E-Spoofer: Attacking and Defending Xiaomi Electric Scooter Ecosystem

THCon - Toulouse 2024

Speaker: Marco Casagrande (EURECOM, FR)

EURECOM
Sophia Antipolis

THCON
TOULOUSE HACKING CONVENTION

Marco Casagrande

PhD student at EURECOM (FR)

Research Topics:

- Bluetooth / Bluetooth Low Energy
- Internet-of-Things
- Android

Email: marco.casagrande@eurecom.fr

Acknowledgements

Riccardo Cestaro
Researcher at University of Padova (IT)

Eleonora Losiouk
Assistant Professor at University of Padova (IT)

Mauro Conti
Professor at University of Padova (IT)

Daniele Antonioli
Assistant Professor at EURECOM (FR)

Talk Outline

- Intro on proprietary e-scooter ecosystems
- Threat model
- Xiaomi BLE protocol vulns and attacks
- Evaluation
- E-Spoofer toolkit and (video) demos
- Countermeasures and responsible disclosure

INTRODUCTION

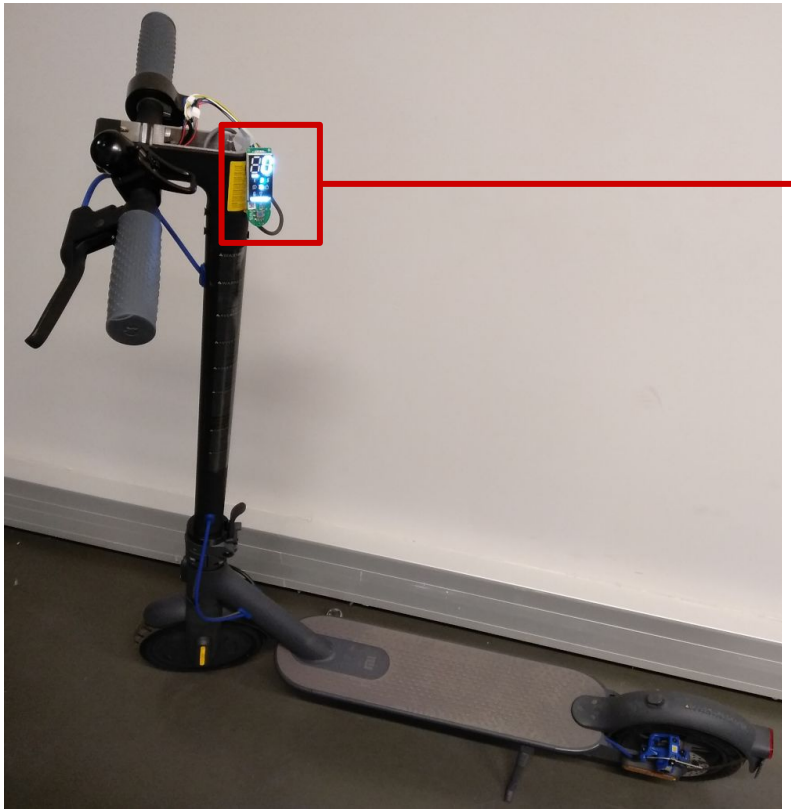
Xiaomi E-Scooter Ecosystem

- Market leader in the private e-scooter segment
  - Also owns Ninebot-Segway
- Released **seven e-scooters** between 2016-2021
  - M365, Pro 1, Pro 2, 1S, Essential, Mi 3, and Mi 4
- Maintains the **Mi Home** smartphone app to manage e-scooters

E-Scooter

- Radio subsystem (**BLE**)
  - BLE communication with Mi Home
  - Gateway to other internal subsystems
- Electric motor subsystem (**DRV**)
  - E.g., max speed and cruise control
- Battery management subsystem (**BMS**)
  - E.g., voltage and charge

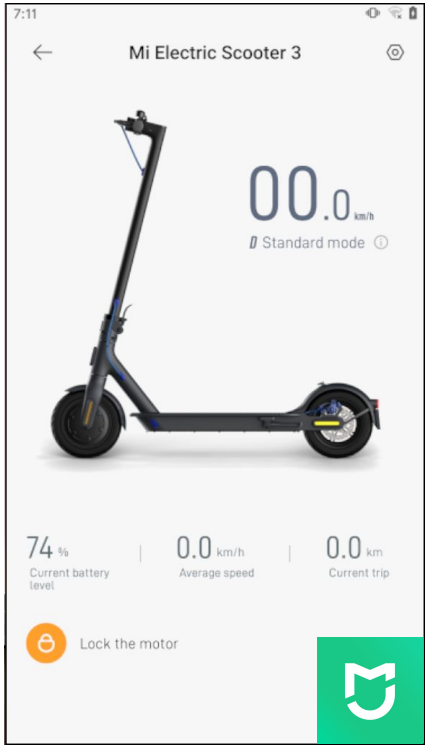
E-Scooter (2)



BLE SoC

Mi Home

- Binds e-scooter to Xiaomi account
  - I.e., pairing
- **Anti-theft software-lock**
  - Locks brakes for 6h
  - Alarm noise
- E-scooter password (optional)
  - 6-digit alphanumeric
  - Required to connect to the e-scooter



THREAT MODEL

System Model

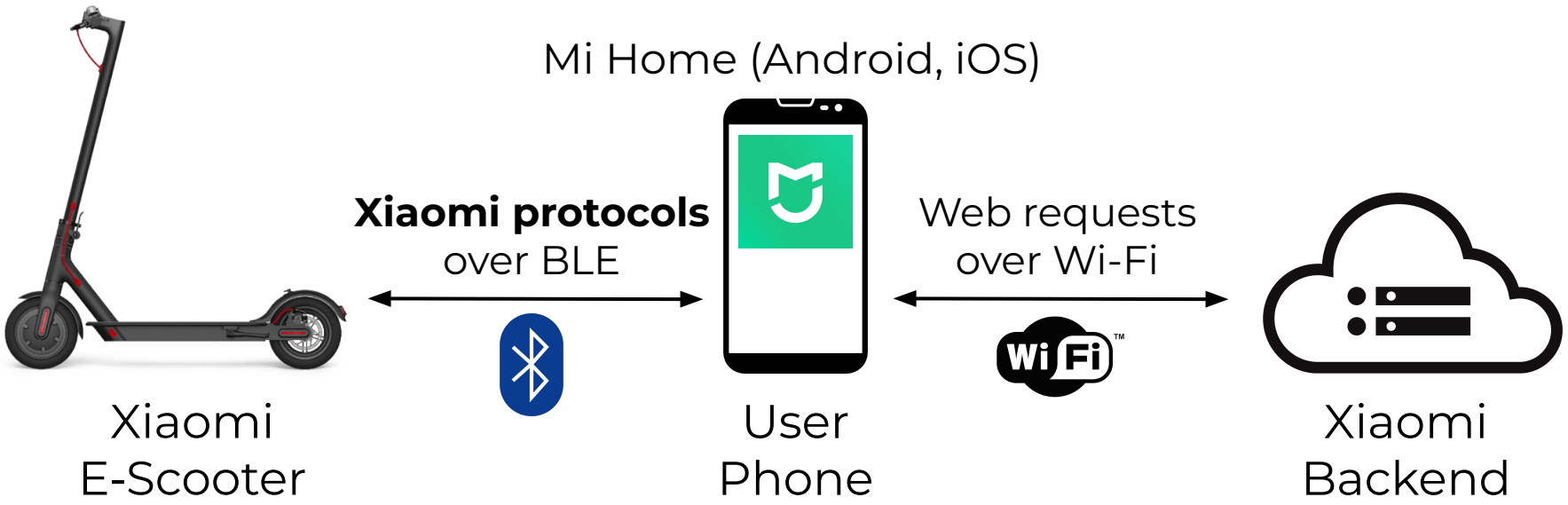
Xiaomi E-Scooter

Mi Home (Android, iOS)

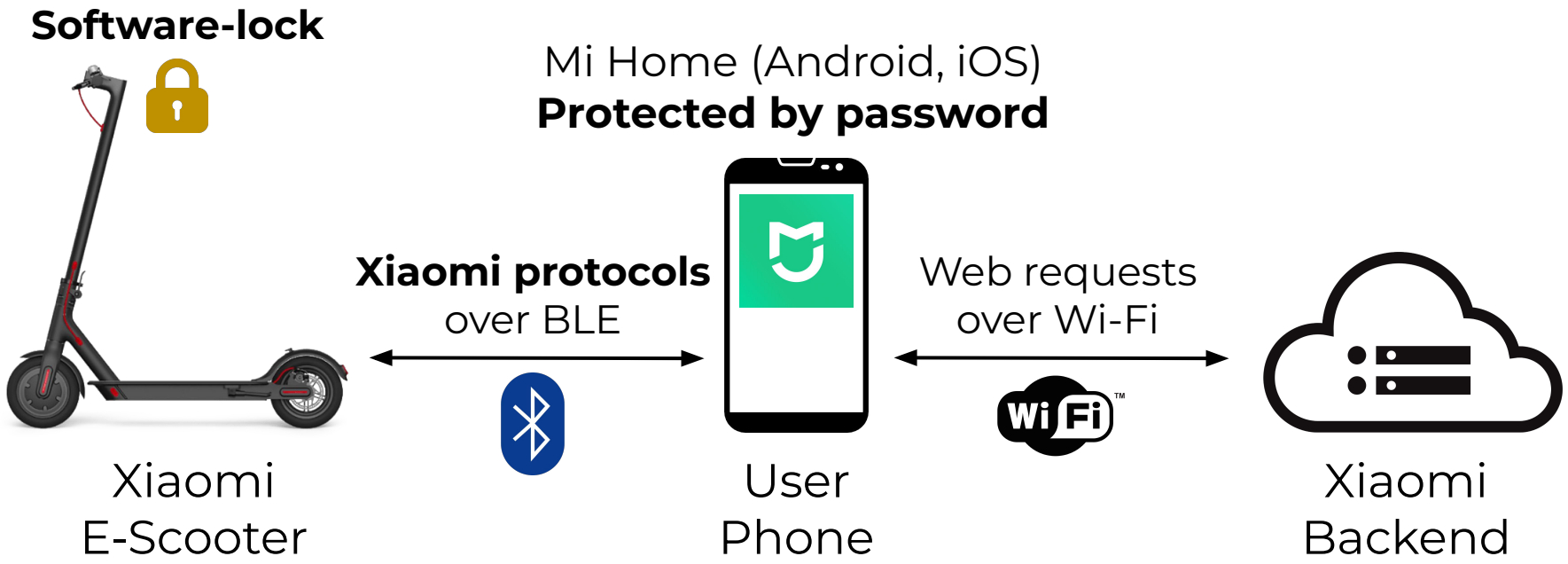
User Phone

Xiaomi Backend

System Model (2)



System Model (3)



Security Assumptions

- E-scooter and Mi Home are **securely paired**
- All firmware (BLE, DRV, BMS) is **up-to-date**
- E-scooter **password** is enabled and strong
- E-scooter is **software-locked** at all times

Proximity Attacker

Xiaomi
E-scooter

Xiaomi proprietary protocol over BLE

Proximity Attacker

Remote Attacker

Xiaomi
E-scooter

Xiaomi proprietary protocol over BLE

Remote Attacker (Android app)

User
Phone

Attacker's Goals

- **Spoof** Mi Home to the e-scooter
- Send **arbitrary and unauthorized** BLE packets
  - Without user consent or warning
  - I.e., memory read and write

SECURITY ANALYSIS OF XIAOMI PROPRIETARY PROTOCOLS

Xiaomi E-Scooter Protocol

Xiaomi
E-Scooter

Xiaomi **application-layer** proprietary protocol built on top of BLE transport

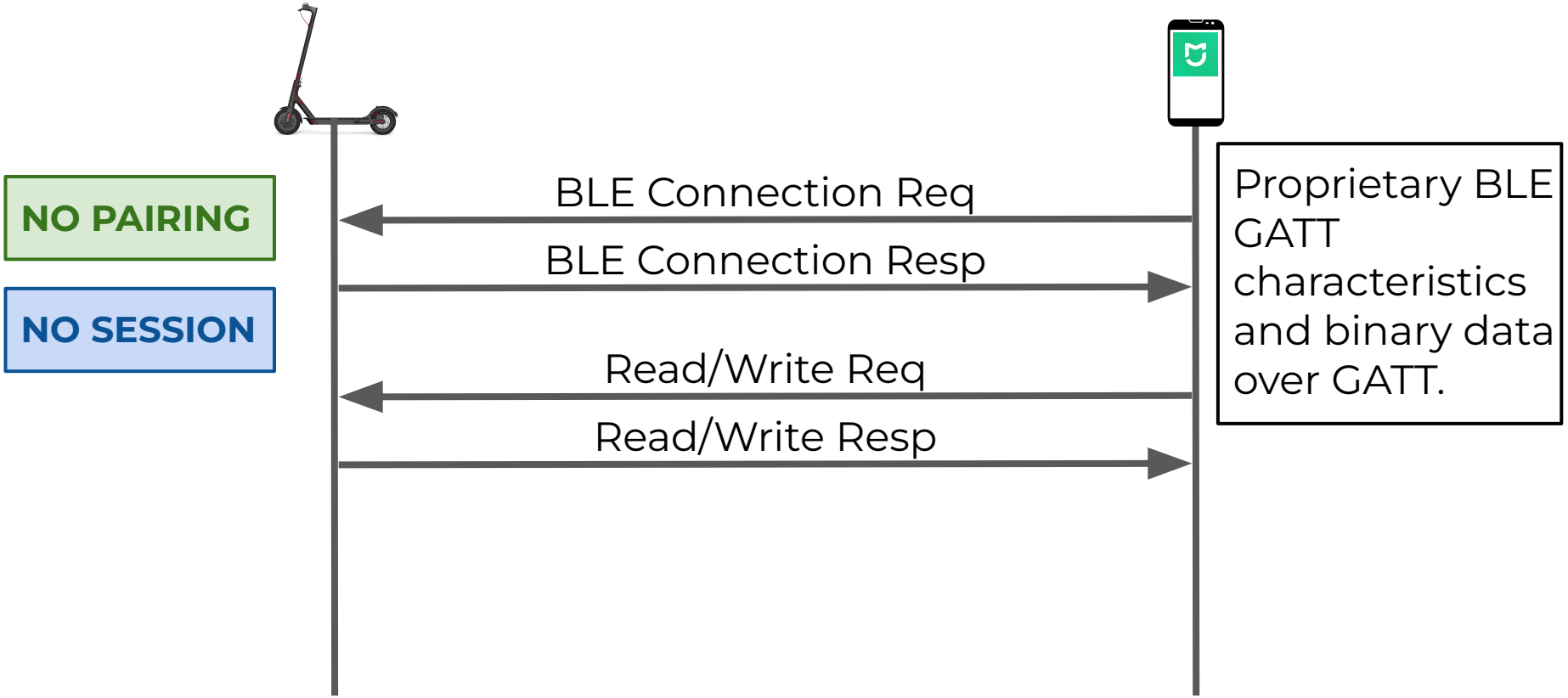
Mi Home (Android, iOS)

User
Phone

Xiaomi E-Scooter Protocols (2)

- **P1, P2, P3, P4 (since 2016)**
  - Application-layer Pairing and Session phases
  - No BLE link-layer security
- **Pairing** phase
  - Devices agree on a **Pairing Key** (**PK**)
- **Session** phase
  - Devices compute a **Session Key** (**SK**) from PK
  - Devices use SK to establish a secure channel

P1: No Security Mechanisms



P1: Proximity/Remote Attacks

NO PAIRING

NO SESSION

Spoofed BLE Connection Req

BLE Connection Resp

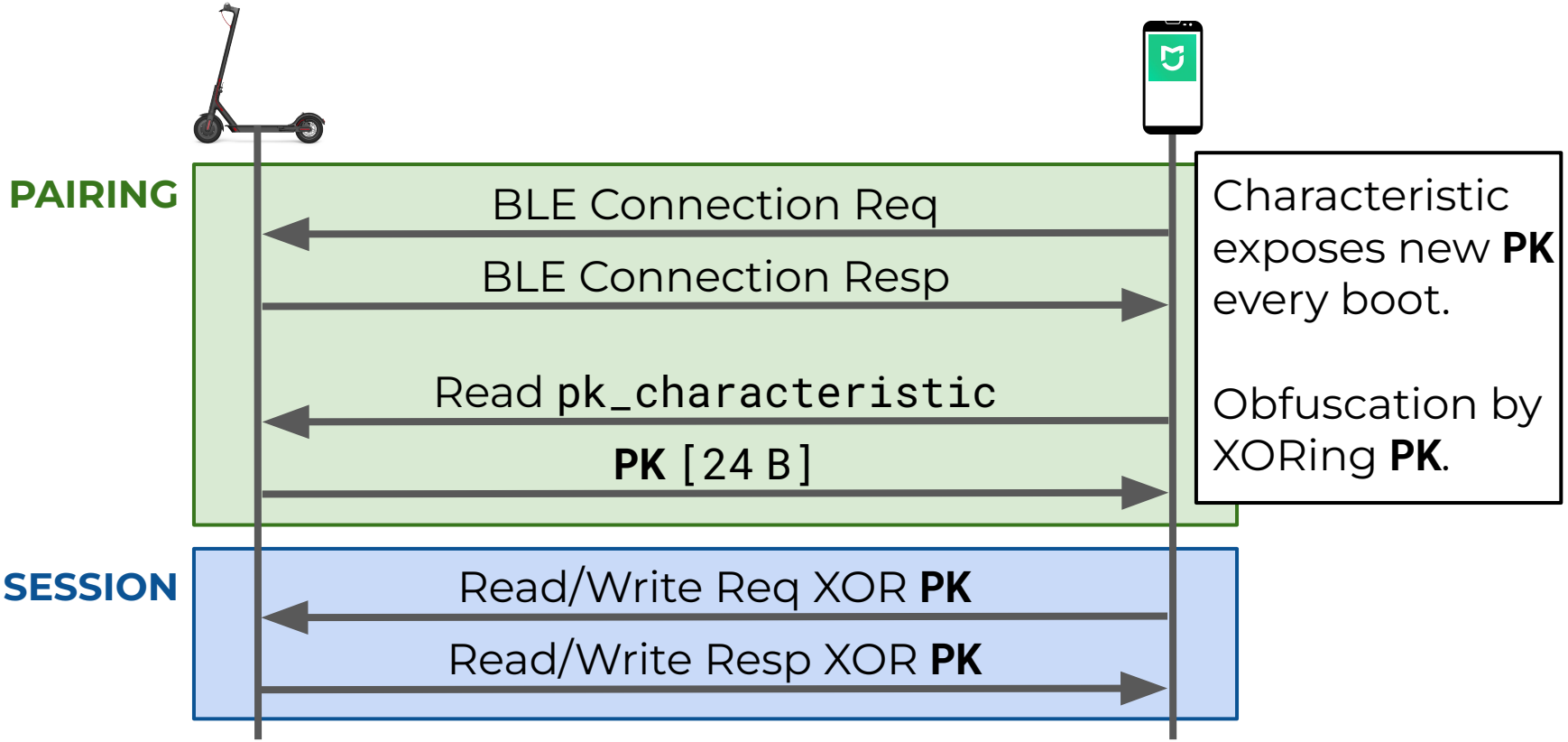
Arbitrary Read/Write Req

Read/Write Resp

Read all data:
password, mileage.

Write all data:
lock/unlock, password, max speed.

P2: Public PK and XOR Obfuscation



P2: Proximity/Remote Attacks

PAIRING

Spoofed BLE Connection Req

BLE Connection Resp

Read `pk_characteristic`

PK [24 B]

SESSION

Arbitrary Read/Write Req XOR **PK**

Read/Write Resp XOR **PK**

PK exposed **publicly**.

PK can be reversed from a BLE capture.

P2: Proximity/Remote Attacks

MALICIOUS PAIRING

Spoofed BLE Connection Req

BLE Connection Resp

Read `pk_characteristic`

PK [24 B]

SESSION

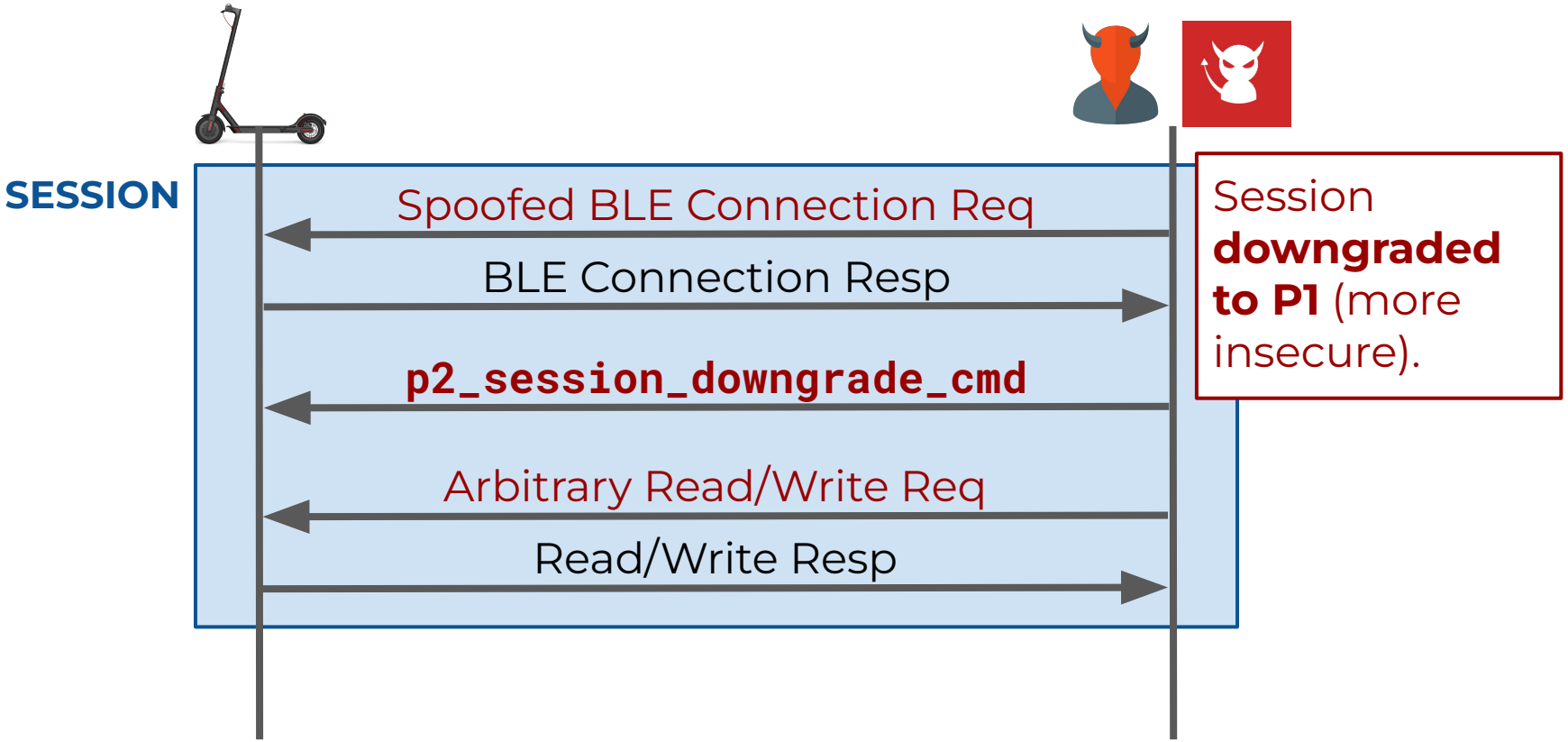
Arbitrary Read/Write Req XOR **PK**

Read/Write Resp XOR **PK**

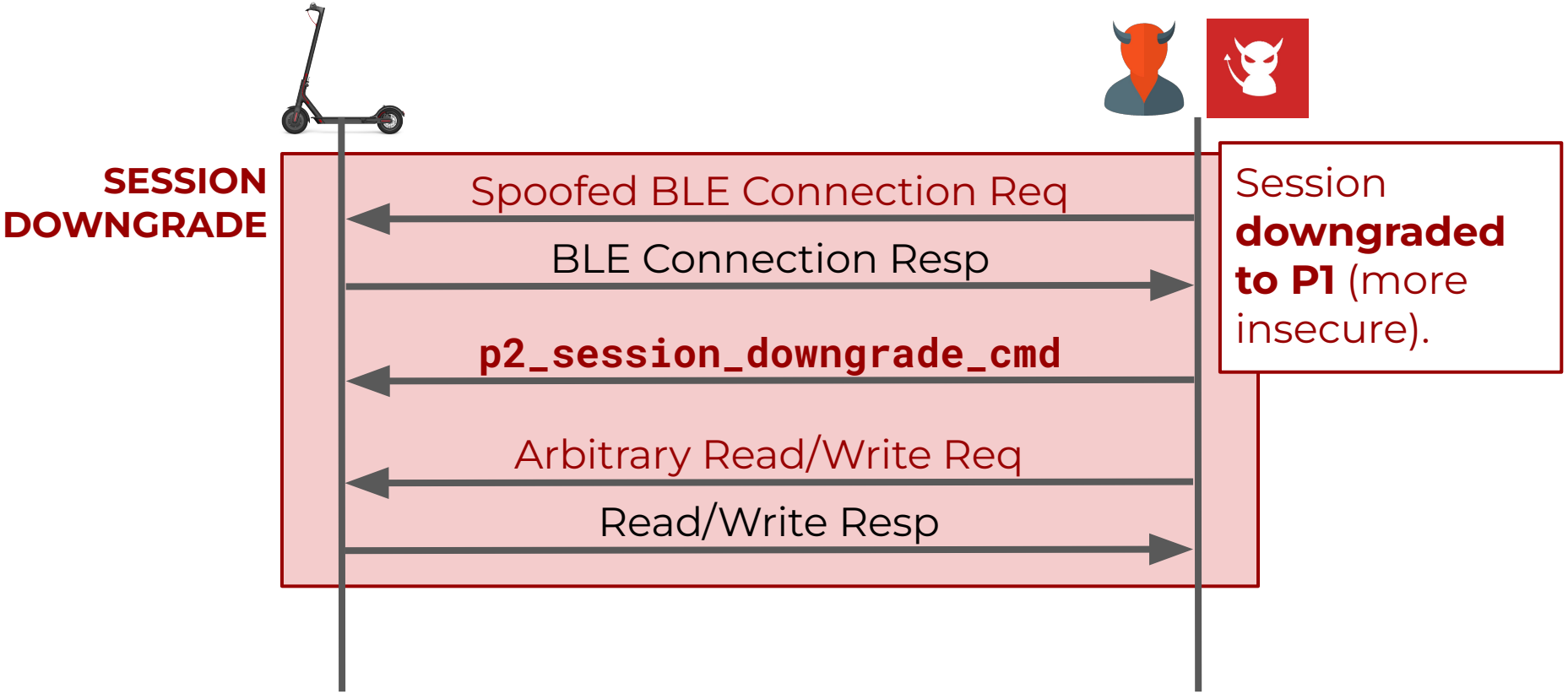
PK exposed **publicly**.

PK can be reversed from a BLE capture.

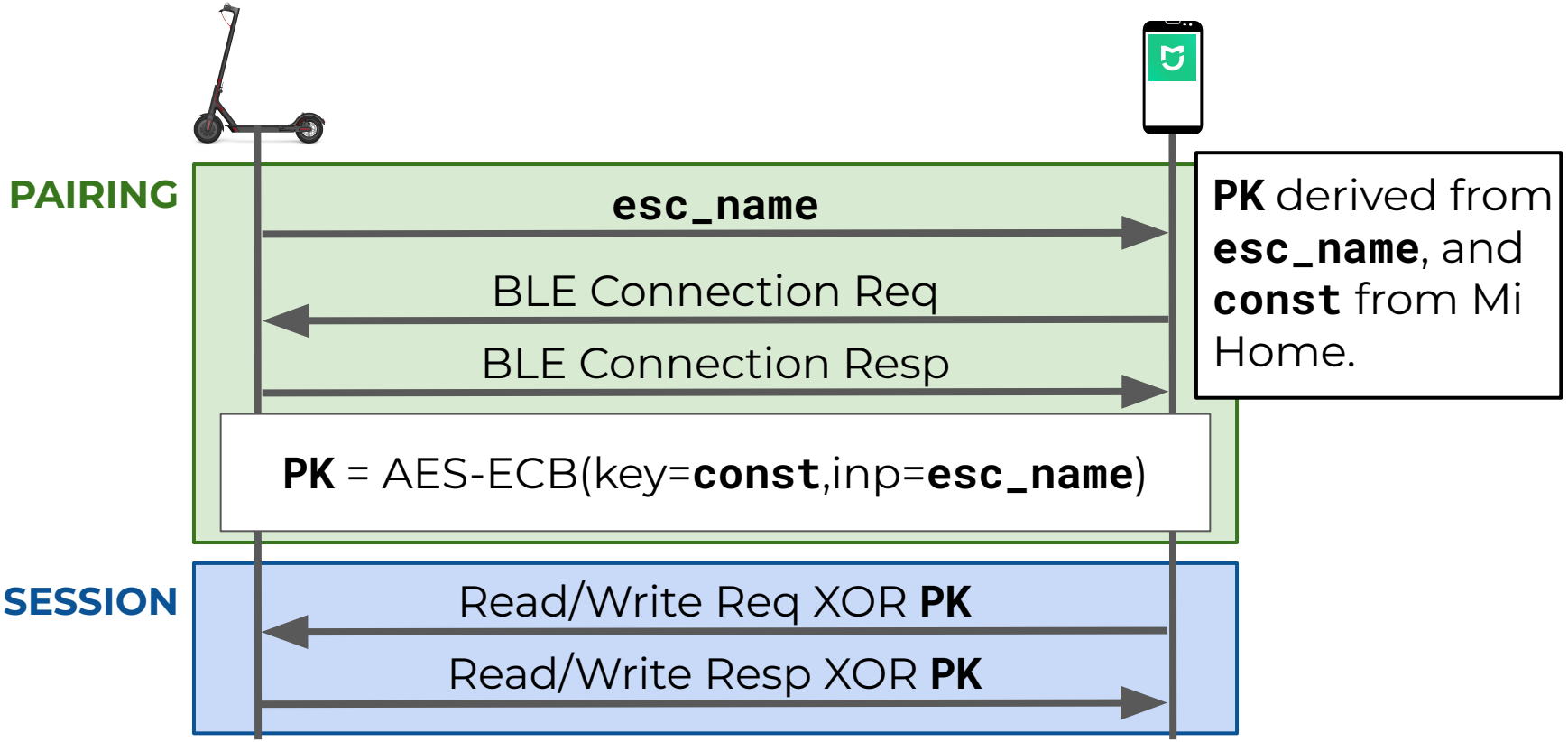
P2: Proximity/Remote Attacks



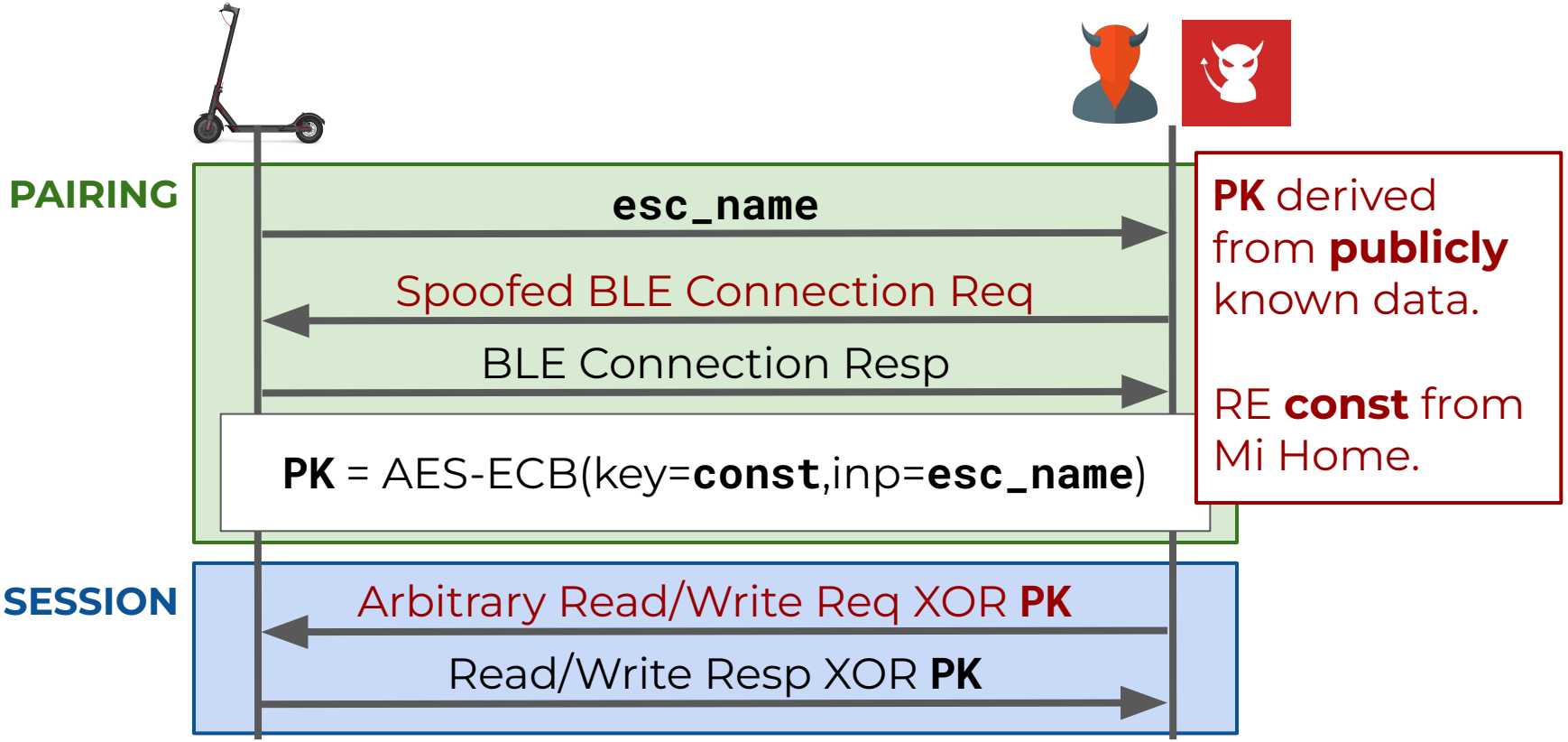
P2: Proximity/Remote Attacks



P3: Const PK and XOR Obfuscation



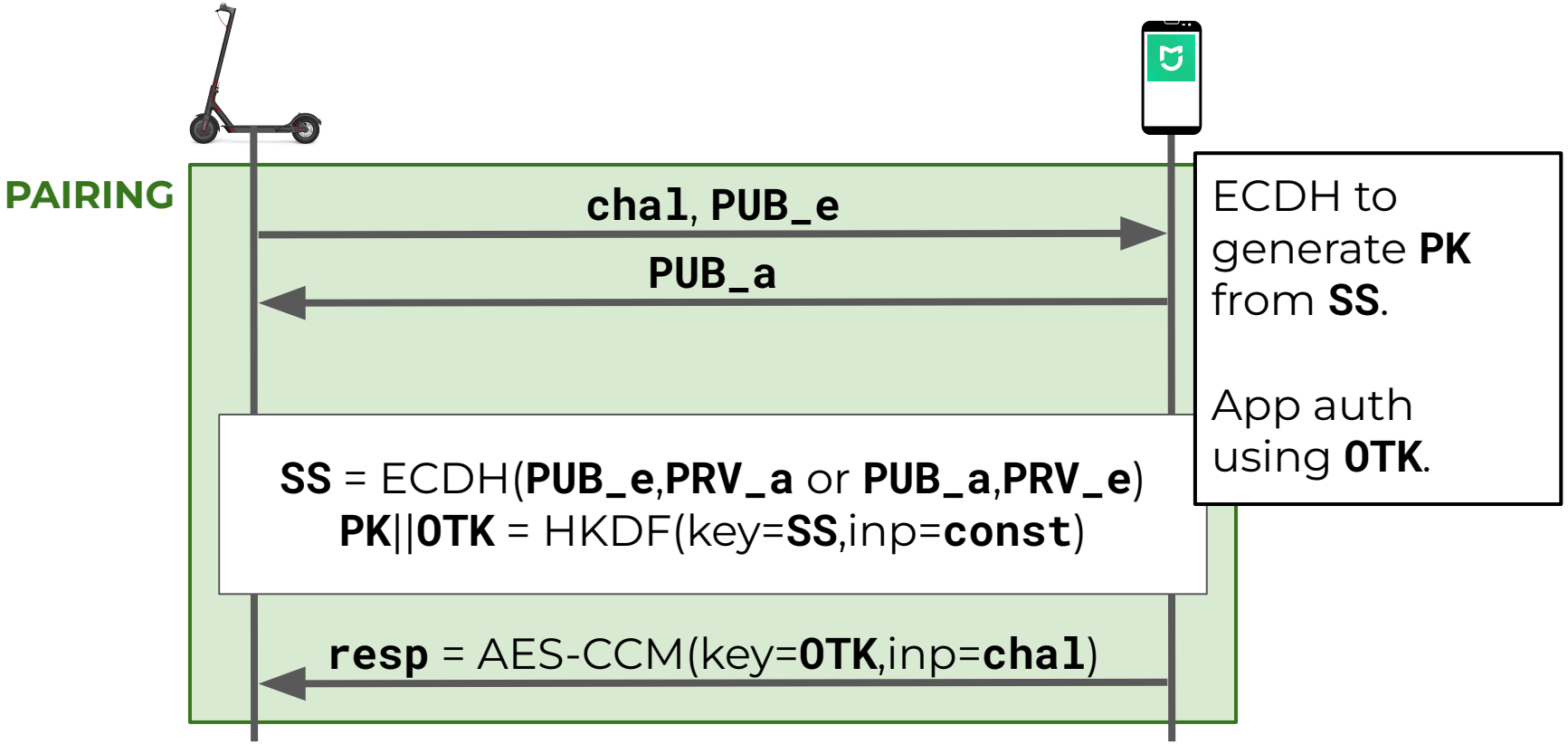
P3: Proximity/Remote Attacks



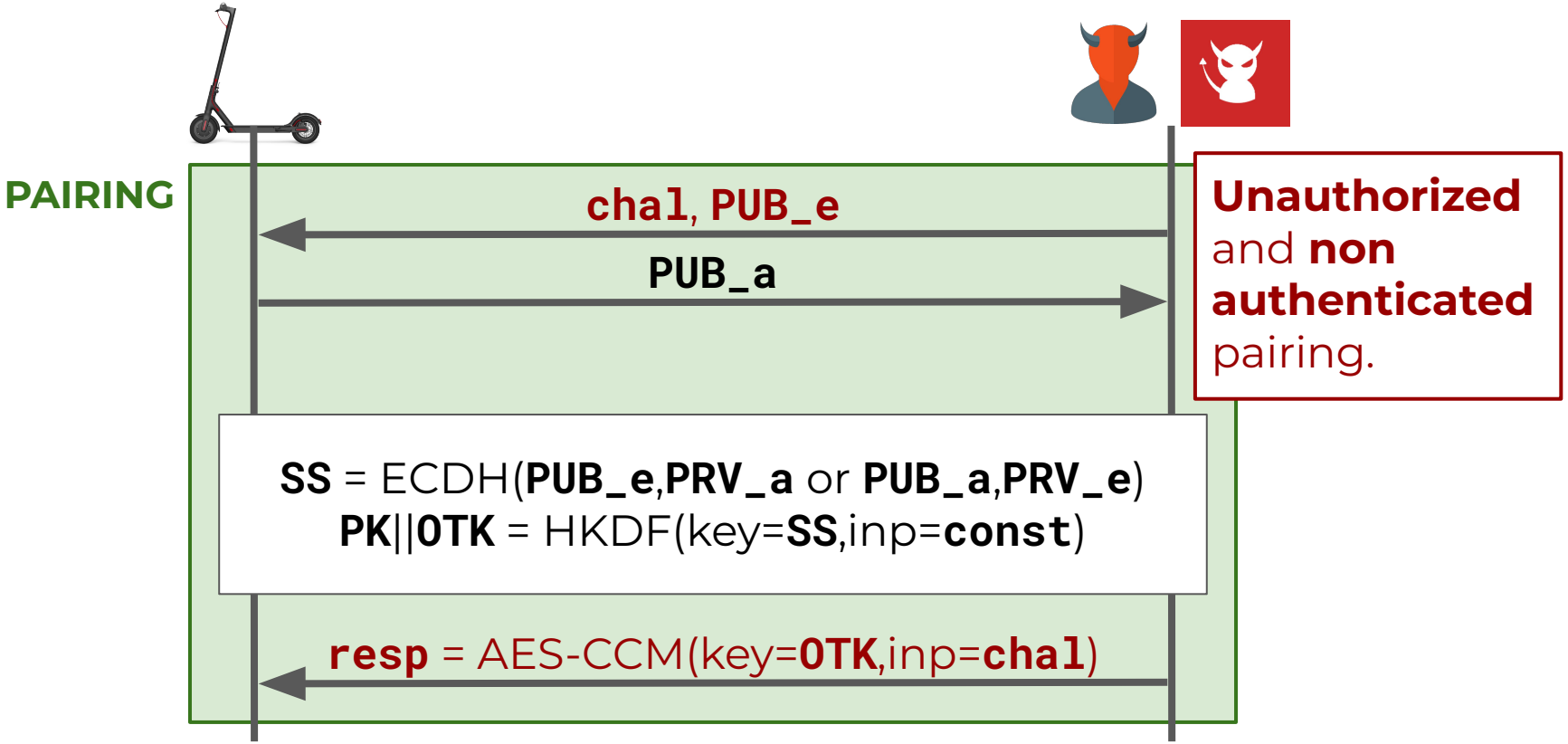
Recap: P1, P2, P3 insecurity

- **P1**, **P2**, and **P3** are **insecure by design**
  - Security through obscurity
  - E.g., XOR, public seeds, and binary data
  - Proximity/remote **impersonation is trivial**
  - Legacy protocols, only exist on non-updated devices
- **P4** to the rescue?
  - **NOT** really

P4: Pairing (ECDH, AES-CCM)



P4: Proximity/Remote Attacks



P4: Proximity/Remote Attacks

MALICIOUS PAIRING

chal, **PUB_e**

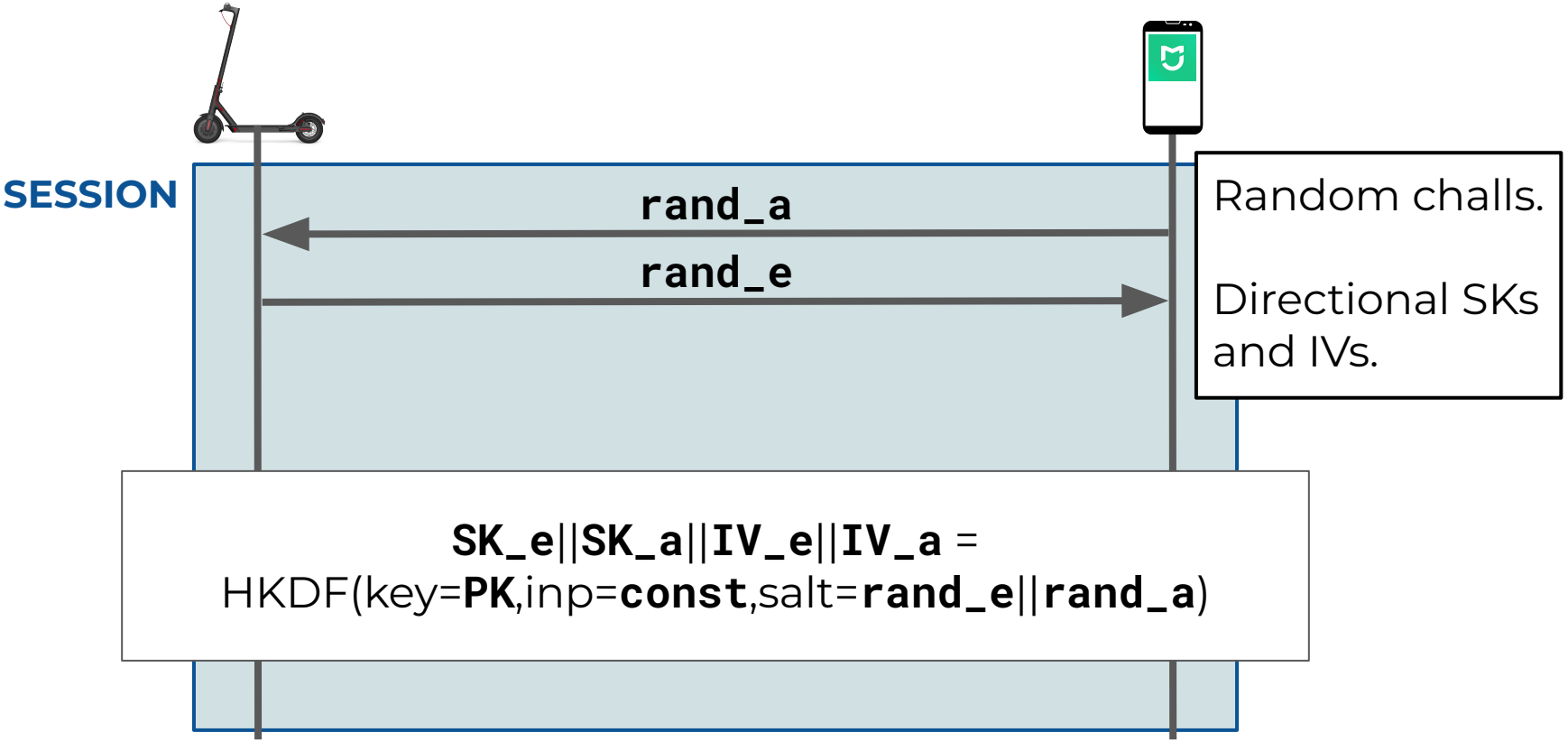
PUB_a

Unauthorized and **non authenticated** pairing.

SS = ECDH(**PUB_e**,**PRV_a** or **PUB_a**,**PRV_e**)
PK||OTK = HKDF(key=**SS**,inp=**const**)

resp = AES-CCM(key=**OTK**,inp=**chal**)

P4: Session (HKDF, AES-CCM) (1)



P4: Session (HKDF, AES-CCM) (2)

SESSION

resp_a = HKDF(key=**SK_a**,inp=**rand_a**||**rand_e**)

resp_e = HKDF(key=**SK_e**,inp=**rand_e**||**rand_a**)

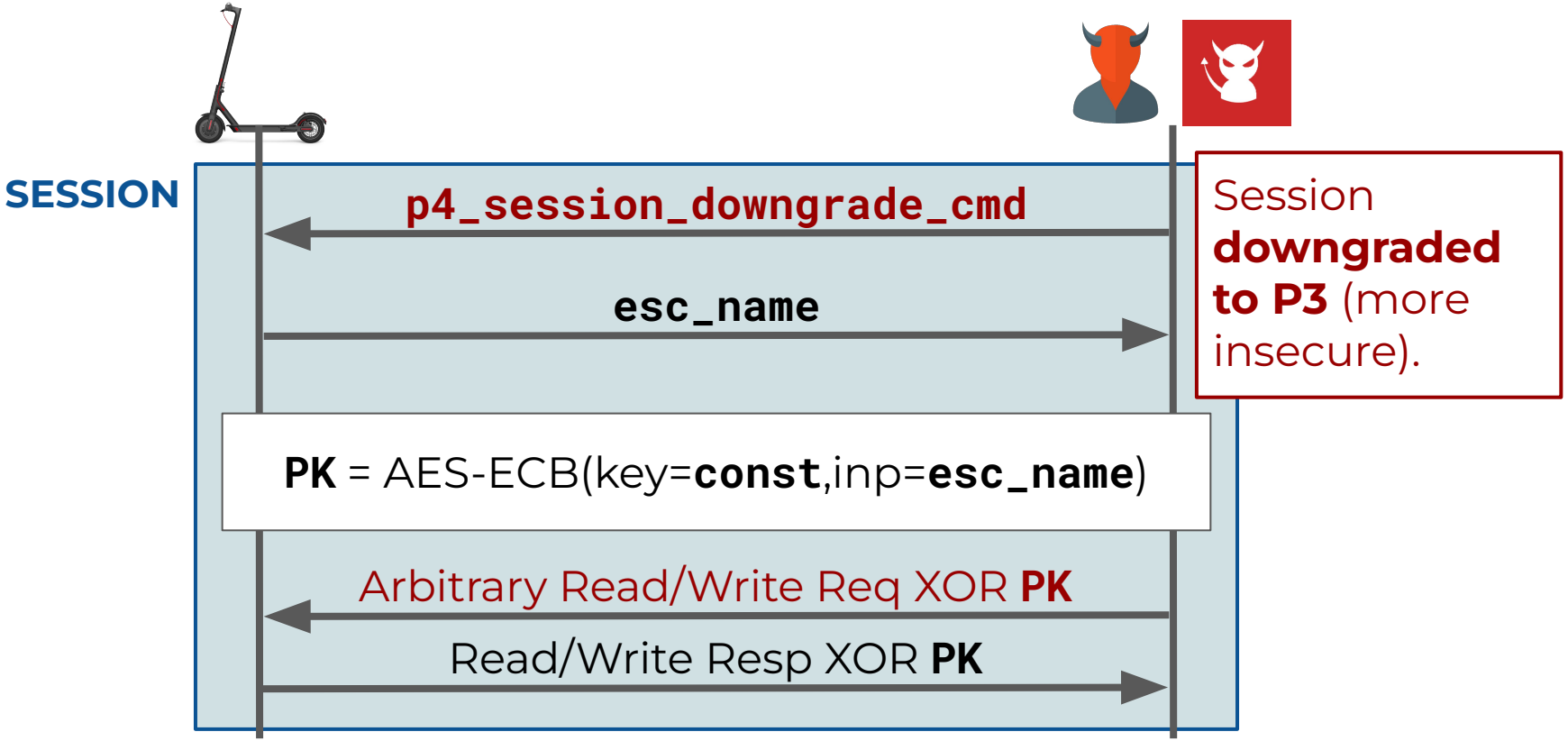
AES-CCM(key=**SK_a**,IV=**IV_a**||**cnt**, inp=**Read/Write Req**)

AES-CCM(key=**SK_e**,IV=**IV_e**||**cnt**, inp=**Read/Write Resp**)

Mutual session auth.

Encrypted and integrity protected comms.

P4: Proximity/Remote Attacks



P4: Proximity/Remote Attacks

SESSION DOWNGRADE

`p4_session_downgrade_cmd`

`esc_name`

Session **downgraded to P3** (more insecure).

PK = AES-ECB(key=**`const`**,inp=**`esc_name`**)

Arbitrary Read/Write Req XOR **PK**

Read/Write Resp XOR **PK**

Xiaomi Custom Protocols

Id	*Name*	*Pairing*	*Session*
P1	No security	None	None
P2	XOR obfuscation	Public XOR mask	XOR mask obfuscation, no auth, no integrity
P3	AES-ECB and XOR obfuscation	Weak AES-ECB key agreement, no auth	XOR obfuscation, implicit auth, no integrity
P4	ECDH and AES-CCM	ECDH, AES-CCM unil. auth	**v1**: HKDF, HMAC, AES-CCM, mutual auth
			v2: v1 with downgrade protection

EVALUATION

Evaluation Setup (E-Scooters)

M365

Essential

Mi 3

- 5 BLE boards (M365, Pro 1, Pro 2, Essential, Mi 3)
- 8 BLE firmware (P1, P2, P3, P4)

Evaluation Setup (Mi Home)

- Mi Home app versions
  - Android v7.11.704 and v7.6.704
  - iOS v7.12.204
- Smartphone models
  - OnePlus 3 (Android 12), Pixel 2 (Android 11), and RealMe GT (Android 9)
  - iPhone 7 (iOS 15.7)

Evaluation Results

E-Scooter	BLE Board	BLE Fw	Protocol	Strategy	Prox/Rem Adv.	
					Spoof Mi Home	*Arb R/W*
M365	M365	072	P1	RE	✓	✓
M365	M365	081	P2	RE, MP, SD	✓	✓
M365	Pro 1	090	P3	RE	✓	✓
M365	M365	122	P4v1	RE, MP, SD	✓	✓
M365	Pro 2	129	P4v1	RE, MP, SD	✓	✓
Essential	Essential	152	P4v1	RE, MP, SD	✓	✓
Mi 3	Mi 3	153	P4v1	RE, MP, SD	✓	✓
Mi 3	Mi 3	157	P4v2	RE, MP	✓	✓

E-SPOOFER TOOLKIT

E-Spoofer Toolkit

- **E-Spoofer** is open-source
  - Automated Proximity MP
  - Automated Remote SD
- **Reversed BLE firmware** (Ghidra)
- Xiaomi **protocol dissectors** (pyshark, scapy)
- **Code hooks** for dynamic testing (Frida)

E-Spoofer: Proximity MP Demo

E-Spoofer: Remote SD Demo

COUNTERMEASURES AND DISCLOSURE

Countermeasures

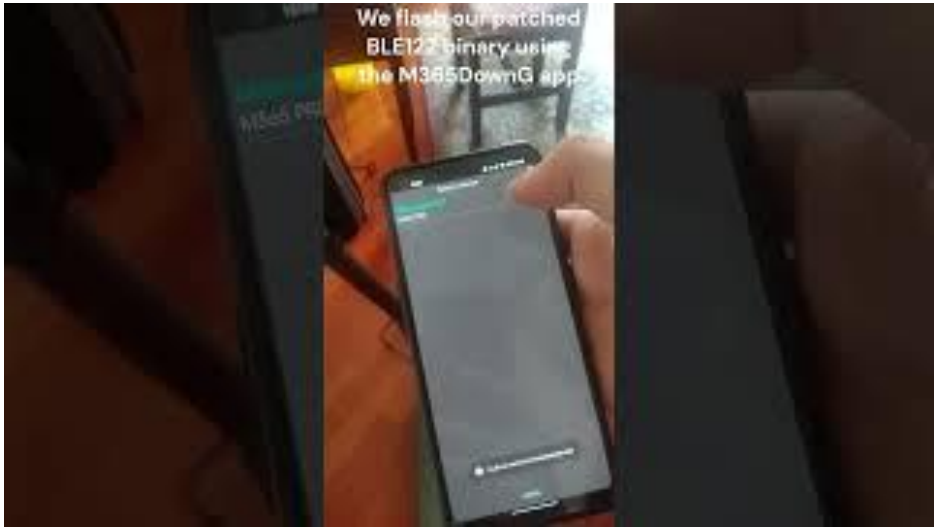
- (C1) Update firmware via Mi Home
  - From P1, P2, P3 to P4v1 or P4v2
- (C2) **Authorized and authenticated pairing**
  - Addresses MP on P4v1 and P4v2
- (C3) **Anti-downgrade BLE fw patching script**
  - Addresses SD on P4v1
  - Evaluated on a real M365

Authorized and Authenticated Pairing

- Upgrade to Xiaomi pairing
  - Secure and backward-compatible
- **Authorized pairing mode**
  - Mandatory gesture to enable pairing mode
- **Password-protected authenticated pairing**
  - Mandatory e-scooter password to start pairing

Anti-Downgrade BLE Fw Patching Script

- Automated tool that modifies BLE122 binary
  - Deletes P4v1 session downgrade command
  - Blocks any P3 packet received



Disclosure

- Xiaomi Bug Bounty on Hackerone
  - Sent paper, toolkit, and demos (21/11/22)
  - Made a few requests for an update
  - Xiaomi: "**Cannot reproduce the attacks**" (06/02/23)
- Also disclosed a Mi Home app bug
  - UI delay allows e-scooter software-unlock even without a password (14/08/22)
  - Xiaomi awarded a 200$ **bounty** (23/12/22)

Conclusion and Q&A

- RE all **Xiaomi e-scooter protocols** since 2016
  - Pairing and Session phases
- Uncover critical **protocol-level vulnerabilities**
  - E.g., unwanted pairing and weak authentication
- **Proximity** and **remote** wireless attacks
  - I.e., malicious pairing and session downgrade
- **E-Spoofer** open-source toolkit
- **Countermeasures** and **disclosure** to Xiaomi