Unfit for Purpose? A Security and Privacy Analysis of the Fitbit Tracking System

Paul Patras
The University of Edinburgh

Fitness wristbands and smartwatches are becoming increasingly popular, forecasts suggesting that 830 million wearable gadgets will be shipped by 2020. Beyond fitness and sleep tracking capabilities, their potential to improve patient health monitoring and assist in criminal investigations is yet to be fulfilled. Specifically, given the sensitive nature (daily step counts, heart rate profiles, and locations visited) and often monetary value (rewards, insurance, workplace provisioning) of the data fitness trackers collect, their success will ultimately depend on guaranteeing records' authenticity, tamper-proof hardware, secure operation and communication, and user privacy.

In this talk I will present an in depth security and privacy analysis of the Fitbit ecosystem, scrutinizing the devie↔cloud communication, official mobile app, and tracker firmware. As a market leader, Fitbit has developed perhaps the most secure wearables system architecture that now guards communication with end-to-end encryption and the brand makes continuous efforts to harden its products. I will demonstrate, however, a series of vulnerabilities with potentially severe implications to user privacy and device security.

I will first reveal an intricate security through obscurity approach implemented by the user activity synchronization protocol running on earlier device models. Based on reverse engineering of the message semantics, I will show how sensitive personal information can be extracted in human-readable format, and demonstrate that malicious users can inject fabricated activity records to obtain personal benefits.

I will discuss how attackers can exploit information present in activity reports intercepted from nearby victim trackers, to associate these with a controlled account and subsequently exfiltrate all recently recorded fitness measurement data. In addition, I will explain how an attacker can acquire authentication credentials for any device, then replay these to gain access to tracker commands. This includes triggering "live mode" operation, which forces target trackers to leak unencrypted data in real-time. I will also show that the firmware update protocol can be compromised and the code running on selected device types within wireless range can be modified. This enables crafting and injecting malicious firmware without consent, disabling authentication and encryption.

Finally I will discuss how we modified the official smartphone app and discovered developer options that can be enabled via configuration files for all original app versions. I reveal that the Fitbit server endpoint is reprogrammable, and argue that it is possible to develop an independent custom service, which subverts the Fitbit cloud and gives full control over user privacy.

Although the majority of the vulnerabilities identified have been patched by Fitbit following responsible disclosure, the lessons learned and design recommendations made apply to other Internet of Things applications governed by gadget↔app↔cloud paradigms, where the smartphone acts as a mediator between the user, device, and service.