

CAR HACKING VILLAGE | ROOTCON

VEHICLES | RESEARCH | COMMUNITY

HACKING
MOBILITY
FOR A SAFER
TOMORROW

RIDE HACKED

IMPLANTING OFFENSIVE HARDWARE
INTO CONNECTED E-SCOOTERS

By

Omkar Mali

Security Researcher



HARDWARE
IMPLANTS



GSM / SIM
COMMANDS



REAL-WORLD
IMPACT

SAME ROADS. NEW RISKS.



REMOTE
COMMANDS
REAL IMPACT



THANK YOU

SHUBHAM

FOR GIVING ME A
BRAND NEW SCOOTER
FOR RESEARCH

YOUR SUPPORT
HELPS FUEL
EXPLORATION,
LEARNING AND
RESEARCH.



EXPLORE



REVERSE



LEARN



BUILD

TWO WHEELS.
A BIGGER TOMORROW.



02

BACKGROUND & MOTIVATION

WHY THIS RESEARCH MATTERS?

Modern two-wheelers are no longer just mechanical machines — they are connected, software-defined and remotely manageable.



CELLULAR CONNECTIVITY

2G/4G modules for telematics, tracking and remote services.



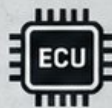
BLUETOOTH PAIRING

Smartphone apps for vehicle control, analytics and notifications.



CLOUD INTEGRATION

Enables remote diagnostics, updates and fleet management.



MULTIPLE ATTACK SURFACES

Mobile app, backend APIs, cellular module, infotainment cluster and internal buses (e.g., CAN).



RESEARCH GOAL

To investigate how a **simple** phone call can be leveraged as an initial entry point to **compromise connected** two-wheelers, and demonstrate the real-world impact of such an attack.

02.1

REAL-WORLD SCENARIO

A rider receives a phone call. What seems like a normal interaction could be the beginning of a complete vehicle compromise.



ATTACKER

Initiates a phone call using crafted input (e.g., voice, DTMF, or network-based tricks).



PHONE CALL

Triggers vulnerability in the connected system (modem, app or backend).



REMOTE ACCESS

Gains foothold in the vehicle's telematics or control systems.



SCOOTER TAKEOVER

Execute commands (e.g., track, lock/unlock, disable, or manipulate vehicle functions).



A PHONE CALL
CAN BE MORE
THAN A CONVERSATION.
IT CAN BE A COMMAND.



KEY TAKEAWAY

CONNECTED MOBILITY BRINGS CONVENIENCE, BUT ALSO NEW AND OFTEN OVERLOOKED ATTACK VECTORS.

TWO WHEELS.
A BIGGER ATTACK SURFACE.

03 ATTACK SURFACE ANALYSIS

A WIDER ATTACK SURFACE

MODERN SCOOTERS ARE CONNECTED ECOSYSTEMS

A simple phone call can interact with multiple interconnected components, expanding the attack surface far beyond traditional vehicle boundaries.

3.1 ATTACK SURFACE OVERVIEW



CELLULAR MODULE

2G/3G/4G (Voice, SMS, Data)
Telematics & remote services



BLUETOOTH

Smartphone pairing
App integration
Diagnostics



MOBILE APP

Vehicle control
User accounts
Cloud connectivity



DIAGNOSTIC INTERFACE

OBD / Service port
Firmware updates
Maintenance access



CLOUD INFRASTRUCTURE

Backend APIs
Fleet management
Remote commands



INSTRUMENT CLUSTER

Display, alerts, pairing
Firmware updates
User interactions



ECU / CONTROLLER

Processes commands
Controls vehicle functions
Interfaces with CAN bus



CAN BUS NETWORK

Internal communication
Between ECUs and modules
Critical control functions



KEY TAKEAWAY

Connectivity, convenience and remote management introduce new entry points. Each interface is a potential attack vector that can be chained towards vehicle control.

IT'S NOT JUST A SCOOTER ANYMORE. IT'S A **CONNECTED PLATFORM**.

3.2 CONNECTIVITY ECOSYSTEM



SMARTPHONE
(App + Call + SMS)



CELLULAR NETWORK
(2G/3G/4G)



VENDOR CLOUD
(Backend Services)



SCOOTER
(ECU / Telematics)

MULTIPLE TRUST BOUNDARIES. MULTIPLE OPPORTUNITIES.

3.3 POTENTIAL THREAT ACTORS



REMOTE ATTACKER

Exploits cellular or cloud services to send malicious commands.



INSIDER THREAT

Misuses legitimate access (apps, tools, service accounts).



CELLULAR ADVERSARY

Exploits network weaknesses (e.g., SS7, SIM swap, IMSI catchers).



THIRD-PARTY RISK

Compromised apps, APIs or supply chain components.

DIFFERENT ACTORS. SAME OUTCOME. LOSS OF CONTROL.

06 TECHNICAL BACKGROUND

WHAT IS CAN BUS?

THE NERVOUS SYSTEM OF MODERN TWO-WHEELERS

CAN bus (Controller Area Network) is a robust communication system used in vehicles to enable ECUs (Electronic Control Units) to communicate with each other without a central host computer.

In a scooter, the CAN bus allows different control units (e.g., engine control, instrument cluster, ABS, telematics, keyless module) to quickly and reliably share information such as speed, throttle input, brake status, and diagnostic data.



LIKE A HUMAN BODY

The CAN bus acts as the nervous system, enabling communication between all ECU "organs".



ECUs ARE THE NODES

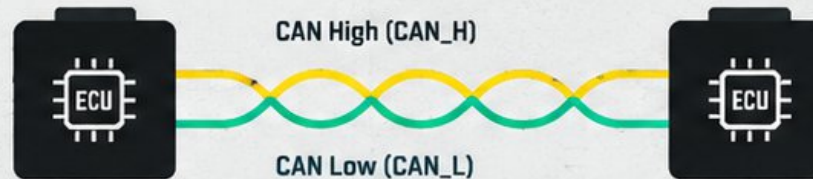
Each ECU is like a part of the body, interconnected via the CAN bus. Information sensed by one node can be shared with others.



TWO-WIRE BUS

All ECUs are connected using a twisted pair: CAN High and CAN Low. The wires are often color coded (yellow for CAN High, green for CAN Low).

6.1 CAN BUS WIRING



TYPICAL CHARACTERISTICS

- Two-wire differential bus (CAN_H & CAN_L)
- High noise resistance
- Supports multiple ECUs on the same bus
- Real-time, reliable communication
- Widely used in modern scooters and motorcycles

08 TECHNICAL BACKGROUND

EVOLUTION OF CAN BUS

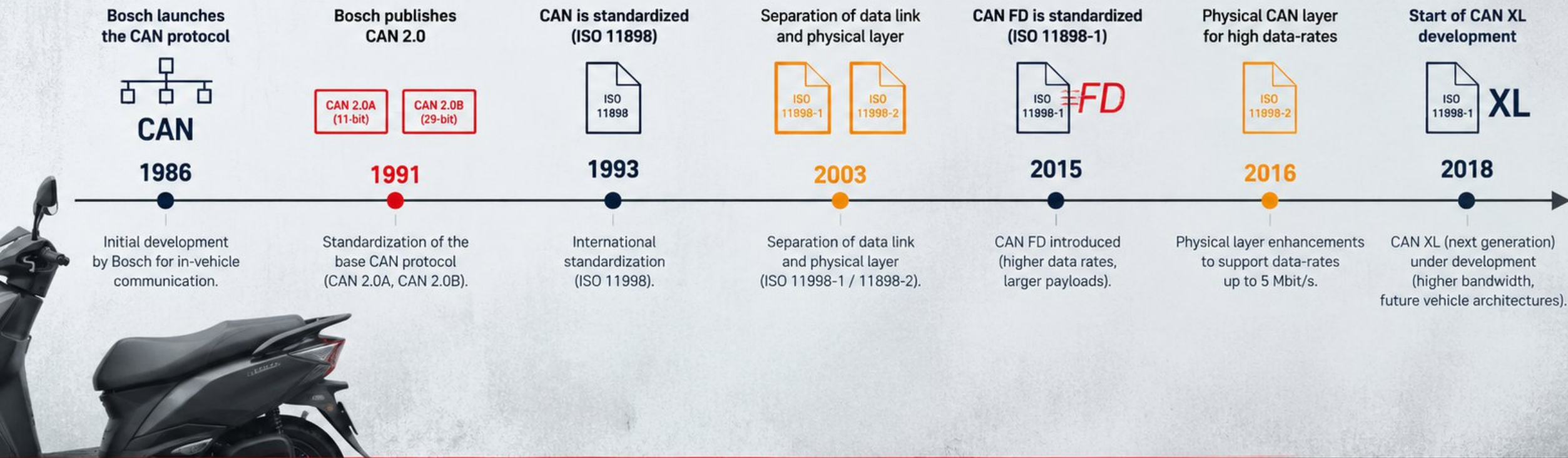
FROM AUTOMOTIVE ORIGINS TO MODERN CONNECTED TWO-WHEELERS

The CAN bus, originally developed for automotive applications, has evolved over the decades to support higher data rates, enhanced security and new use cases. Modern scooters leverage CAN (and emerging CAN FD) to interconnect multiple ECUs for control, diagnostics and connectivity.



WHY IT MATTERS FOR SCOOTERS?

Modern scooters use CAN and CAN FD to connect essential systems such as engine control, ABS, instrument cluster, telematics and more. Understanding the evolution helps identify legacy design decisions, capabilities and potential security shortcomings.



KEY TAKEAWAY

THE CAN BUS HAS EVOLVED TO SUPPORT HIGHER PERFORMANCE, MORE FEATURES AND CONNECTED VEHICLES. MODERN SCOOTERS LEVERAGE CAN/CAN FD, INCREASING BOTH CAPABILITIES AND ATTACK SURFACE.

TWO WHEELS.
A BIGGER ATTACK SURFACE.

09 TECHNICAL BACKGROUND

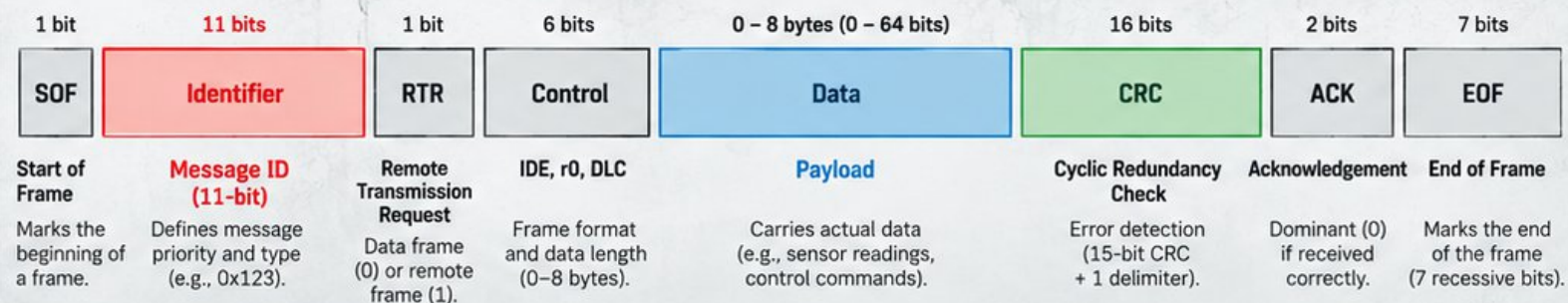
WHAT IS A CAN FRAME?

THE BUILDING BLOCK OF VEHICLE COMMUNICATION

Communication over the CAN bus is done via CAN frames. A standard CAN 2.0A frame uses an 11-bit identifier, which is the most common format in vehicles. The extended 29-bit identifier (CAN 2.0B) is identical except for the longer ID and is less commonly used in scooters.

The **CAN ID** and **Data** fields are the most important parts as they reveal the message type and actual values being transmitted (e.g., speed, throttle, brake, etc.).

9.1 STANDARD CAN 2.0A FRAME FORMAT (11-BIT IDENTIFIER)



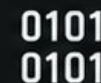
9.2 EXTENDED CAN 2.0B FRAME FORMAT (29-BIT IDENTIFIER)



KEY POINTS

**IDENTIFIER**

Determines message priority / arbitration and is used to distinguish different message types (e.g., speed, brake, throttle, diagnostics).

**DATA**

Carries payload values such as sensor readings, status information or control commands.

**NO SOURCE ADDRESS**

CAN frames do not inherently authenticate the sender. Any node on the bus can transmit a frame with a valid ID.

**BUS-WIDE VISIBILITY**

All nodes can observe frames on the shared bus, making it easier to monitor, analyze and potentially inject malicious frames.

**IMPACT IN SCOOTERS**

A single manipulated CAN frame can influence critical functions such as throttle control, braking, speed limiting or disable safety features depending on the target ECU and ID.

07 TECHNICAL BACKGROUND

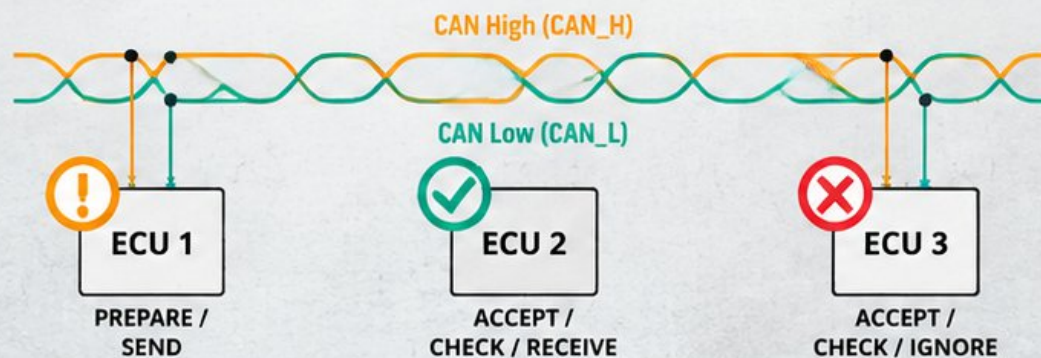
WHAT IS AN ECU?

THE CONTROL NODES INSIDE A CONNECTED SCOOTER

Electronic Control Units (ECUs) are embedded controllers responsible for specific vehicle functions such as engine/motor control, braking/ABS, instrument cluster, lighting, battery management, telematics and security/immobilizer.

Multiple ECUs communicate over the CAN bus (Controller Area Network). Any ECU can prepare and broadcast a CAN frame (e.g., sensor data, control commands) and all other ECUs on the network can independently accept, process or ignore it based on the message ID and their internal logic.

7.1 CAN BUS MESSAGE FLOW

**INSTRUMENT CLUSTER**

Speed, indicators, alerts, vehicle status

**TELEMATICS ECU**

Cellular, GPS, app connectivity, remote services

**ENGINE / MOTOR ECU**

Motor/engine control, throttle, torque, ignition

**IMMOBILIZER / SECURITY**

Key validation, anti-theft, access control

**BCM / LIGHTING**

Lights, indicators, body control functions

**ABS / BRAKE ECU**

Braking control, wheel speed, safety

**BMS / POWER CONTROL**

Battery management, power distribution

7.2

WHY IT MATTERS

Compromising an ECU or the CAN bus communication can allow an attacker to manipulate safety-critical functions (e.g., braking, throttle), disable security features, or control user-facing features (e.g., lights, instrument cluster, connectivity), leading to real-world safety, privacy and financial risks.

**KEY TAKEAWAY**

ECUs ARE THE DECISION-MAKING NODES OF THE SCOOTER. THE CAN BUS CONNECTS THEM — MAKING BUS INTEGRITY CRITICAL TO VEHICLE SECURITY.

TWO WHEELS.
A BIGGER ATTACK SURFACE.

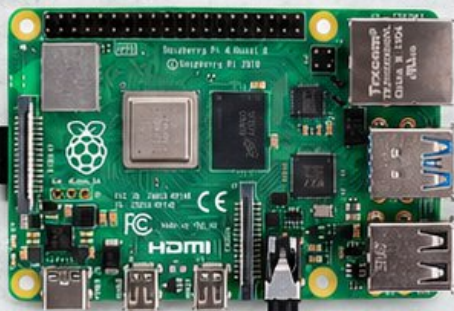
06 HARDWARE SETUP

HARDWARE IMPLANT – COMPONENTS USED

OFF-THE-SHELF COMPONENTS | REAL CAPABILITIES | REAL IMPACT

HARDWARE
RESEARCH
REAL IMPACT

01 RASPBERRY PI 4 MODEL B



IMPLANT CONTROLLER

Runs implant software, handles logic, interfaces with modular components and manages communication.

02 T-CALL V1.4 (ESP32 + SIM800L)



CELLULAR CALL/DATA INTERFACE

Provides 2G cellular connectivity (voice, SMS, data) via SIM800L with ESP32 for control and AT command handling.

03 RS485 CAN HAT



CAN BUS INTERFACE

Enables connection to the vehicle's CAN bus. Supports CAN (via MCP2515) and RS485, allowing send/receive of CAN frames.

04 WAVESHARE USB-CAN-A



CAN TRAFFIC ANALYSIS / TESTING

Used for monitoring, analyzing and testing CAN traffic during development and research. Helps in capturing and sending custom CAN frames.

05 PORTABLE POWER BANK



PORTABLE POWER SOURCE

Provides a compact and reliable power supply for the entire implant setup, enabling stealthy and independent operation.

IMPLANT ARCHITECTURE (HIGH LEVEL)

CELLULAR
(2G / GSM)

Phone Call / SMS / Data

CONTROLLER
(Raspberry Pi 4)

Process & Control Logic



CAN INTERFACE
(RS485 CAN HAT / USB-CAN-A)
Send / Receive CAN Frames



VEHICLE NETWORK
(CAN Bus)
Trigger Vehicle Functions

SAME
COMPONENTS.
DIFFERENT
PERSPECTIVE.
BIGGER IMPACT.

KEY TAKEAWAY

THE IMPLANT COMBINES OFF-THE-SHELF COMPUTING, CELLULAR CONNECTIVITY AND CAN ACCESS IN A COMPACT PLATFORM.

TWO WHEELS.
A BIGGER ATTACK SURFACE.

10 DEMO

DEMO - HARDWARE IMPLANT

REAL DEVICE | REAL INSTALLATION | REAL IMPACT

A compact hardware implant is installed inside the scooter, bridging the cellular network with the vehicle's CAN bus to enable remote control via a phone call.

**CAN INTERFACE**

RS485 CAN HAT to interface with scooter's CAN bus (CAN High / CAN Low).

**CELLULAR CONNECTIVITY**

Handles incoming calls via GSM/4G module to trigger predefined commands.

**COMPACT & STEALTHY**

Small form factor, easily concealable inside the scooter with minimal power consumption.

**DEMO OBJECTIVE**

Show how a phone call can trigger CAN commands and influence scooter functions.

**COMPONENTS USED**

- Raspberry Pi (controller)
- RS485 CAN HAT
- Cellular module (GSM/4G)
- Power and CAN connection inside scooter

**RESULT**

On receiving the phone call, the device sends crafted CAN messages to the scooter, leading to the intended action (e.g., speed change / function control).

DEMO

LET'S SEE IT IN ACTION

04 HARDWARE COMPONENT

T-CALL V1.4 ESP32 WIRELESS MODULE

ESP32 + SIM800L + CELLULAR + GPS READY (ALL IN ONE)

T-Call V1.4 is a compact development board that combines an ESP32 microcontroller with a SIM800L GSM/GPRS module, making it capable of cellular communication (calls, SMS, data) while also supporting Wi-Fi, Bluetooth and low power operation.

KEY FEATURES

**ESP32 MCU**

Wi-Fi, Bluetooth, rich I/O, low power.

**SIM800L GSM/GPRS**

Make/receive calls, send/receive SMS, GPRS data (2G).

**SIM CARD SUPPORT**

Use a standard SIM card for cellular connectivity.

**EXTERNAL ANTENNA**

Improved network coverage and signal stability.

**USB TYPE-C**

Easy programming and power supply (5V).

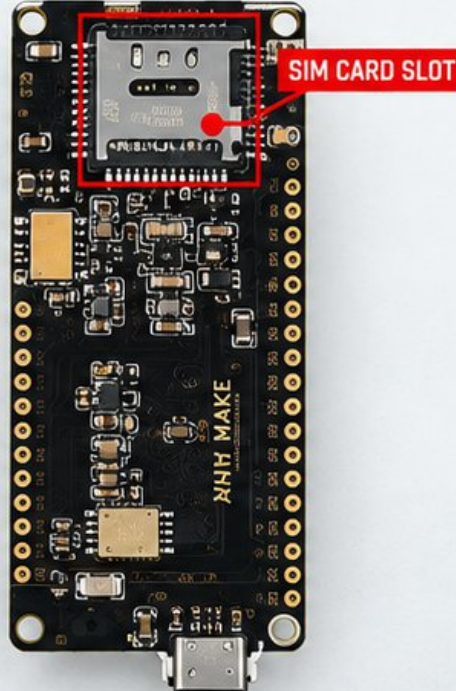
**COMPACT FORM FACTOR**

Small, low power, ideal for embedded/hidden installations.

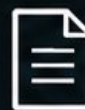
FRONT VIEW (TOP SIDE)



BACK VIEW (BOTTOM SIDE)



WHAT IS THIS MODULE?



T-Call V1.4 is an ESP32 development board with an integrated SIM800L cellular modem. It allows the device to connect to mobile networks (2G) for voice calls, SMS and data communication, along with Wi-Fi/Bluetooth capabilities of the ESP32.

WHY WE USE IT FOR THIS?



We use this module to enable remote communication with the hardware implant installed in the scooter. It allows us to receive a phone call, SMS or data command over the cellular network and trigger specific actions on the scooter via the CAN interface.

USE CASE IN OUR RESEARCH



- Receive phone call from authorized number
- Parse DTMF/SMS commands
- Send CAN messages to control scooter functions (e.g., ignition, throttle, mode change)
- Send status/telemetry back (SMS/Call)
- Works remotely over cellular network (no need for local Wi-Fi)

05 HARDWARE IMPLANT

CELLULAR IMPLANT: IN ACTION

A SMALL DEVICE. A BIG IMPACT.

A low-cost hardware implant is installed in the scooter's internal network, bridging the cellular network with the vehicle's CAN bus. When a **phone** call is received, the device executes predefined commands on the scooter.



CELLULAR CONNECTIVITY
Handles incoming calls via GSM/4G module.



CAN INTERFACE
Interfaces with scooter's CAN bus (RS485/CAN transceiver).

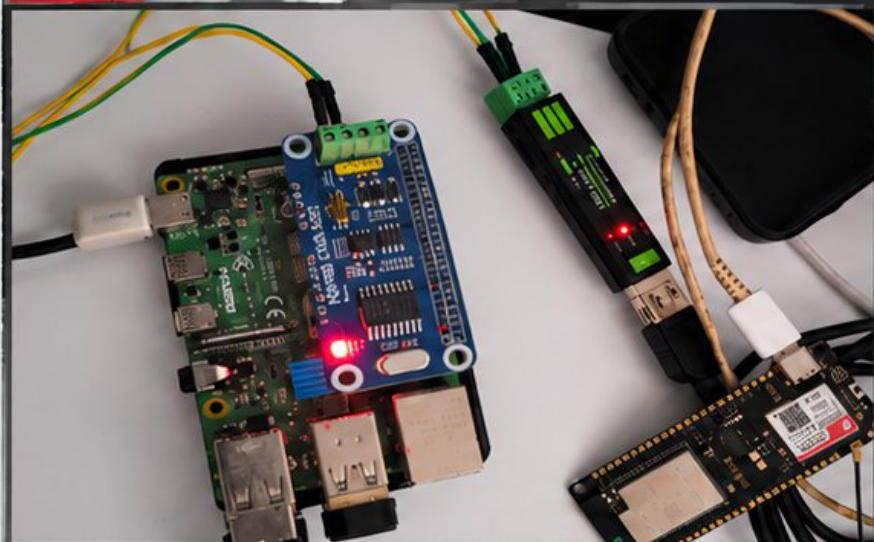


COMMAND LOGIC
Parses caller ID / input to execute predefined vehicle commands.



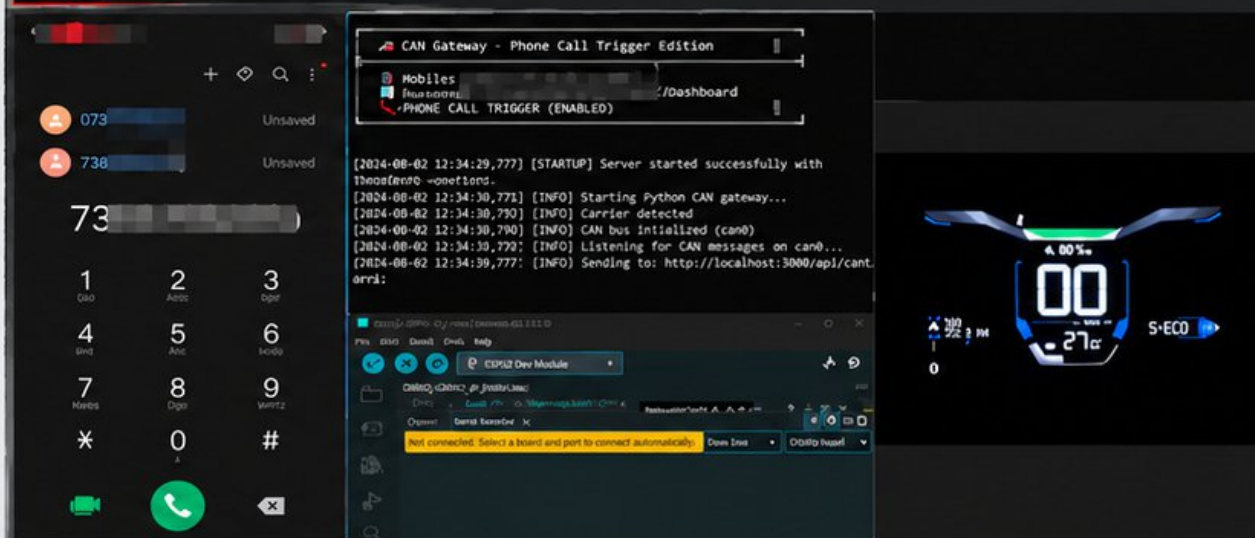
STEALTHY & LOW COST
Compact, easily concealable and low power.

5.1 HARDWARE SETUP (LAB)



Raspberry Pi + RS485 CAN HAT + ESP32 (Cellular Module)

5.3 PHONE CALL TRIGGERED CONTROL



Incoming phone call → Command parsed → CAN messages sent → Scooter responds

DEMO

LET'S SEE IT IN ACTION

06 MITIGATIONS

BREAK THE CHAIN OF CONTROL

DEFEND AGAINST CELLULAR → CAN ATTACK PATHS

The cellular implant shows how a simple phone call can lead to vehicle control. These mitigations help reduce the risk by securing each step of the attack chain.

HARDEN THE CAN BUS



- Authenticate or validate safety-critical CAN commands where architecture permits
- Implement message plausibility and freshness checks
- Monitor abnormal CAN IDs, frequency, and command sequences
- Isolate critical ECUs using secure gateways or firewalls

PROTECT PHYSICAL ACCESS



- Prevent unauthorized access to CAN wiring and diagnostic connectors
- Use tamper-evident enclosures for telematics/control modules
- Secure service ports and debug interfaces
- Detect unexpected hardware additions to vehicle networks

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

THANK YOU

FOR YOUR TIME AND SUPPORT



LET'S STAY CONNECTED