BreakMi: Reversing, Exploiting and Fixing Xiaomi Fitness Tracking Ecosystem

CHES 2022, Leuven (Belgium)

Marco Casagrande, Eleonora Losiouk, Mauro Conti, Mathias Payer and Daniele Antonioli
Motivations

- Fitness tracking ecosystems are pervasive
- **Critical** security and privacy concerns
  - Health data
- No prior research on Xiaomi despite being the market leader (19.6% share in 2021)
- Xiaomi ecosystem runs proprietary protocols
  - Attacks affect millions of devices regardless of hardware
Contributions

● Reversing Xiaomi custom protocols uncovering severe and novel vulnerabilities
● Deploying 6 impactful and low-cost attacks on the most recent trackers
● Open-sourcing BreakMi, an automated toolkit
● Fixing the protocols, and disclosing to Xiaomi
● Comparison with Fitbit ecosystem
Xiaomi custom protocols over Bluetooth Low Energy

Our main focus
Pairing

Key Agreement

Fitness Tracker
Pairing Key

Companion App
Pairing Key
Authentication

Proving possession of shared Key

Fitness Tracker

Pairing Key

Companion App

Pairing Key
Communication

Exchanging data

Pairing Key

Fitness Tracker

Pairing Key

Companion App

Bluetooth
Proximity Attacks

● Four proximity over-the-air attacks
  ○ Eavesdropping
  ○ Tracker Impersonation
  ○ App Impersonation
  ○ Man-in-the-Middle
Proximity Threat Model

Pairing v1 / Pairing v2 / Authentication / Communication

Fitness Tracker

Eavesdropping

App Impersonation

Tracker Impersonation

Attacker

Man-in-the-Middle

Companion App
Proximity Eavesdropping

1) Pairing Key sent in clear

2) Pairing Key Seed sent in clear

3) No encryption

Key = SHA256(BLEaddr, Seed)
Proximity Tracker Impersonation

The Attacker is trusted during Communication with app

Attacker

Auth Req

Chal

Resp=AES(Chal, Key)

App

Auth OK

Ignore Resp

Unlock Fake Data

4) Unilateral app authentication
Proximity App Impersonation

The Attacker is trusted during 
**Communication** with tracker

5) Replayable authentication
Proximity Man-in-the-Middle

The Attacker gains a MitM position during Communication between app and tracker

- Tracker
  - Auth Req → Chal
  - Chal → Resp
  - Check Resp
  - Unlock Data

- Attacker
  - Auth Req → Chal
  - Chal → Resp = AES(Chal, Key)
  - Auth OK

- App
  - Auth Req → Chal
  - Chal → Resp = AES(Chal, Key)
  - Auth OK

3) No encryption
6) No integrity protection
Remote Attacks

- Two remote software-based attacks
  - Eavesdropping
  - App Impersonation
Remote Threat Model

- **Eavesdropping**
- **App Impersonation**

- **Android BLE API**
- **Xiaomi App**
- **Attacker App**

Marco Casagrande - BreakMi: Reversing, Exploiting and Fixing Xiaomi Fitness Tracking Ecosystem
Remote Eavesdropping

1) Pairing Key sent in clear
2) Pairing Key Seed sent in clear
3) No encryption
Remote App Impersonation

Factory reset

New BLE address

Android BLE API

Xiaomi App

Attacker App

7) Weak user confirmation

Marco Casagrande - BreakMi: Reversing, Exploiting and Fixing Xiaomi Fitness Tracking Ecosystem
### Evaluation Setup

| Tracker      | Release Year | Pairing Version | Bluetooth Version | LE Secure Conn. | Link Layer Security |
|--------------|--------------|-----------------|-------------------|-----------------|---------------------|
| Mi Band 2    | 2016         | 1               | 4.2               | X               | ✔                   |
| Mi Band 3    | 2018         | 1               | 4.2               | X               | ✔                   |
| Cor 2        | 2019         | 1               | 4.2               | X               | ✔                   |
| Mi Band 4    | 2019         | 2               | 5.0               | ✔               | ✔                   |
| Mi Band 5    | 2020         | 2               | 5.0               | ✔               | ✔                   |
| Mi Band 6    | 2021         | 2               | 5.0               | ✔               | ✔                   |
### Evaluation Setup - cont.

| App                          | App Version | Year | OS    |
|------------------------------|-------------|------|-------|
| Zepp Life (formerly Mi Fit)  | 4.8.1       | 2020 | Android |
| Zepp (formerly Amazfit)      | 5.9.2       | 2021 | Android |

- Acer Aspire 3 laptop
- CSR8510 A-10 Controller
- BLE sniffer (BBC Micro Bit + btlejack)
## Evaluation Results

|                      | 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      | ✔        |
## Vulnerable Android Versions (stats)

| Smartphone   | Android Version | Remote Attacks | Eavesdropping | App Impersonation |
|--------------|-----------------|----------------|---------------|-------------------|
| Pixel 4A     | 12 (23.58%)     | ✔️*            | ✔️*           |                   |
| Pixel 2XL    | 11 (27.96%)     | ✔             |               | ✔                 |
| Pixel 2XL    | 10 (20.98%)     | ✔             |               | ✔                 |
| Galaxy J5    | 9 (10.58%)      | ✔             |               | ✔                 |
| Redmi 5 Plus | 8 (8.08%)       | ✔             |               | ✔                 |
| Galaxy S5    | 6 (2.25%)       | ✔             |               | ✔                 |

* Requires dangerous runtime permission `BLUETOOTH_CONNECT`
BreakMi

- BreakMi on Github
- Attack videos on Youtube
  - Xiaomi and Fitbit
- CHES Artifact approval

Proximity Man-in-the-Middle demo
Conclusion

- Reversing Xiaomi custom protocols uncovering severe and novel vulnerabilities
- Deploying 6 impactful and low-cost attacks on the most recent trackers
- Open-sourcing BreakMi, an automated toolkit
- Fixing the protocols, and disclosing to Xiaomi
- Comparison with Fitbit ecosystem
Summary

● Cover slide
● Threat model (system + protocols + attacker model)
● Summary of 4 OTA attacks (TI, AI, MitM, Eave)
● Describe OTA attacks, related vulns, remember RE
● Remote attacks (AI, Eave)
● Evaluation (trackers, apps, results)
● Countermeasures (optional)
● Conclusions
**Pairing v1**

- Tracker
  - Pairing Init
  - `pair_v1`
  - Key [16 B]
  - Wait for user confirmation
  - Pairing Complete

- App
  - Pairing key sent in clear
  - Pairing not authenticated

- Weak user confirmation

Marco Casagrande - BreakMi: Reversing, Exploiting and Fixing Xiaomi Fitness Tracking Ecosystem
Pairing v2

Tracker

Pairing Init

Pair_v2, SHA1(pub_k)

Rand Req

Rand [16 B]

Key=kdf(TR_A, Rand)

App

Key=kdf(TR_A, Rand)

Backend

Default keypair

SHA1(pub_k), Base64(Key)

Sig=sign(Key, pri_k)

Pairing key seed sent in clear

Continues in the next slide
Pairing v2 - cont.

Tracker ► App

Sig

verify(Sig, pub_k)

Valid Sig

Wait for user confirmation

Pairing Complete

Reset Data

Backend

B64(Sig)

Weak user confirmation

Pairing (weakly) authenticates only the app
Authentication

Tracker

Auth Req

Resp = AES(Chal, Key)

Check Resp

Unlock Data

App

Auth OK

Replayable authentication

Unilateral app authentication
Communication

Tracker

Enable notifications

Send data update

Send data update

Send data update

App

No encryption

No integrity protection
Speaker Info

Marco Casagrande
Email: marco.casagrande@eurecom.fr

PhD @ EURECOM (France)
S3 System Security Research Group

Research Topics:
● Bluetooth / Bluetooth Low Energy
● IoT
● Android
## Market Share

| Vendor  | Q2 2021 Shipments | Q2 2021 Market Share | Q2 2020 Shipments | Q2 2020 Market Share |
|---------|-------------------|----------------------|-------------------|----------------------|
| Xiaomi  | 8.0m              | 19.6%                | 7.8m              | 20.1%                |
| Apple   | 7.9m              | 19.3%                | 6.1m              | 15.8%                |
| Fitbit  | 3.0m              | 7.3%                 | 2.5m              | 6.4%                 |
| Others  | 22m               | 53.8%                | 22.3m             | 57.7%                |
| Total   | 40.9m             | 100%                 | 38.7m             | 100%                 |

Canalys wearable band analysis August 2021 [source](#)
Countermeasures

1. **(Authenticated) Key Establishment**
   - Tracker and app generate a keypair, sharing the public key
   - Both perform Diffie-Hellman to generate a **SharedSecret**

2. **Strong Pairing Confirmation**
   - Both exchange nonces and calculate confirmation value
   - User confirmation if values match
Countermeasures

3. **Strong Key Authentication**
   - Need for mutual authentication
   - Tracker and app exchange ChalApp and ChalTra
   - $\text{Resp1}, \text{Resp2} = \text{HASH(SharedSecret, ChalApp, ChalTra)}$
   - Responses are checked
Countermeasures

4. Authenticated Encryption
   - Need for encrypted Communication session
   - Tracker and app exchange nonces
   - $\text{SessionKey} = \text{HKDF}(\text{SharedSecret, NonceApp, NonceTra})$
   - AES-CCM encrypted session using SessionKey

5. BLE Link-Layer Security
   - Complementary to Application-Layer Security
   - Enable LE Secure Connections feature on Mi Band 4/5/6