E-Spoofer: Attacking and Defending Xiaomi Electric Scooter Ecosystem

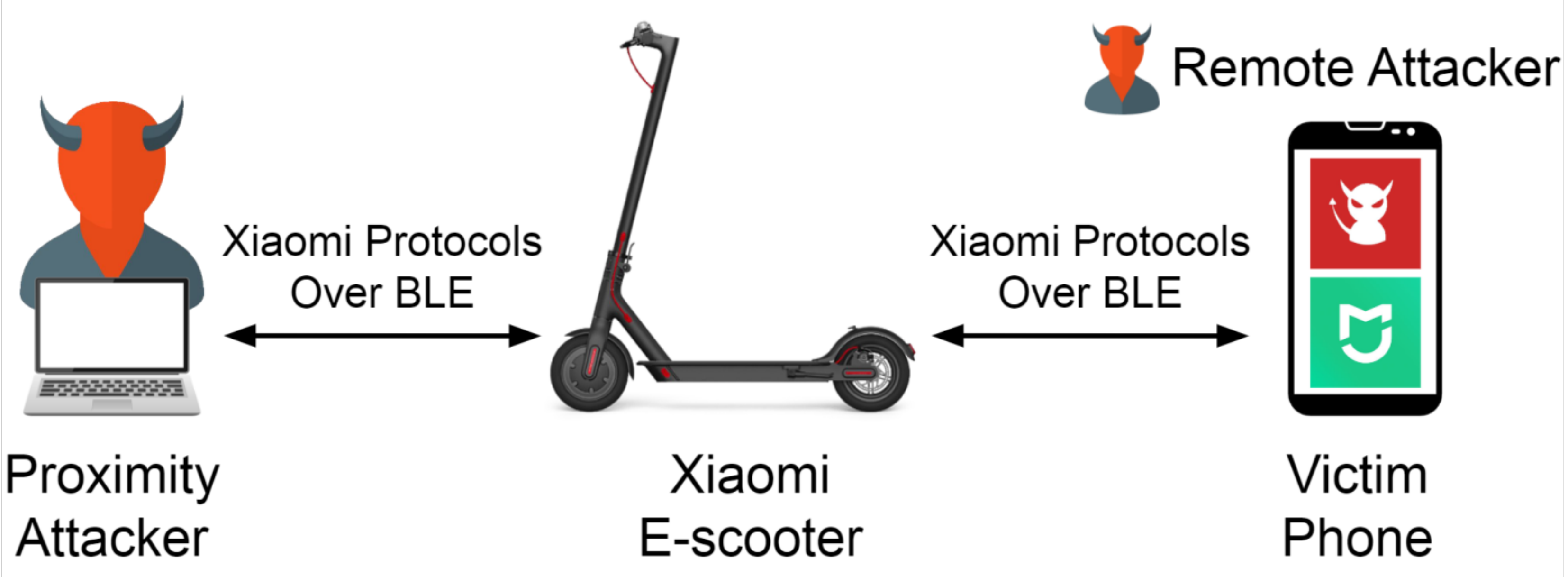
Marco Casagrande (EURECOM), Riccardo Cestaro (UNIPD), Eleonora Losiouk (UNIPD), Mauro Conti (UNIPD), and Daniele Antonioli (EURECOM)

Abstract: We present the first security evaluation on all proprietary wireless protocols deployed to Xiaomi e-scooters released from 2016 to 2021. We identify four protocols, with ad-hoc Pairing and Session phases. We develop four application-layer attacks and we call them Malicious Pairing (MP) and Session Downgrade (SD). They exploit six vulnerabilities in the Xiaomi proprietary protocols spoken over Bluetooth Low Energy (BLE). We successfully evaluate our attacks against three e-scooters and five BLE boards, and we design two practical countermeasures. We open-source E-Spoofer, a toolkit to reproduce the attacks and reverse Xiaomi firmware.

1. MOTIVATION

Despite security, privacy, and safety concerns, no prior research was done on Xiaomi e-scooter ecosystem. Xiaomi, as a market leader, released seven e-scooter models. All of them would be affected by any critical vulnerability found in the application-layer protocols.

2. THREAT MODEL



The e-scooter is paired with the user, software-locked, and password-protected. The attacker sends BLE packets from proximity, or installs a malicious Android app on the phone of the victim. She knows Xiaomi Pairing and Session phase protocols. She does not need physical access.

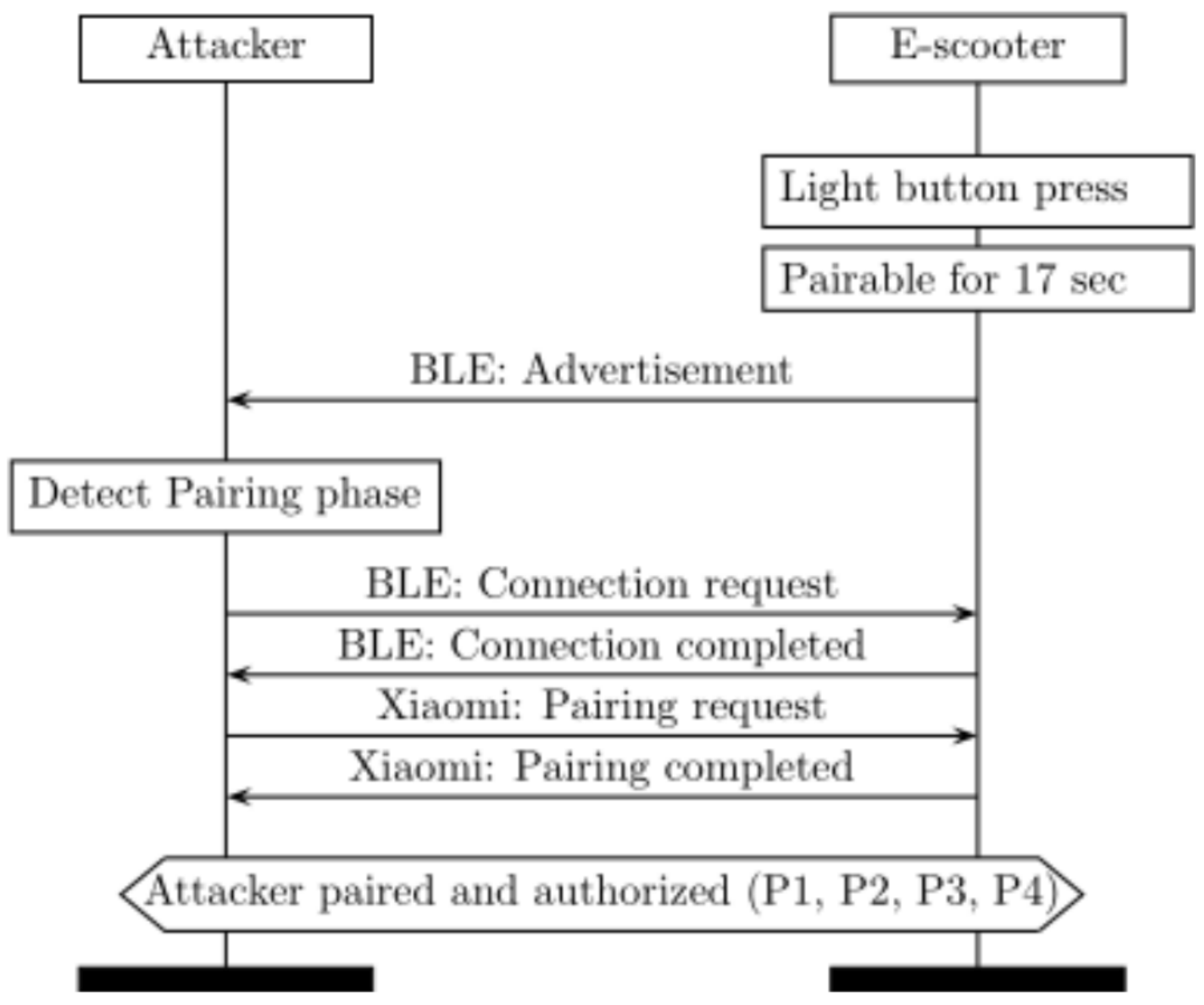
3. VULNERABILITIES

- Unauthenticated Pairing
- Unintentional Pairing mode
- Improper e-scooter password enforcement
- Unprotected sensitive memory
- Downgradable and insecure Session
- No BLE security despite device support

4. XIAOMI PROTOCOLS

- P1 has no security guarantees as it lacks Pairing and Session phases. This is an example of security-by-obscurity.
- P2 uses XOR-based obfuscation. BLE packets are XORed with a 12-byte mask, sent in plaintext during Pairing.
- P3 uses a weak key establishment based on AES-ECB and XOR obfuscation. Pairing derives a key from data available publicly. BLE Session packets are XORed with such key.
- P4 Pairing uses ECDH key agreement and unilateral pairing key authentication through a challenge-response. P4 Session uses HKDF to derive directional session keys and HMAC-based authentication. P4v1 is downgradable to P3, as opposed to the latest non-downgradable P4v2.

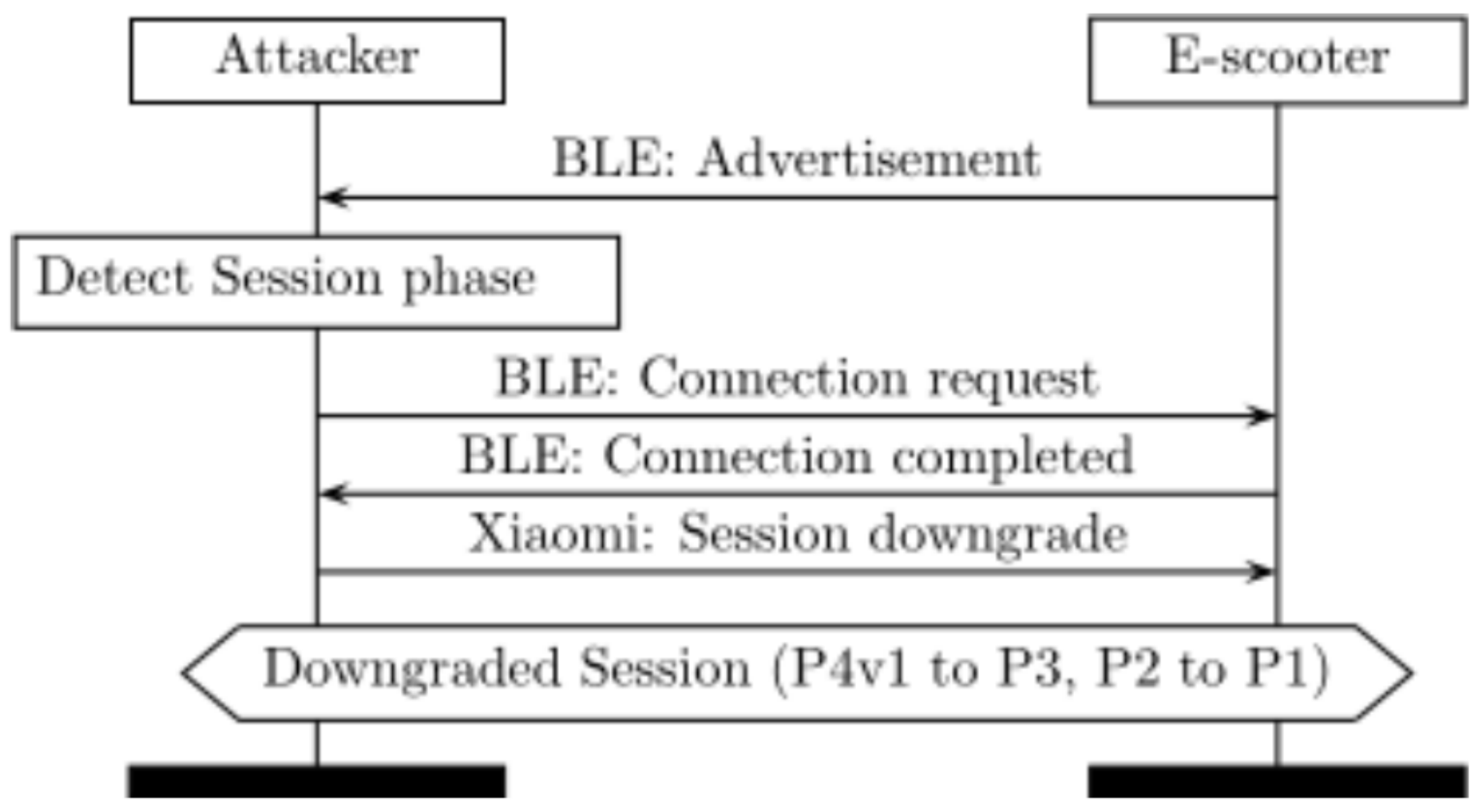
5. MALICIOUS PAIRING



Attacker
E-scooter
Light button press
Pairable for 17 sec
BLE: Advertisement
Detect Pairing phase
BLE: Connection request
BLE: Connection completed
Xiaomi: Pairing request
Xiaomi: Pairing completed
Attacker paired and authorized (P1, P2, P3, P4)

The attacker detects e-scooters in pairing mode and pairs with them to obtain authorized access.

6. SESSION DOWNGRADE



Attacker
E-scooter
BLE: Advertisement
Detect Session phase
BLE: Connection request
BLE: Connection completed
Xiaomi: Session downgrade
Downgraded Session (P4v1 to P3, P2 to P1)

The attacker sends an unprotected Session downgrade command, downgrading P4v1 to P3 or P2 to P1.

7. EVALUATION

					Proximity		Remote	
Firmware	Protocol	E-Scooter	BLE Sub. Board	SoC	MP	SD	MP	SD
BLE072	P1	M365	M365 (Original)	nRF51822 QFAA	✓	-	✓	-
BLE081	P2	M365	M365 (Original)	nRF51822 QFAA	✓	✓	✓	✓
BLE090	P3	M365	Pro 1 (Clone)	nRF51822 QFAA	✓	✗	✓	✗
BLE122	P4v1	M365	M365 (Original)	nRF51822 QFAA	✓	✓	✓	✓
BLE129	P4v1	M365	Pro 2 (Clone)	nRF51822 QFAC	✓	✓	✓	✓
BLE152	P4v1	Essential	Essential (Original)	nRF51822 QFAC	✓	✓	✓	✓
BLE153	P4v1	Mi 3	Mi 3 (Original)	nRF51822 QFAC	✓	✓	✓	✓
BLE157	P4v2	Mi 3	Mi 3 (Original)	nRF51822 QFAC	✓	✗	✓	✗

Scan the QR code on the left, to read our full paper.

Scan the QR code on the right, to access E-Spoofer source code and our video demonstrations.

Published on Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, May 2023, pp 85–95.