Wearable fitness devices carry security risks

5 August 2015, by Jacob Betzner, Pittsburgh Post-Gazette

During a 2014 competition among Netflix employees to create potential new features, one group hacked into a Fitbit and created a "Sleep Bookmark" function, automatically pausing Netflix as the wearer started to fall asleep.

Though used to create a function for the on-demand Internet streaming content company that might be appealing to late-night movie watchers, the competition showed the vulnerability of wearable fitness devices to hacking.

From allowing a user to accidentally post activity logs on social media showing the number of calories burned during sex to helping jealous types keep tabs on their significant others to permitting the owner to transmit false data about physical activity, wearable fitness devices such as Fitbit, Nike FuelBand, Polar Loop and Jawbone UP come with the potential for a number of unintended consequences.

The devices log vast amounts of data about the user, tracking steps and the number of calories burned, heart rate and sleep patterns among other information. The devices link the gathered information to a user profile connected to a laptop or smartphone through a Bluetooth connection and send the information to the cloud for safekeeping. The potential for a hack exists during the data exchanges.

On the technology blog evilsocket, Simone Margaritelli, a software developer and security researcher for mobile security company Zimperium, reverse-engineered a Nike FuelBand and accessed data logs on the device.

"The information you can leak from the device itself is not sensitive, only a bunch of data about people's health habits," he said.

However, Margaritelli said tapping into a device sync gives hackers backdoors into laptops and smartphones loaded with personal information. The device requires no user authentication. But hacking into the devices takes time, skill, technical knowledge and, most importantly, opportunity.

"It would require a high level of experience - someone who's able to reverse the original firmware, modify it and reassemble it before actually sending it to the device," Margaritelli said.

A study by German antivirus company AV-TEST concluded that six out of nine of the world's top-selling fitness trackers - including the Fitbit Charge - can be hacked into, and data can be altered through any Bluetooth-LE enabled device.

Bogdan Carbunar, a professor at the Florida International University School of Computing and Information Sciences, showed another type of hacking into wearable fitness devices. A team led by Carbunar reverse-engineered a Fitbit Ultra and a Garmin Forerunner.

After entering the unencrypted backdoor on the device, Carbunar found a way to inject exaggerated information into a Fitbit user profile linked to the rewards site EarndIt. The site offers users redeemable rewards, usually gift cards, for reaching certain fitness goals. The ability to manually manipulate results could carry higher consequences as health insurers consider using the data tracked by wearable fitness devices to adjust plan rates.

"This data could be considered by health insurance companies to give discounts on premiums," Carbunar said. "If you show every day you walk 10,000 steps, you pay less, without actually doing the work."

Amy Baker, a vice president at Pittsburgh-based Wombat Security Technology, said marketers seek user profiles and GPS logs from the devices for targeted advertising. The logs - combined with

gender, height and weight - give marketers insight into how, when and where to advertise to a specific user.

Baker said being able to track places visited by the user makes phishing attacks possible. Knowing a place recently visited by the wearer allows hackers to send a fake email offering deals or a customer survey from the store or restaurant with the link actually linked to spyware or a virus.

"A lot of applications ask to access your contacts or location services," she said. "You can protect yourself by thinking 'I don't need to share this; I want to keep it private.'"

In fact, Dan Nydick, technical director at Avere Systems in Pittsburgh, urged wearable fitness device users only to give out information essential to the functioning of the device.

"If someone knocked on your door and asked for your birthday, you probably wouldn't just tell them," he said. "It should be the same for your apps and devices."

Besides marketers, John Christiansen, a Seattle-based attorney specializing in information technology and health care law, said hackers seek the vast amounts of raw data stored in wearable personal fitness devices servers to sell on active "data black markets."

Hackers "can turn around and sell the information through various channels for financial gain," he said.

Christiansen said a data breach involving wearable fitness devices could allow identity thieves to commit Medicare fraud or potentially blackmail individuals in paying to prevent health information from being leaked. Worse, the greater the amount of information a criminal gathers about a potential victim, the higher the chance of gaining access to more sensitive information.

A Fitbit spokesman wrote: "It has always been our policy not to sell user data; we have never sold personal data and we do not share personal data unless a user specifically directs us to do so, or under the limited exceptions described in our privacy policy."