Payatu

Payatu Casestudy

Automotive Startup Finds Critical Vulnerabilities in EV With Payatu’s Automotive Security Testing

Payatu Security Consulting Pvt. Ltd

Project Overview

The disruption in the automotive industry is leading to a prominent shift from ICE (internal combustion engine) vehicles to EVs (electric vehicles). More and more companies are trying to make a name for themselves in this space, keeping sustainability and security at the core. One such promising startup approached Payatu to test its products.

This electric mobility firm designs, manufactures, and sells high-performance electric scooters. The client has a product rolled out in the market that offers super-fast dashboard interactions, great design, and seamless rides.

Payatu was now given the responsibility of assessing different elements of the electric scooter and helping the company in improving the security posture of the product's hardware and software.

The Scope

- The Dashboard
  - Firmware
  - Hardware
- The in-vehicle network (CAN Bus)
- Wireless communication (Bluetooth) with associated app

IoT Security Assessment of the product was performed, considering below common security issues -

☑ If any hardware debug ports are open

☑ If proper access control is implemented across the vehicle

☑ If proper Authorization & Authentication System is implemented

☑ If the user input is properly managed

Test Cases

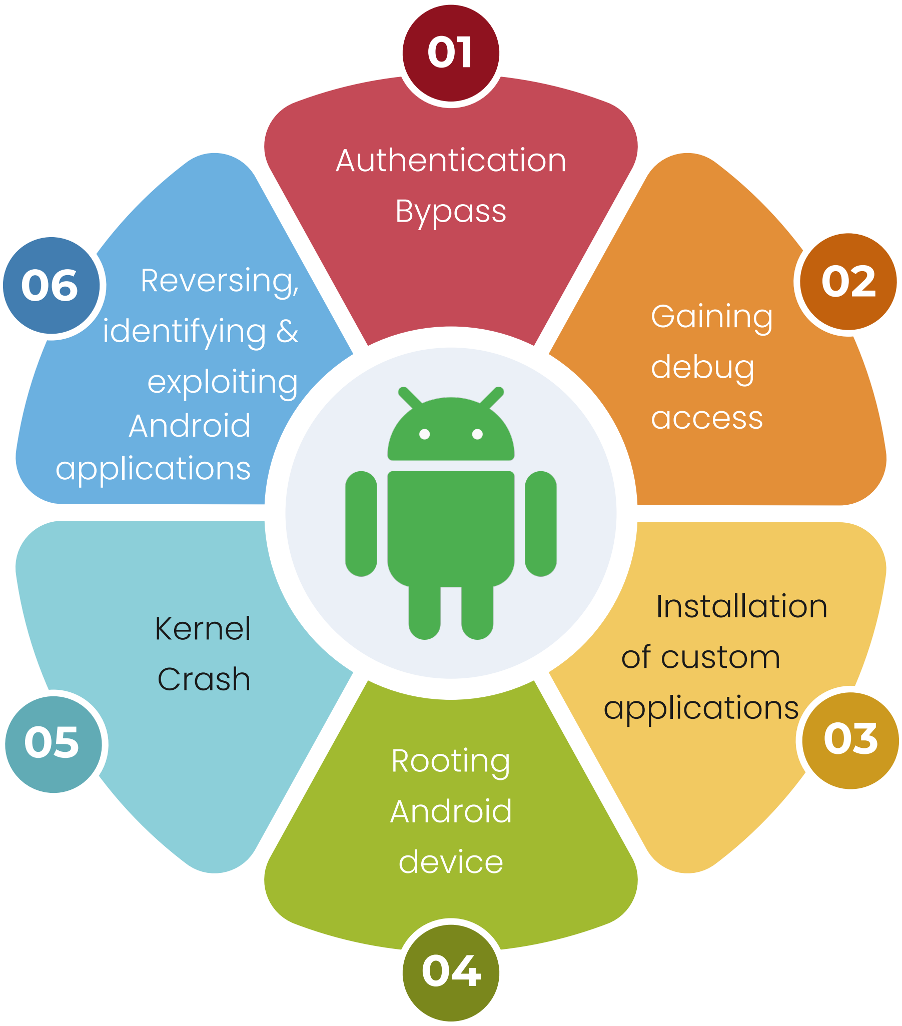
Track Firmware for the Testcases

1. Overall kernel, bootloader, architecture inspection
2. Finding running services
3. Extracting firmware/credentials/hardcoded sensitive information
4. Identifying and analyzing custom binaries
5. Analyzing firmware for vulnerabilities' processes
6. Firmware Update Mechanism
7. Updating the device with malicious files
8. Firmware Encryption Mechanism
9. Firmware Validation using secure boot

Track Hardware for the Testcases

- List out all controller and memory chips used in system
- Check for test points debug ports on the PCB
- Gather information on various ICs
- Map internal architecture of the system
- Find Datasheets and Pinouts of SOC
- Get Datasheet for memory chips used
- List out possible memory extraction methods
- Extract the Memory (SPI flash, EMMC, NAND flash)
- Reflash the extracted Memory
- Find UART Port on the dashboard
- Access to the device root shell UART
- Find JTAG/SWD on the dashboard
- Firmware extraction via JTAG/SWD
- Check if modified firmware can be written back to the device
- Sniff communication over the bus (SPI/I2C)

Track Android for the Testcases



01 Authentication Bypass

02 Gaining debug access

03 Installation of custom applications

04 Rooting Android device

05 Kernel Crash

06 Reversing, identifying & exploiting Android applications

Track Wireless for the Testcases

1 Identify BLE communication (version, MAC)

2 Sniff BLE communication

3 Identify handles being read and written

4 BLE replay and relay attack

5 Character Fuzzing

6 BLE MiTM

7 Verify that WPA2 or higher is used to protect Wi-Fi communications

8 User Data Exfiltration

9 Compromise the confidentiality of data

Track Network for the Testcases

- Sniff data packets from exposed Bus endpoints
- Replay attack on the CAN nodes (network of devices required)
- Spoofing attack on the CAN nodes (network of devices required)
- Reverse CAN Bus packets
- Fuzzing CAN Bus communication
- UDS packet injection

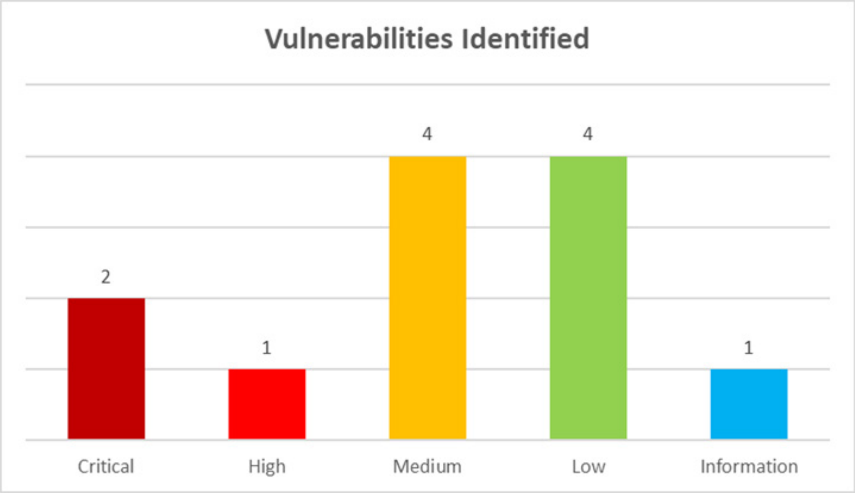
Challenges

Crunched Timelines

Access to the internal E/E components of the vehicle was limited

Limitations to the assessment made the entire process quite challenging

Findings



Critical Vulnerabilities

1. Escape to system via ADB

During the assessment, the ADB shell was found to be accessible to the normal user. This allows the user to execute shell commands on the dashboard to escape out of the EV interface to the core Android settings.

2. Outdated/Vulnerable Android Version

During the assessment, it was discovered that the Android running on the dash-board is an outdated version without any recent security patches making remote exploitation possible.

High Vulnerabilities

1. I2C Memory Extraction (Odometer Data)

During the assessment, it was observed that the I2C EEPROM is used for storing odometer data. An attacker can dump the data and modify and reflash the modified data.

2. DoS on CAN Bus (Vehicle in standby mode)

During the assessment, it was observed that the vehicle CAN Bus network was not encrypted. The vulnerability allows the attacker to analyze the data packets and deploy a DoS attack by injecting packets at a very high bitrate.

3. Packet injection on CAN Bus (Indication signal spoofing)

During the assessment, it was observed that the vehicle CAN Bus network was not encrypted. The vulnerability allows the attacker to analyze the signal indicators' data packets and deploy a packet injection attack which gives the attacker control of the signal indicators.

4. Dashboard logs in Cleartext

During the assessment, it was observed that the dashboard is exposing the logs in Cleartext. It was also observed that the JWT token and Google map API Key are exposed in application logs which can be used by the attacker to remotely read these logs through any application.

Low Vulnerabilities

1. DoS on CAN Bus (Vehicle in riding mode)

During the assessment, it was observed that the vehicle CAN Bus network was not encrypted. The vulnerability allows the attacker to analyze the data packets and deploy a DoS attack by injecting packets at a very high bitrate.

2. SWD port open

During the assessment, it was observed that the SWD port is open, and an attacker can dump the firmware, also reflash the modified binary.

3. Android recovery/fastboot mode via ADB

During the assessment, it was observed that the Android recovery and fastboot modes were accessible via ADB. It was also observed that the dashboard had an unlocked bootloader.

Remediations

- Debug (ADB) access should not be provided to end users
- Device should be provided with regular security patches
- Application installation permissions should be restricted
- Use an encrypted way of storing EEPROM data, which should be tamper proof
- A Bus guardian is needed to monitor the CAN Bus usage engage kill switch
- CAN Bus IDS is necessary for monitoring several packet injection attacks and defending CAN Bus attacks
- Device log access should be restricted to system apps
- Always make sure the SWD pins are not exposed on the PCB
- Bootloader functionalities should be locked to end users

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

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.com

+91 20 41207726