BreakMi: Reversing, Exploiting and Fixing Xiaomi Fitness Tracking Ecosystem

CHES 2022, Leuven (Belgium)



<u>Marco Casagrande</u>, Eleonora Losiouk, Mauro Conti, Mathias Payer and Daniele Antonioli





Università degli Studi di Padova



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 **<u>BreakMi</u>**, an automated toolkit
- Fixing the protocols, and disclosing to Xiaomi
- Comparison with Fitbit ecosystem

System Model



Our main focus

Pairing



Authentication



Communication



Proximity Attacks

- Four proximity over-the-air attacks
 - Eavesdropping
 - Tracker Impersonation
 - App Impersonation
 - Man-in-the-Middle

Proximity Threat Model



Proximity Eavesdropping



Proximity Tracker Impersonation



Proximity App Impersonation



Proximity Man-in-the-Middle



Remote Attacks

- Two remote software-based attacks
 - Eavesdropping
 - App Impersonation

Remote Threat Model



Remote Eavesdropping



Remote App Impersonation



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.

Арр	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	v	~	~	~	n/a
Mi Band 2	~	n/a	~	~	n/a	~
Mi Band 3	v	n/a	~	~	n/a	~
Amazfit Cor 2	v	n/a	v	~	n/a	~
Mi Band 4	v	n/a	v	~	n/a	~
Mi Band 5	v	n/a	v	~	n/a	~
Mi Band 6	 ✓ 	n/a	v	~	n/a	~

Vulnerable Android Versions (stats)

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

* Requires dangerous runtime permission **BLUETOOTH_CONNECT**

BreakMi

- BreakMi on <u>Github</u>
- Attack videos on <u>Youtube</u>
 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 **<u>BreakMi</u>**, an automated toolkit
- Fixing the protocols, and disclosing to Xiaomi
- Comparison with Fitbit ecosystem

BACKUP SLIDES

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]

Pairing v1



Pairing v2



Pairing v2 - cont.







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
- o Resp1,Resp2 = HASH(SharedSecret,ChalApp,ChalTra)
- Responses are checked

Countermeasures

4. Authenticated Encryption

- Need for encrypted Communication session
- Tracker and app exchange nonces
- o SessionKey = HKDF(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