PHYS ORG

Are fitness trackers fit for security?

September 9 2016

They may look like a normal watch but are capable to do much more than just showing the time: So called fitness trackers are collecting data on their users' lifestyle and health status on a large scale helping them with training or losing weight. Ahmad-Reza Sadeghi, system security professor at the cybersecurity profile area (CYSEC) of TU Darmstadt and his team investigated fraud opportunities with fitness trackers and detected serious security flaws.

The popularity of these devices is constantly growing. Worldwide, nearly 20 million fitness trackers have been sold in the first quarter of 2016. Many of them track via GPS the kilometers the user run, measure heart rate and pulse or check if the user is asleep. "These data are not only used for the original purpose but are increasingly being used by third parties," explains professor Sadeghi.

Data collected by fitness trackers have been used as evidence in court trials in the US, as reported by Forbes Magazine in 2014. Police and attorneys have started to recognize wearable devices as the human body's "black box," the NY Daily News wrote in April 2016. Some health insurance companies recently started to offer discounts if the insured persons provide personal data from their fitness trackers. This could attract scammers who manipulate the tracked data to fraudulently gain financial benefits or even influence a court trial, says Sadeghi. This makes it all the more important that transmission, processing and storing of the sensitive personal data meet high security standards.

To investigate this, Sadeghi and his team conducted a study in cooperation with the University of Padua (Italy) on 17 different fitness trackers including devices from less well-known manufacturers as well as devices from popular brands like Xiaomi, Garmin and Jawbone. The researchers concentrated on manipulating the data on their way to the cloud server by a "man-in-the-middle" attack and examined the security of communication protocols used by the fitness trackers.

The result: Although all cloud-based tracking systems use an encrypted protocol like HTTPS to transfer data, the researchers were able to falsify data in all cases. Out of all fitness trackers examined, only devices from four manufacturers took some minor measures to protect data integrity, i.e. to ensure that data remain intact and unaltered. "These hurdles cannot stop a motivated attacker. Scammers can manipulate the data even with very little IT knowledge," Sadeghi warns, as none of the trackers employ End-to-End encryption or other effective tamper protection measures when synchronizing data.

Five of the examined fitness trackers did not provide a possibility to synchronize fitness data with an online service. However, these manufacturers store the collected fitness data in plain-text, i.e. un-encrypted and readable by everyone, on the smartphone which introduces a potential risk of unauthorized data leakage should the smartphone be stolen or infected with malware. This is another serious security flaw of fitness trackers the researchers from TU Darmstadt and University of Padua found.

"Health insurances and all other companies who want to use fitness trackers for their services should seek advice from security experts before doing so," Sadeghi suggests. The flaws found in the study could be fixed with known standard technologies, "it's just that the manufacturers have to put some more effort in employing these technologies in their products."

Provided by Technische Universitat Darmstadt

Citation: Are fitness trackers fit for security? (2016, September 9) retrieved 10 July 2024 from https://phys.org/news/2016-09-trackers.html