Watch out: If you've got a smart watch, hackers could get your data

September 10 2015, by David Robertson

Using a homegrown app, researchers were able to guess what a user was typing through data 'leaks' produced by the motion sensors on smart watches. Credit: University of Illinois

They're the latest rage in jewelry and gadgetry, but like all computer devices, smart watches are vulnerable to hackers, say researchers at the University of Illinois at Urbana-Champaign.

Using a homegrown app on a Samsung Gear Live smart watch, the researchers were able to guess what a user was typing through data "leaks" produced by the motion sensors on smart watches. The project, called Motion Leaks through Smartwatch Sensors, or MoLe, has privacy implications, as an app that is camouflaged as a pedometer, for example, could gather data from emails, search queries and other confidential documents.

The work, funded by the National Science Foundation, is being presented this week at the MobiCom 2015 conference in Paris.

"Sensor data from wearable devices will clearly be a double-edged sword," said Romit Roy Choudhury, associate professor of electrical and computer engineering at Illinois. "While the device's contact to the human body will offer invaluable insights into human health and context, it will also make way for deeper violation into human privacy. The core challenge is in characterizing what can or cannot be inferred from sensor data and the MoLe project is one example along this direction."

The app uses an accelerometer and gyroscope to track the micro-motion of keystrokes as a wearer types on a keyboard. After collecting the sensor data, researchers ran it through a "Keystroke Detection" module, which analyzed the timing of each keystroke and the net 2D displacement of the watch. For example, the left wrist moves farther to type a "T" than an "F."

While Illinois researchers developed MoLe, it is conceivable that hackers could build a similar app and deploy it to iTunes and other libraries.

Roy Choudhury's team said the rapid proliferation of wearable devices made them ask: Just how secure is the data? They approached this topic from the perspective of an attacker. Rather than directly developing security measures for smart watches, they aimed to discern ways that attackers can decipher users' information.

"There are a lot of good things that smart watches can bring to our lives, but there could be bad things," said He Wang, a PhD student in electrical and computer engineering at Illinois. "So if you think from that perspective—if there are any 'bad' things we could do—we can help other people protect their privacy, or at least make them realize there's a potential problem."

A possible solution to these motion leaks would be to lower the sample rate of the sensors in the watch, Wang says. For instance, the sample rate is normally around 200 Hertz, meaning the system logs 200 accelerometer and gyroscope readings per second. However, if that number is lowered to below 15, the users' wrist movements become extremely difficult to track.

While their work has yielded revolutionary results so far, there is still a long way to go in polishing the data-collection process. The team's current system can't detect special characters such as numbers, punctuation and symbols that might appear in passwords. The "space" bar or key also poses an obstacle. In addition, researchers can only collect data from the hand wearing the watch and from people who have standard typing patterns.

"There's a subset of people who don't type like that," said Ted Tsung-Te Lai, 30, a post-doctorate researcher at Illinois, who noted that the team will develop more models to account for typing differences in the future.

While a Samsung watch was used in this project, the researchers believe

that any wearable device that uses motion sensors—from the Apple Watch to Fitbit—could be vulnerable as well.

Lai said, "We would just like to advise people who use the watch to enjoy it, but know that 'Hey, there's a threat'."

More information: synrg.csl.illinois.edu/papers/mole.pdf

Provided by University of Illinois at Urbana-Champaign