ABSTRACT

Internet of Things (IoT) applications are on the rise within the last decade with many industries transiting to manufacturing IoT products and services. With the increase in connectivity and integration of IoT devices in our daily lives, these devices are becoming ever more pervasive throughout society. IoT devices are opaque black boxes that consumers purchase for their utility but fail to evaluate their potential security risk. With the emergence of wearable fitness trackers that follow your every move and process your sensitive health data, there has been scrutiny placed on these products to determine whether they truly preserve the privacy of your data. Particularly there has been much academic research in recent years examining the security of various Fitbit devices. Following in their footsteps, we will evaluate the security of an unexamined Fitbit product as well as other fitness trackers from other brands to gain an understanding of current security posture present in the IoT wearable industry. We created a workflow that systematizes the reverse engineering process and applied it to find several vulnerabilities across several different trackers.