BreakMi: Reversing, Exploiting and Fixing Xiaomi Fitness Tracking

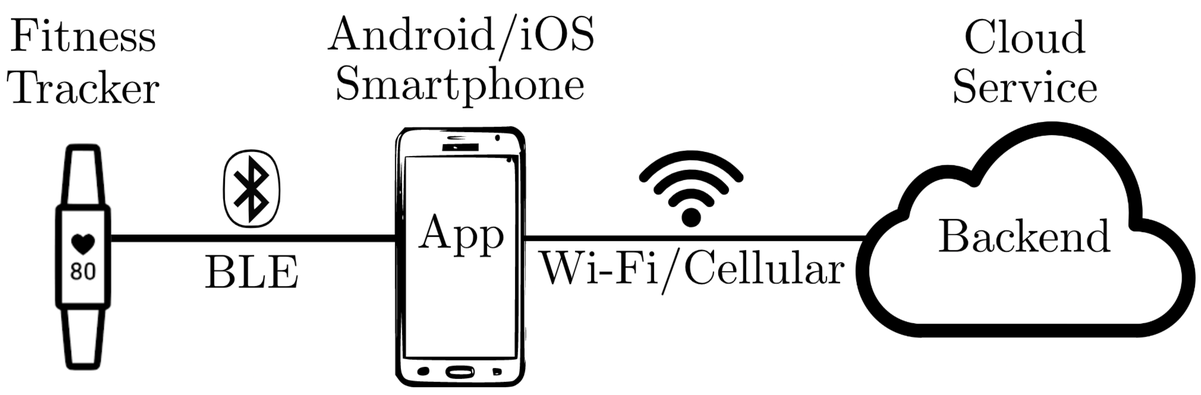
Marco Casagrande (EURECOM), Eleonora Losiouk (UNIPD), Mauro Conti (UNIPD), Mathias Payer (EPFL), and Daniele Antonioli (EURECOM)

Abstract: We present an extensive security evaluation of six Xiaomi fitness trackers released from 2016 to 2021, and two official Android companion apps. We perform six low-cost attacks on Xiaomi fitness trackers, exploiting seven novel vulnerabilities in Xiaomi proprietary application-layer protocols spoken over Bluetooth Low Energy (BLE), and we propose five countermeasures to fix Xiaomi protocols.
We open-source BreakMi, an automated BLE security toolkit capable of impersonation, man-in-the-

1. MOTIVATION

Despite Xiaomi being the fitness tracking market leader, no prior research was done. Xiaomi ecosystem counts millions of trackers sold and active users, all affected by critical security and privacy concerns in Xiaomi

2. THREAT MODEL



The attacker knows public data advertised by the tracker, has no physical access, and knows Xiaomi proprietary Pairing v1/v2, Authentication and Communication protocols. The attacker sends BLE packets from proximity, or installs a malicious

3. VULNERABILITIES

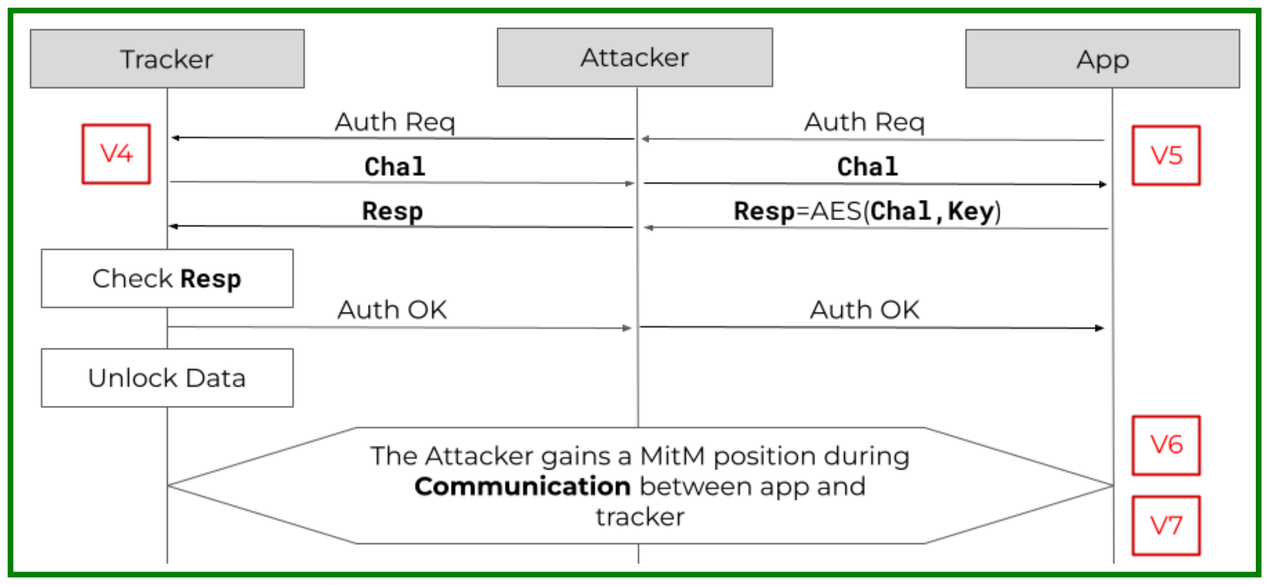
- V1 Pairing key, or key seed, sent in clear (Pairing
- V2 v1/v2)
- V3 Pairing not, or weakly, authenticated (Pairing
- V4 v1/v2)
- V5 Weak user confirmation (Pairing v1/v2)
- V6 Unilateral app authentication (Authentication)
- V7 Replayable challenges and responses

4. ATTACKS

Four proximity attacks deployed over a BLE connection with the victim's tracker or companion app:
• Eavesdropping
• App Impersonation
• Tracker Impersonation

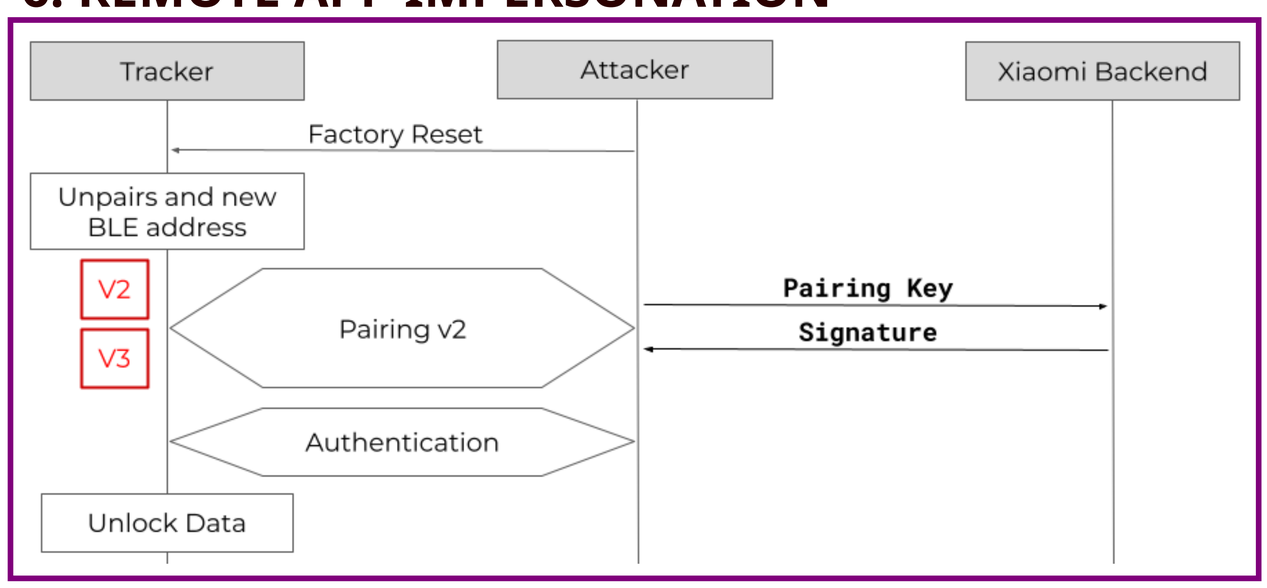
Two remote attacks deployed by a malicious app, which exploits a security issue on the Android BLE API:
• Eavesdropping

5. PROXIMITY MAN-IN-THE-MIDDLE



The attacker impersonates the app to the tracker, and viceversa, thus gaining a man-in-the-middle

6. REMOTE APP IMPERSONATION



The attacker sends an unprotected factory reset command, and triggers a new Pairing, thus gaining complete control.

7. EVALUATION

	Proximity Attacks				Remote Attacks	
	Trac Imp.	App Imp.	MitM	Eavesdr.	App Imp.	Eavesdr.
Zepp Life	n/a	✔	✔	✔	✔	n/a
Zepp	n/a	✔	✔	✔	✔	n/a
Mi Band 2	✔	n/a	✔	✔	n/a	✔
Mi Band 3	✔	n/a	✔	✔	n/a	✔
Amazfit Cor 2	✔	n/a	✔	✔	n/a	✔
Mi Band 4	✔	n/a	✔	✔	n/a	✔
Mi Band 5	✔	n/a	✔	✔	n/a	✔
Mi Band 6	✔	n/a	✔	✔	n/a	✔

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

Scan the QR code on the right, to access BreakMi source code and our video demonstrations.

Published on IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES), Vol. 2022, No. 3, pp. 330–366.