Abstract

SECURITY ANALYSIS OF MI BAND 4

Pragati Mishra, Arpit Gupta, Santiago Carvajal

Carnegie Mellon University

Fitness trackers have become important wearable devices that a large number of people have adopted. Since they track sensitive information and are always connected to the smartphone of the user, they pose a potential security risk. Our research focuses on the security of the Mi Band 4 (a wearable fitness tracker by Xiaomi), trying to identify its general architecture and possible security issues. It tries to look at three different aspects of security: on-device, in-transit and privacy; and performs a deep study on few interesting areas. We chose Mi Band 4 since it is very popular in Southeast Asia and has not been researched upon much.

Fig 1. Architecture

Fig 2. Experimental Setup

After understanding and evaluating some of the aspects of the Mi Band 4, we believe that this tracker has good security features that prevents leak of data. In the privacy field, we saw that the Mi Band 4 was handling user data in an effective way, not leaking any of the sensitive information belonging to a user, although it can do a better job at encrypting some of the information stored by the app, making the system more robust. In the on-device approach, the Mi Band 4 doesn’t allow to dump data easily from the tracker nor the smartphone, since it requires to be rooted. In the in-transit approach, we observe that the services are not public and require authentication. Additionally, the pairing process now requires a valid user for approval by the Xiaomi’s servers, and thus there can be a trace of users who have been paired with the trackers.

References: