information stored in their cloud Payatu’s expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.



## Code Review [↗](#)

Payatu’s Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.



## Red Team Assessment [↗](#)

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization’s crown jewels and test its readiness to detect and withstand a targeted attack.



## Mobile Security Testing [↗](#)

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.



## Critical Infrastructure Assessment [↗](#)

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation systems etc. and can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your critical infrastructure.



## CTI [↗](#)

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting – social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platform monitoring done for their brand.

### More Services Offered

- AI/ML Security Audit [↗](#)
- Trainings [↗](#)

### More Products Offered


- EXPLIoT [↗](#)
- CloudFuzz [↗](#)




**Payatu Security Consulting Pvt. Ltd.**

 [www.payatu.com](http://www.payatu.com)

 [info@payatu.io](mailto:info@payatu.io)

 +91-20-47248026

 +91-8319812123 (SALES)

