black hat BRIEFINGS

AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

E-Trojans: Ransomware, Tracking, DoS, and Data Leaks on Battery-powered Embedded Systems

M. Casagrande (KTH), D. Antonioli (EURECOM).

Marco Casagrande

- Postdoc at KTH (Sweden), Prof. Papadimitratos
  - Networked Systems Security (NSS) group
  - PhD at EURECOM (France), Dec 2024, Prof. Antonioli
- Research in Security and Privacy:
  - Proprietary protocols (fitness trackers, e-scooters, …)
  - Standard protocols (BLE, Wi-Fi, NFC, FIDO2, …)
  - Mobile (Android, …)

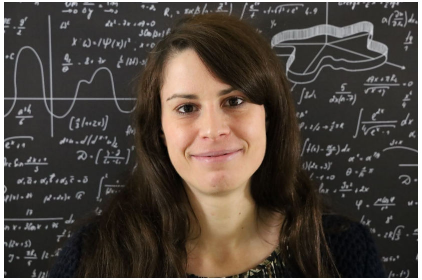
Daniele Antonioli

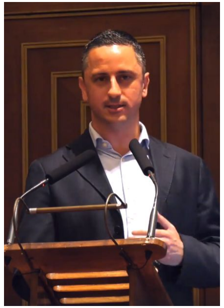
- Professor at EURECOM (France)
  - Software and System Security (S3) group
- Research **security and privacy**
  - Bluetooth (BLUFFS, BLURtooth, BIAS, KNOB, …)
  - E-Scooters (E-Spoofer, E-Trojans, …)
  - FIDO2 (CTRAPS, …)
  - Web tracking (FP-tracer, …)
  - …
- More at https://francozappa.github.io

Acknowledgments

- Co-authors from University of Padova (UniPD)
  - Riccardo Cestaro
  - Prof. Eleonora Losiouk
  - Prof. Mauro Conti

UNIVERSITÀ DEGLI STUDI DI PADOVA



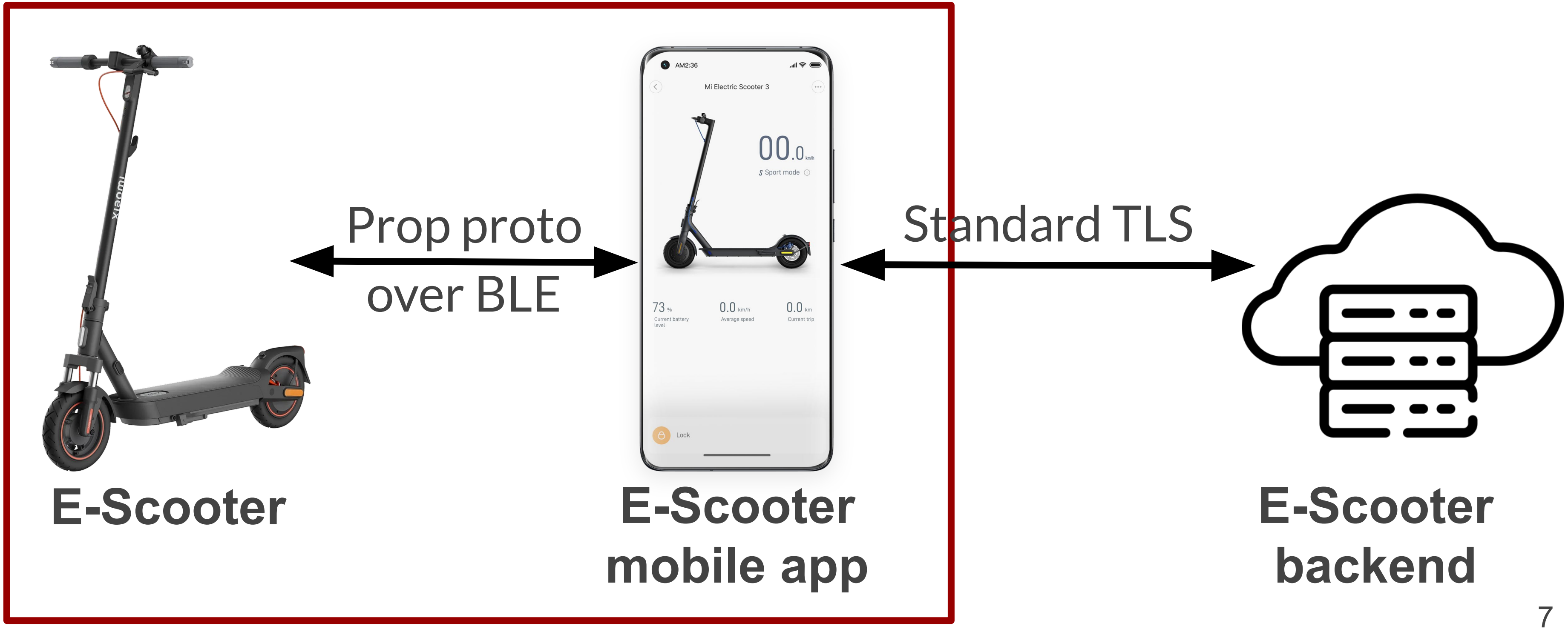


E-Trojans Talk Outline

- Introduction
- Vulnerabilities and Attacks
- Overvoltage Battery Destruction
- Undervoltage Battery Ransomware
- RE, Toolkit, and Evaluation
- Countermeasure and Disclosure

Introduction

E-Scooter Ecosystem



Prop proto over BLE

Standard TLS

E-Scooter

E-Scooter mobile app

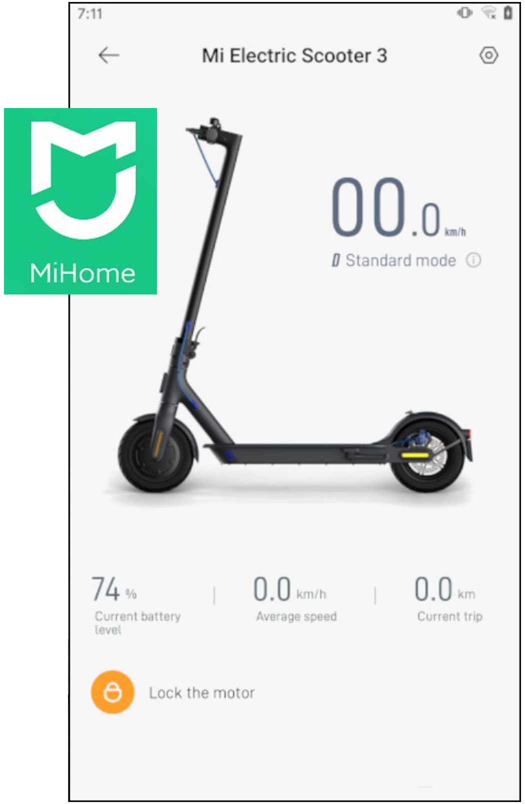
E-Scooter backend

Xiaomi E-Scooter Ecosystem

Xiaomi is a *e-scooter market leader* (personal and rental) e-scooters, including **M365** and **Mi 3**.

Mi Home mobile app to manage the e-scooter (password lock, firmware update, …).

E-scooter can be remotely attacked to compromise security, privacy, and safety.



7:11

Mi Electric Scooter 3

00.0 km/h

Standard mode

74 % Current battery level

0.0 km/h Average speed

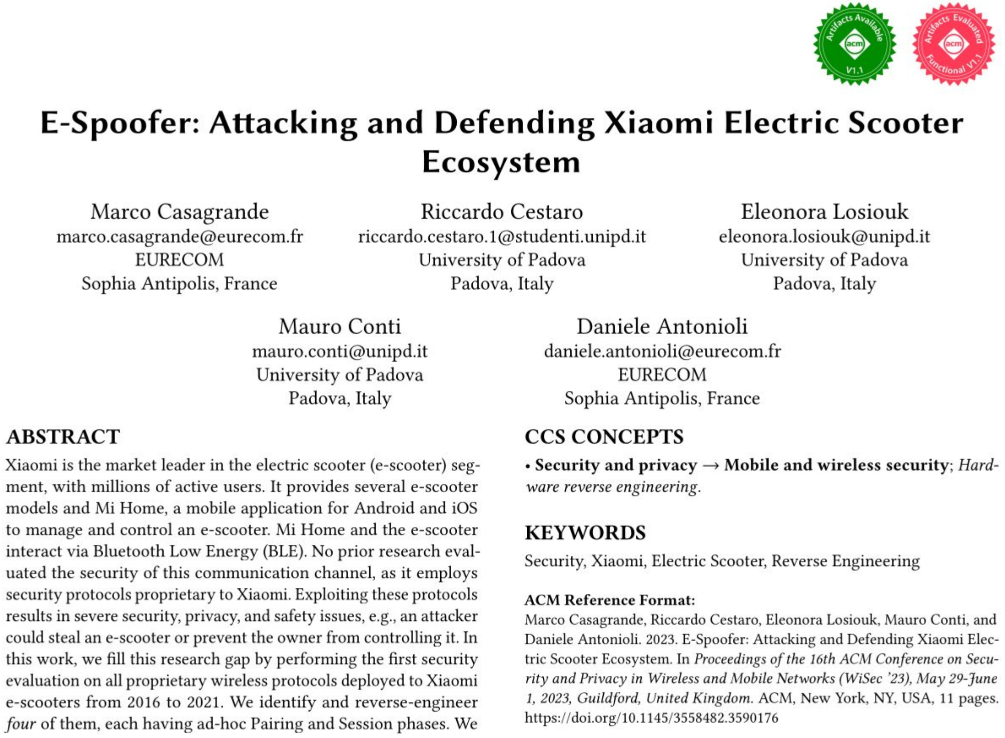
0.0 km Current trip

Lock the motor

Don’t Give me a Brake, Zimperium 2019 [ref]

Attacker remotely locks a Xiaomi M365 e-scooter via a custom wireless message.

Our Xiaomi **E-Spoofer** Attacks 2023 [ref]



E-Spoofer: Attacking and Defending Xiaomi Electric Scooter Ecosystem

Marco Casagrande
marco.casagrande@eurecom.fr
EURECOM
Sophia Antipolis, France

Riccardo Cestaro
riccardo.cestaro.1@studenti.unipd.it
University of Padova
Padova, Italy

Eleonora Losiouk
eleonora.losiouk@unipd.it
University of Padova
Padova, Italy

Mauro Conti
mauro.conti@unipd.it
University of Padova
Padova, Italy

Daniele Antonioli
daniele.antonioli@eurecom.fr
EURECOM
Sophia Antipolis, France

ABSTRACT

Xiaomi is the market leader in the electric scooter (e-scooter) segment, with millions of active users. It provides several e-scooter models and Mi Home, a mobile application for Android and iOS to manage and control an e-scooter. Mi Home and the e-scooter interact via Bluetooth Low Energy (BLE). No prior research evaluated the security of this communication channel, as it employs security protocols proprietary to Xiaomi. Exploiting these protocols results in severe security, privacy, and safety issues, e.g., an attacker could steal an e-scooter or prevent the owner from controlling it. In this work, we fill this research gap by performing the first security evaluation on all proprietary wireless protocols deployed to Xiaomi e-scooters from 2016 to 2021. We identify and reverse-engineer *four* of them, each having ad-hoc Pairing and Session phases. We

CCS CONCEPTS

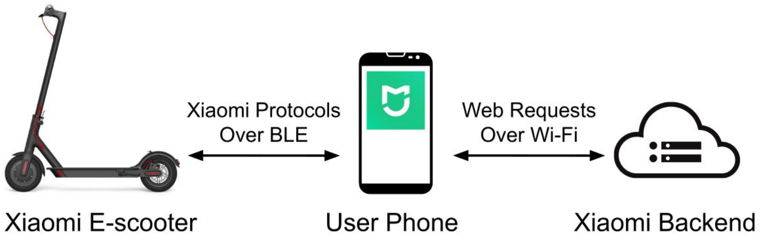
• **Security and privacy** → **Mobile and wireless security**; *Hardware reverse engineering*.

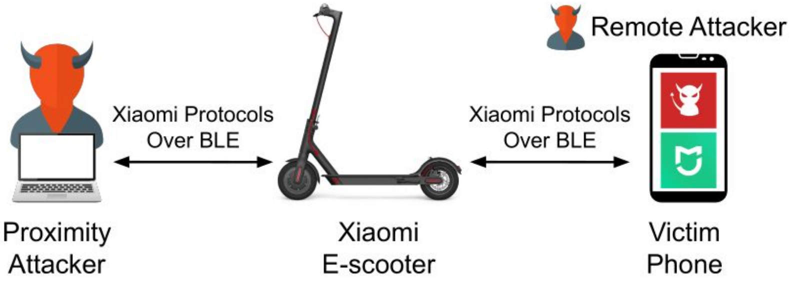
KEYWORDS

Security, Xiaomi, Electric Scooter, Reverse Engineering

ACM Reference Format:

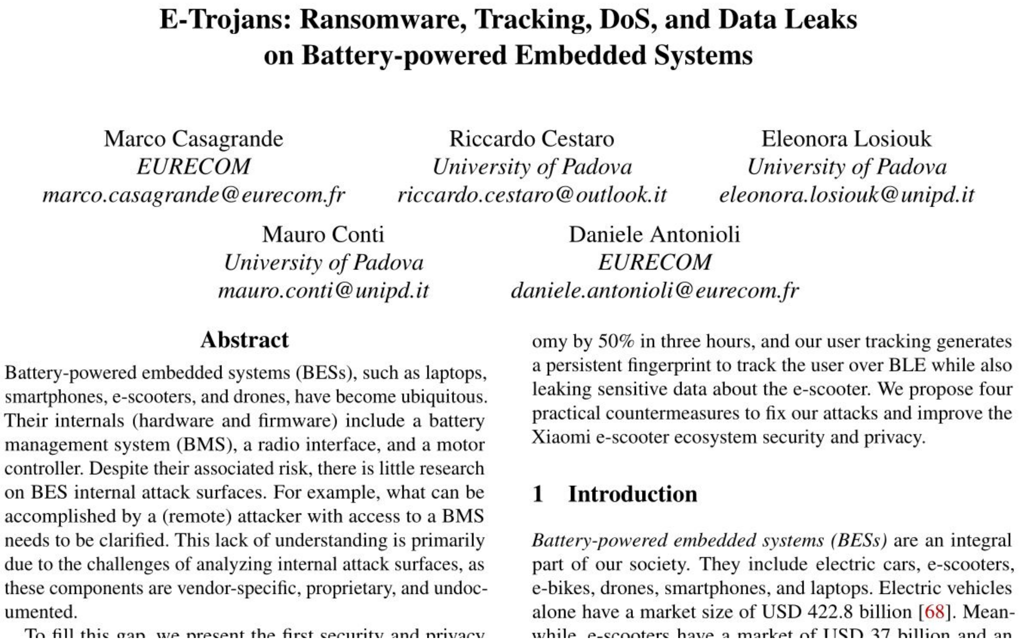
Marco Casagrande, Riccardo Cestaro, Eleonora Losiouk, Mauro Conti, and Daniele Antonioli. 2023. E-Spoofer: Attacking and Defending Xiaomi Electric Scooter Ecosystem. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23), May 29-June 1, 2023, Guildford, United Kingdom.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3558482.3590176





Our Xiaomi **E-Trojans** Attacks 2023 [ref]

ORSHIN



E-Trojans: Ransomware, Tracking, DoS, and Data Leaks on Battery-powered Embedded Systems

Marco Casagrande
EURECOM
marco.casagrande@eurecom.fr

Riccardo Cestaro
University of Padova
riccardo.cestaro@outlook.it

Eleonora Losiouk
University of Padova
eleonora.losiouk@unipd.it

Mauro Conti
University of Padova
mauro.conti@unipd.it

Daniele Antonioli
EURECOM
daniele.antonioli@eurecom.fr

Abstract

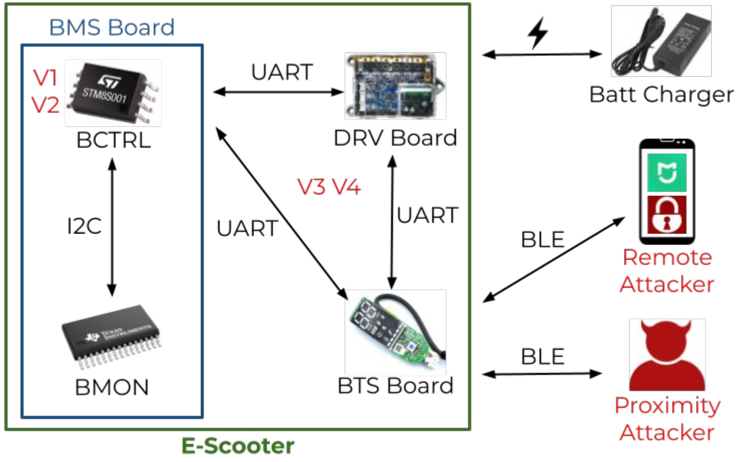
Battery-powered embedded systems (BESs), such as laptops, smartphones, e-scooters, and drones, have become ubiquitous. Their internals (hardware and firmware) include a battery management system (BMS), a radio interface, and a motor controller. Despite their associated risk, there is little research on BES internal attack surfaces. For example, what can be accomplished by a (remote) attacker with access to a BMS needs to be clarified. This lack of understanding is primarily due to the challenges of analyzing internal attack surfaces, as these components are vendor-specific, proprietary, and undocumented.

To fill this gap, we present the first security and privacy

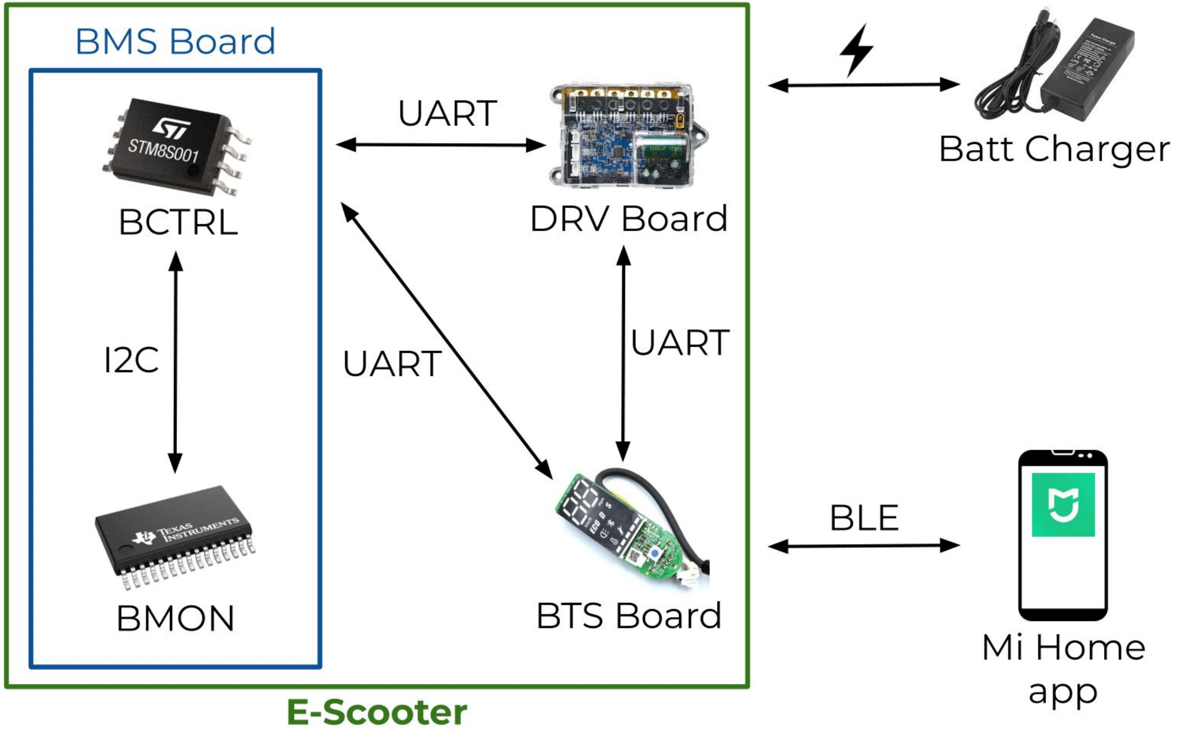
omy by 50% in three hours, and our user tracking generates a persistent fingerprint to track the user over BLE while also leaking sensitive data about the e-scooter. We propose four practical countermeasures to fix our attacks and improve the Xiaomi e-scooter ecosystem security and privacy.

1 Introduction

Battery-powered embedded systems (BESs) are an integral part of our society. They include electric cars, e-scooters, e-bikes, drones, smartphones, and laptops. Electric vehicles alone have a market size of USD 422.8 billion [68]. Meanwhile, e-scooters have a market of USD 37 billion and an



Xiaomi E-Scooter Internals Block Diagram



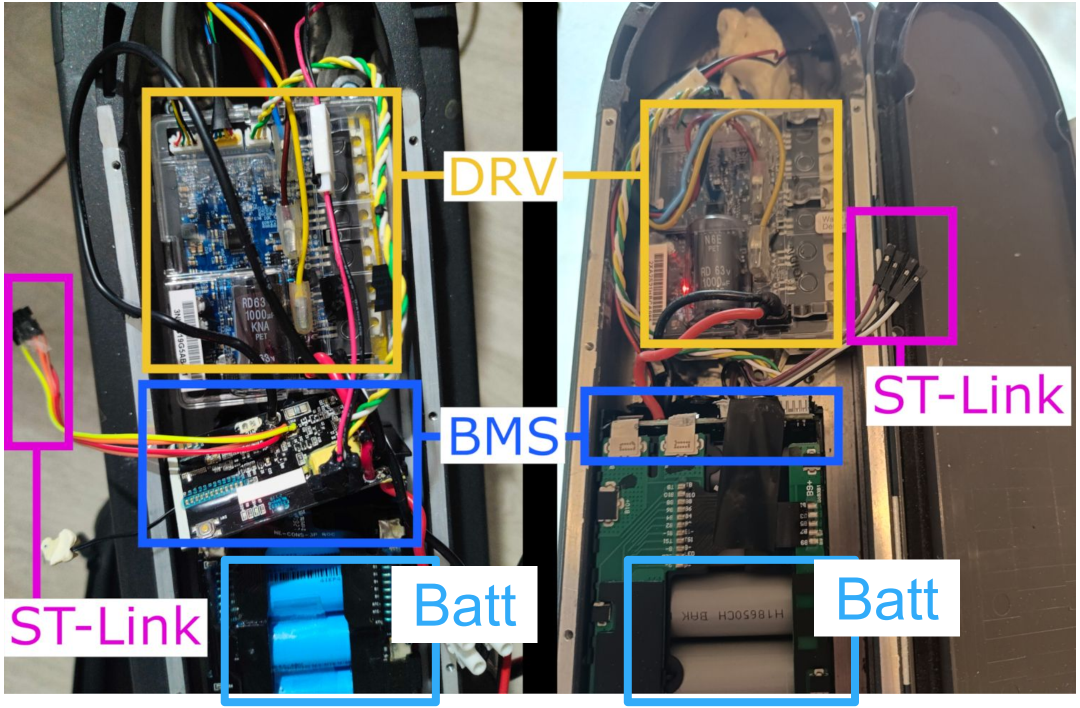
DRV: Electric motor system

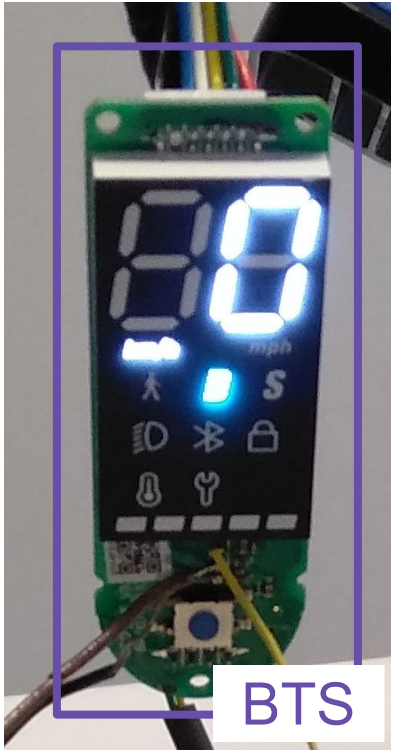
BMS: Battery management system

BTS: Bluetooth radio system for remote control

Xiaomi E-Scooter Internals Pictures

M365 ES3





Target Most Pop E-Scooters Gen in 2023 (+1M sold)

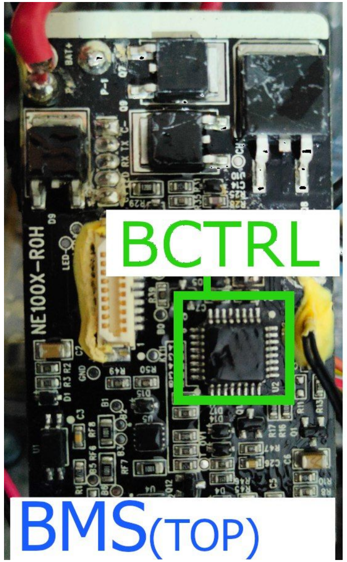
M365: 1st gen, 2016.

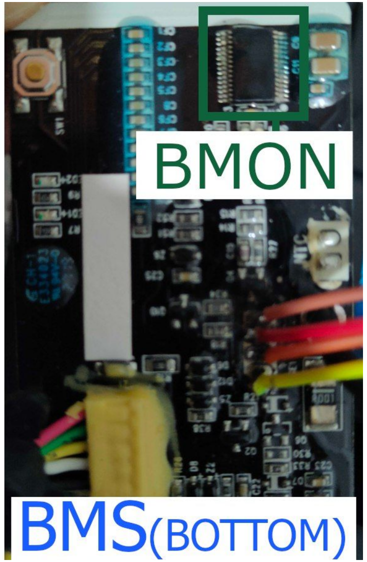
Mi 3 (ES3): 2nd gen, 2021.

Others: Pro (2018), Pro2/1S/Essential (2020).

E-Trojans target E-Scooters and Chips

- **M365**
  - BTS (Nordic nRF51822)
  - BCTRL (STMicro STM8L151K6)
  - BMON (Texas Instr. BQ76930)
- **Mi 3 (ES3)**
  - BTS (Nordic nRF51822)
  - BCTRL (STMicro STM8L151K6)
  - BMON (Texas Instr. BQ76930)



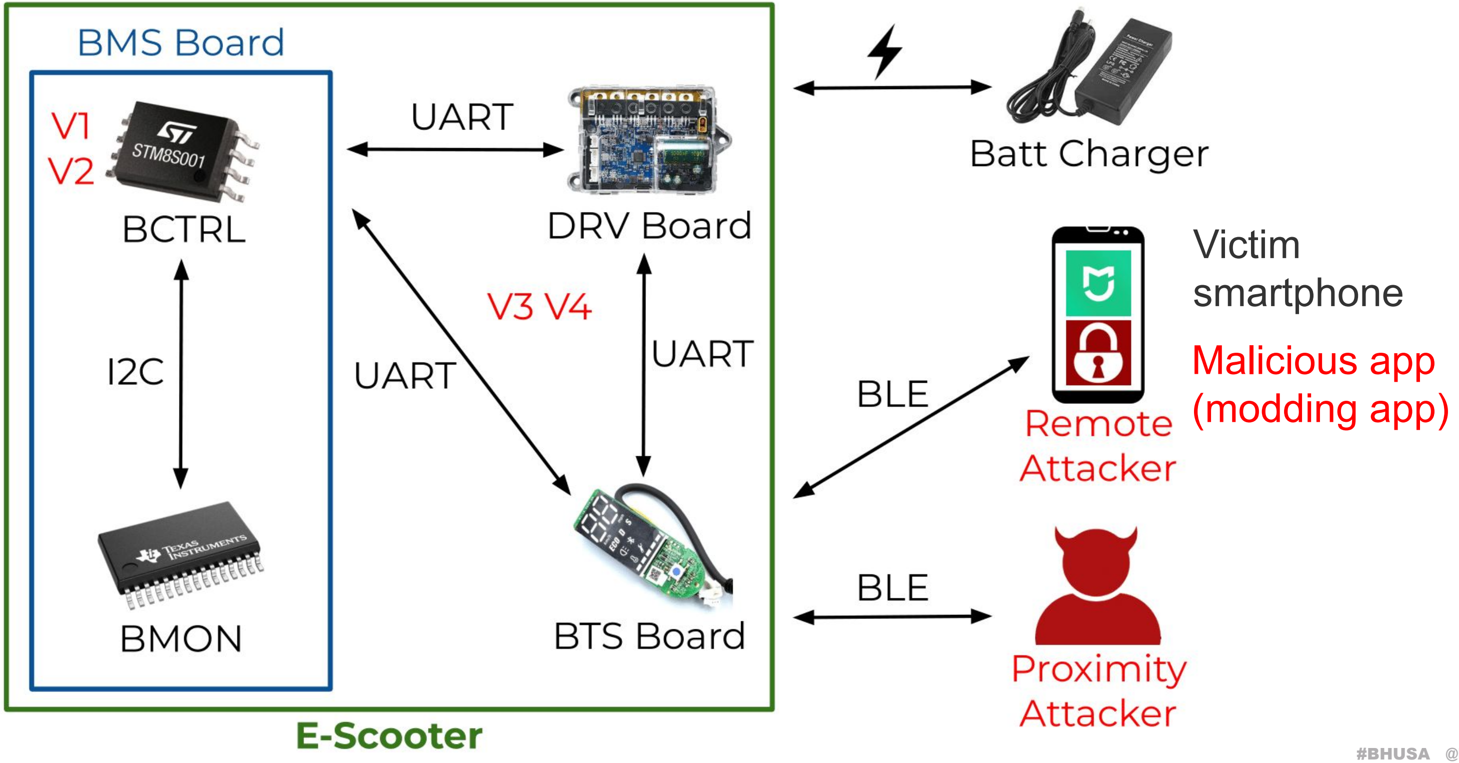


black hat BRIEFINGS

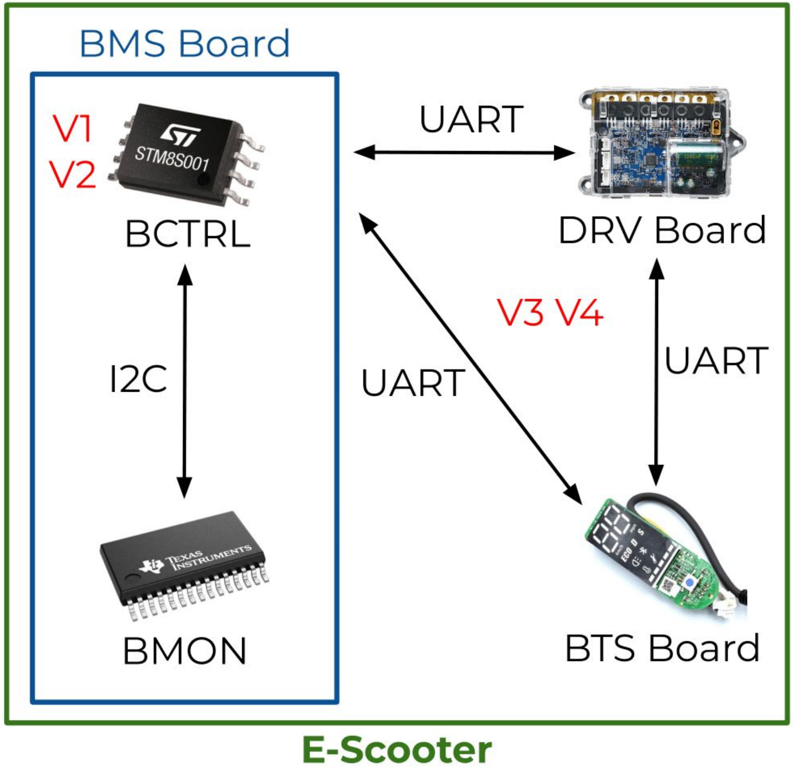
AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

E-Trojans Vulnerabilities and Attacks

Proximity and Remote Attacker Models



Four E-Trojans Vulnerabilities



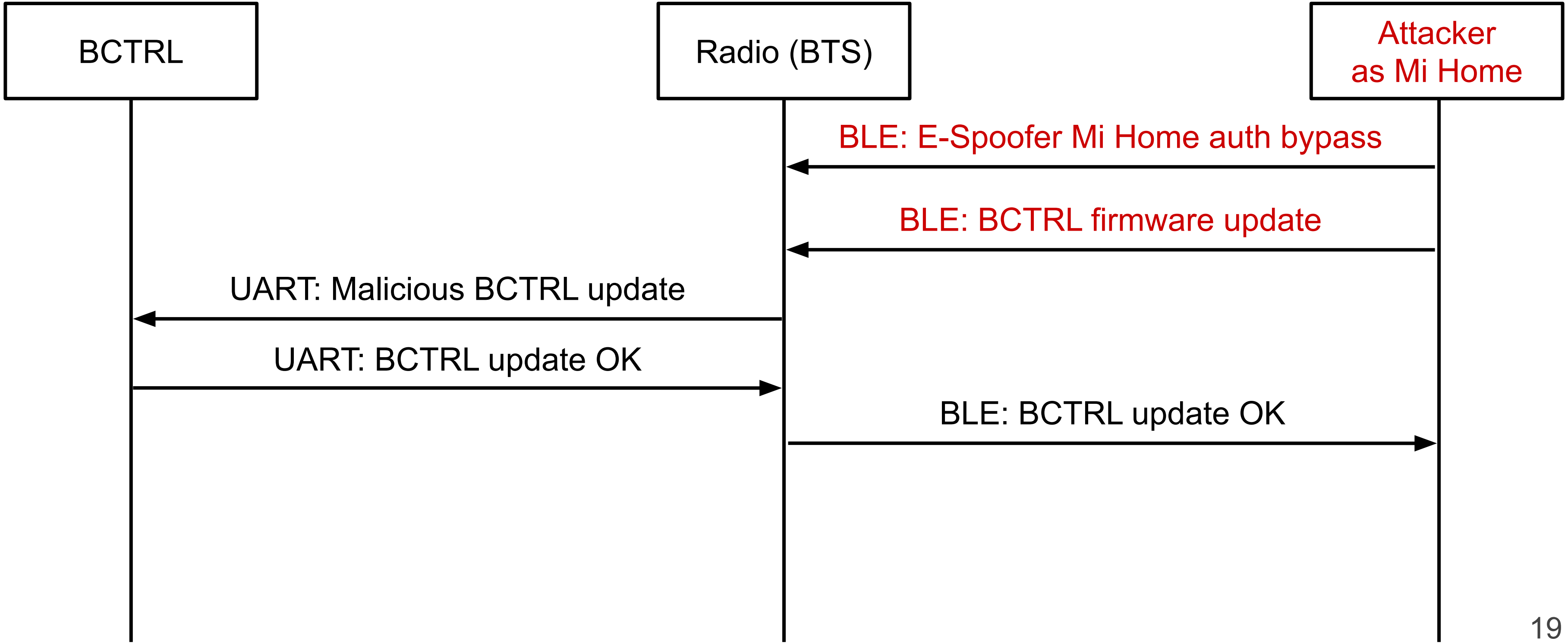
V1: Unencrypted BCTRL firmware

V2: Unsigned BCTRL firmware

V3: UART lacks integrity, encryption, and authentication

V4: UART lacks DoS protection

E-Trojans Attack Technique (E-Spoofer auth bypass)



BCTRL

Radio (BTS)

Attacker as Mi Home

BLE: E-Spoofer Mi Home auth bypass

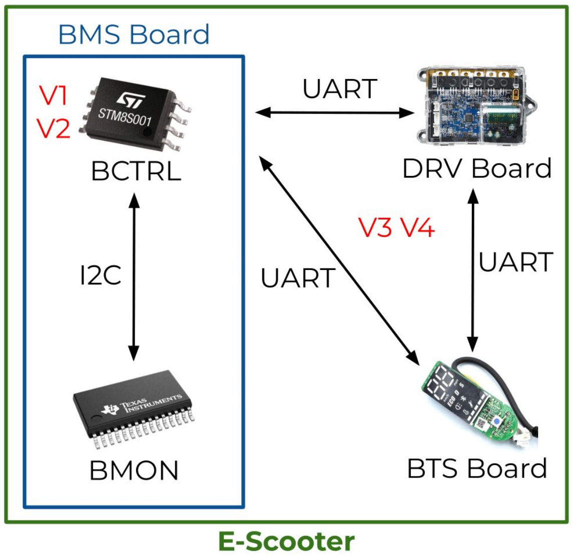
BLE: BCTRL firmware update

UART: Malicious BCTRL update

UART: BCTRL update OK

BLE: BCTRL update OK

Five E-Trojans Attacks on Xiaomi Internals



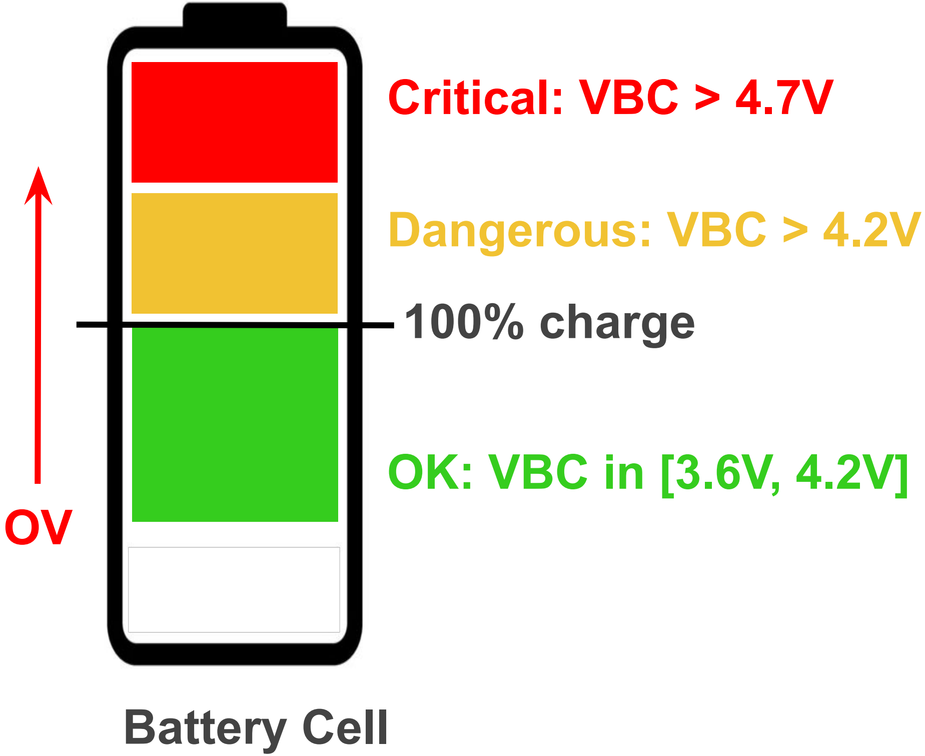
1. **UBR**: Undervoltage Battery Ransomware
2. **OBD**: Overvoltage Battery Destruction
3. **UTI**: User Tracking via Internals
4. **DES**: Denial of E-Scooter Services
5. **PLR**: Password Leak and Recover

black hat®
BRIEFINGS

AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

Overvoltage Battery Destruction (OBD)

E-Scooter Battery Overvoltage

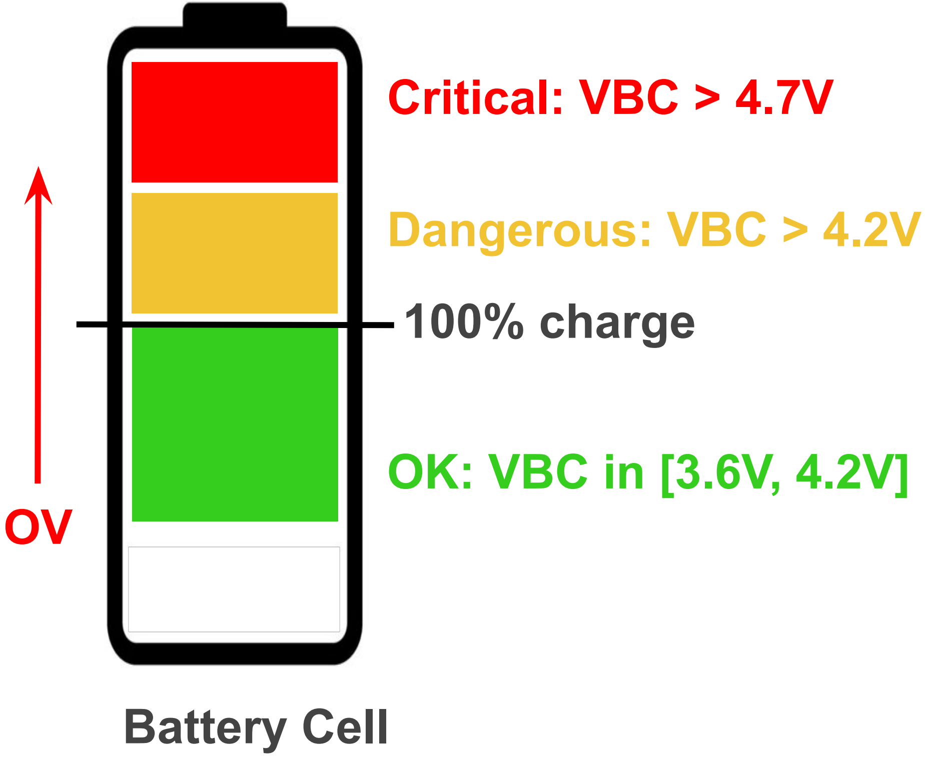


E-scooter plugged to the charger.

BCTRL stops charging when all VBC are at 4.2V (100% charge).

Battery overvoltage (voltage overflow) when a VBC > 4.2V.

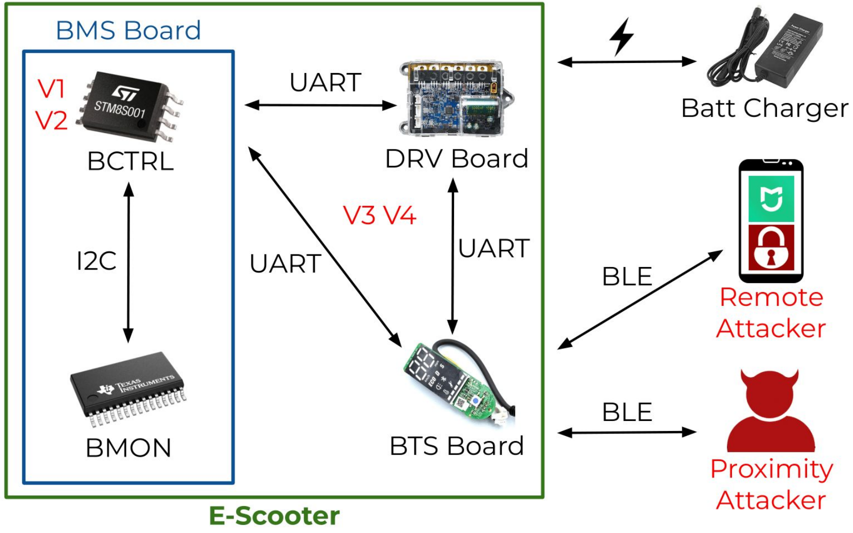
E-Scooter Battery Overvoltage Threshold



BMON has a 1 Byte OV register. When set to 0xFF, BMON sends an OV alarm if VBC > 4.7V (critical OV).

BCTRL initializes the BMON OV register and reacts to OV alarms. Eg: stop charging, load balancing.

Overvoltage Battery Destruction (**OBD**)



OBD flashes BCTRL firmware:
1) Sets BMON OV threshold to 4.7V.
2) Ignores BMON OV alarm
→ cell can overvolt (>4.2V).
3) Ignores load balancing issues
→ faster overvoltage.
4) Reports no overvoltage to BTS
→ stealthy to Mi Home and user.

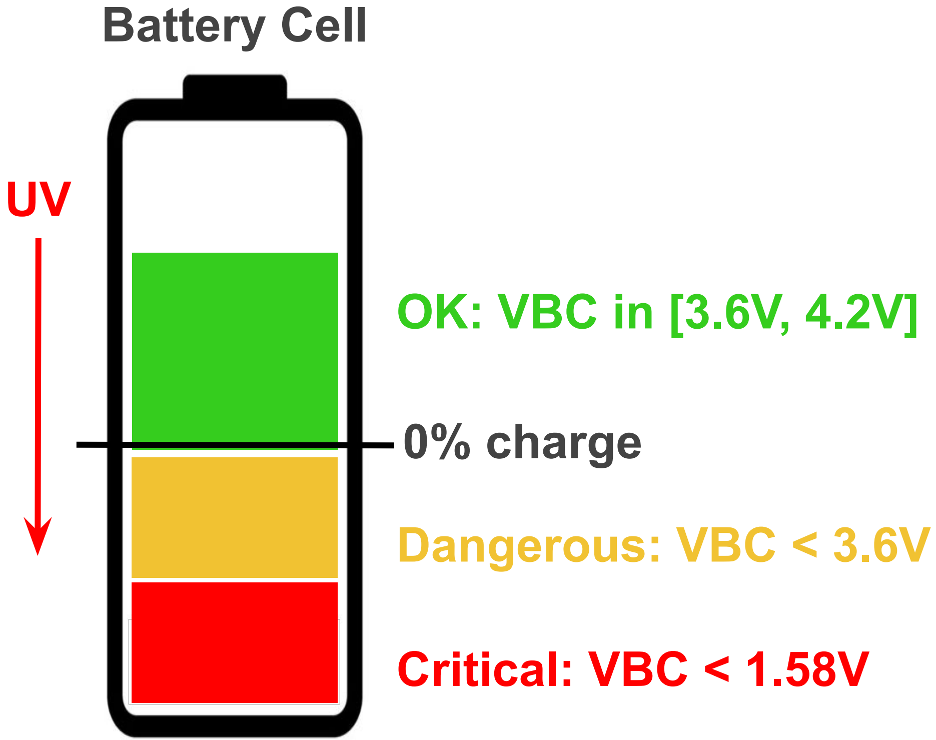
Overvoltage → battery damage, overheating, swelling, fire, explosion.

black hat BRIEFINGS

AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

Undervoltage Battery Ransomware (UBR)

E-Scooter Battery Undervoltage



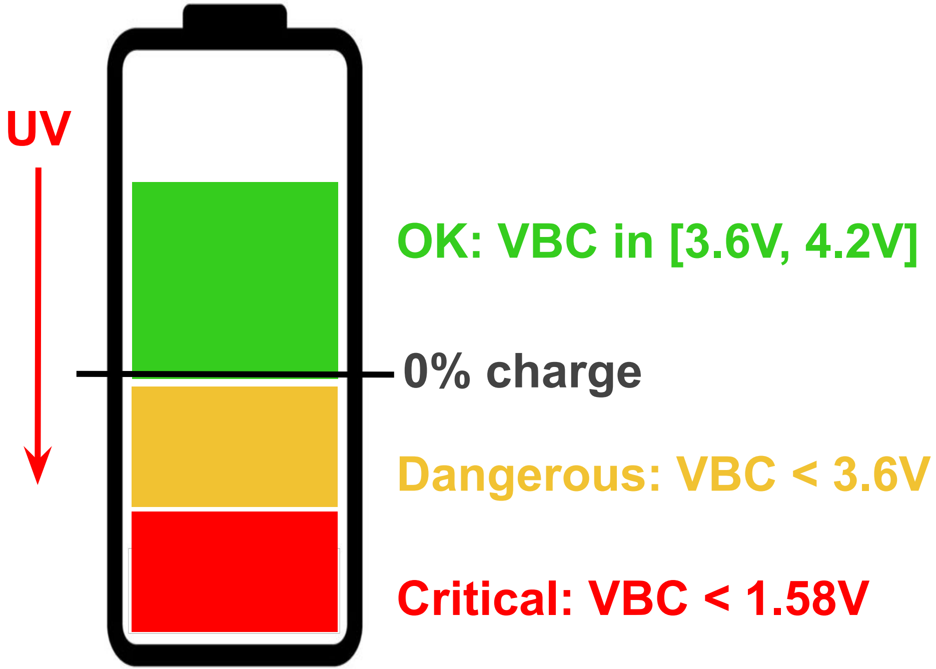
BCTRL activates sleep mode to prevent discharge when all VBC are at 3.6V (0% charge).

Battery undervoltage (voltage underflow) when a VBC < 3.6V.

E-scooter could be charging.

E-Scooter Battery Undervoltage Threshold

Battery Cell



UV

OK: VBC in [3.6V, 4.2V]

0% charge

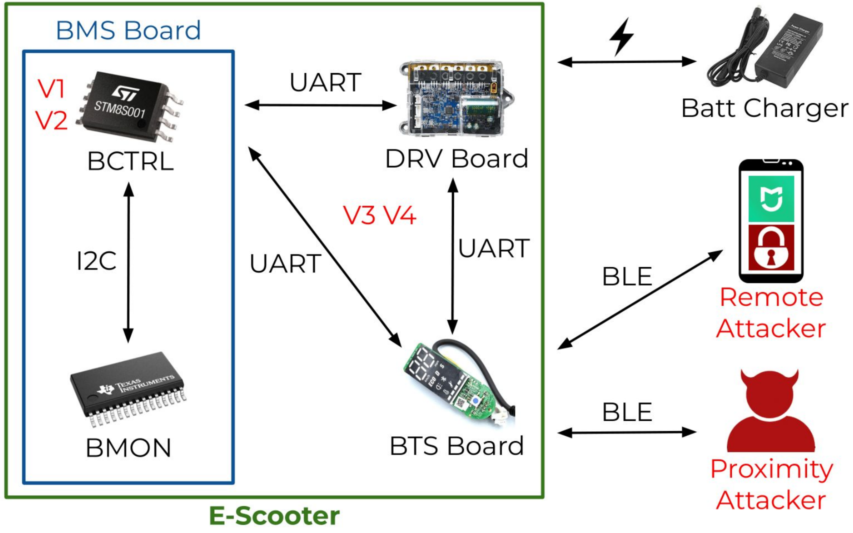
Dangerous: VBC < 3.6V

Critical: VBC < 1.58V

BMON has a 1 Byte UV register. When set to 0x00, BMON sends an UV alarm if VBC <1.58V (critical UV).

BCTRL initializes the BMON UV register and reacts UV alarms. Eg: sleep mode, load balancing.

Undervoltage Battery Ransomware (**UBR**)



UBR flashes BCTRL firmware:
1) Sets BMON UV threshold to 1.58V.
2) Ignores BMON UV alarm
→ cell can undervolt (<3.6V).
3) Ignores load balancing issues,
no charging, no sleep mode.
4) Reports no undervoltage to BTS.
5) Asks for a ransom over BLE.

Undervoltage → battery damage, gas, short circuit, polarity inversion.

black hat BRIEFINGS

AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

RE, Toolkit, and Evaluation

Reverse Engineering E-Scooters

- Months of static and dynamic RE
  - Static: firmware decompiling, disassembling, …
  - Dynamic: firmware debugging, internal traffic analysis, …
- RE of BCTRL firmware with Ghidra
  - Downloaded STM8 plugin, LE (ref)
  - Set memory map: FLASH, RAM, … (ref)
- BCTRL firmware runtime debugging
  - ST-Link, SWIM, COSMIC debugger

E-Trojans Toolkit has 3 Modules (repo)

- Binary patcher
  - Adds malicious features to BCTRL firmware via binary patching
  - Eg: ignore BMON alarms, disable charging, disable balancing, …
- Malicious BCTRL firmware
  - UBR, OBR, UTI, …
  - Flashable with a script
- UBR ransom app and backend
  - To be installed to pay the ransom
  - Backend with Django and MongoDB

E-Trojans Attack Evaluation (2024)

Attack	M365	ES3
UBR	✓	✓*
OBD	✓	✓
UTI	✓	✓
DES	✓	✓
PLR	✓	✓

*: Best undervoltage is 2.75V because of DRV.

Pro, Pro2, 1S, and Essential also vulnerable because they are affected by **V1--V4**.

black hat BRIEFINGS

AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

Countermeasures and Disclosure

E-Trojans Four Countermeasures

- We propose **4 countermeasures** (C_N fixes V_N)
  - **C_1**: Encrypt the BCTRL firmware with Xiaomi TEA
  - **C_2**: Sign and verify the BCTRL firmware with ECDSA
  - **C_3**: Protect the UART bus with SCP03
  - **C_4**: Protect the UART bus with rate limiting
- Lightweight and legacy-compliant
  - Compatible with Xiaomi TEA and ECDSA used by Xiaomi

Xiaomi Disclosure (via HackerOne)

- E-Spoofer disclosure
  - Nov 2021, informative (vulns not repro)
- E-Trojans 1st disclosure
  - Nov 2023, informative (attacks not repro)
- E-Trojans 2nd disclosure
  - June 2025, acknowledged our attacks
  - Medium CVE to be assigned, highest bounty for its category

Xiaomi Statement about E-Trojans BHUS Talk

- The M365 and ES3 (Mi3) models have reached the end of their lifecycle. For more details, please refer to our Trust Center.
- These vulnerabilities have been mitigated in all subsequent Xiaomi electric scooter models, which now incorporate enhanced security measures.

E-Trojans Sound Bytes

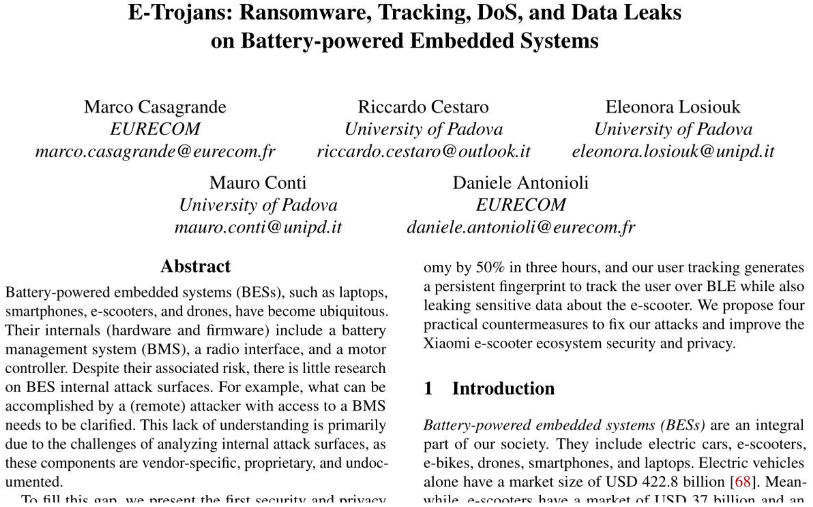
- E-scooter internals can be (remotely) attacked
  - Overvolt the battery via rogue BCTRL firmware (**OBD**)
  - Undervolt the battery via rogue BCTRL firmware (**UBR**)
- Safety, security, and privacy implications
  - Damage battery, fire, explosion, …
  - Track a user via e-scooter, …
- Security-through-obscurity is bad
- E-Trojans on other battery-powered devices?!

Grazie! Q&A

EURECOM
Sophia Antipolis

KTH VETENSKAP OCH KONST

ORSHIN



E-Trojans: Ransomware, Tracking, DoS, and Data Leaks on Battery-powered Embedded Systems

Marco Casagrande
EURECOM
marco.casagrande@eurecom.fr

Riccardo Cestaro
University of Padova
riccardo.cestaro@outlook.it

Eleonora Losiouk
University of Padova
eleonora.losiouk@unipd.it

Mauro Conti
University of Padova
mauro.conti@unipd.it

Daniele Antonioli
EURECOM
daniele.antonioli@eurecom.fr

Abstract

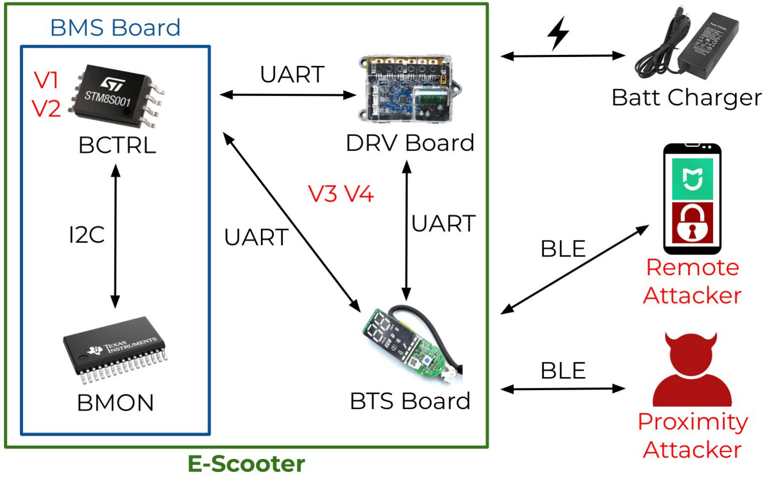
Battery-powered embedded systems (BESs), such as laptops, smartphones, e-scooters, and drones, have become ubiquitous. Their internals (hardware and firmware) include a battery management system (BMS), a radio interface, and a motor controller. Despite their associated risk, there is little research on BES internal attack surfaces. For example, what can be accomplished by a (remote) attacker with access to a BMS needs to be clarified. This lack of understanding is primarily due to the challenges of analyzing internal attack surfaces, as these components are vendor-specific, proprietary, and undocumented.

To fill this gap, we present the first security and privacy

omy by 50% in three hours, and our user tracking generates a persistent fingerprint to track the user over BLE while also leaking sensitive data about the e-scooter. We propose four practical countermeasures to fix our attacks and improve the Xiaomi e-scooter ecosystem security and privacy.

1 Introduction

Battery-powered embedded systems (BESs) are an integral part of our society. They include electric cars, e-scooters, e-bikes, drones, smartphones, and laptops. Electric vehicles alone have a market size of USD 422.8 billion [68]. Meanwhile, e-scooters have a market of USD 37 billion and an


BMS Board
V1
V2
BCTRL
I2C
BMON
UART
DRV Board
V3 V4
UART
UART
BTS Board
E-Scooter
Batt Charger
BLE
Remote Attacker
BLE
Proximity Attacker