Your smartwatch is giving away your ATM PIN

July 6 2016

Credit: CC0 Public Domain

Wearable devices—Fitbits, Jawbones, Nike+, Apple Watches and the like—are white-hot. The tech segment is already producing an estimated $14 billion in sales worldwide, and expected to more than double within

four years, climbing to north of $30 billion.

But a new Stevens Institute of Technology research report reveals those cool wearables just may leak information as you use them. Stevens researchers discovered that the motions of your hands as you use PIN pads, which is continually and automatically recorded by your device, can be hacked in real time and used to guess your PIN with more than 90 percent accuracy within a few attempts.

Electrical and computer engineering professor Yingying Chen and three of her graduate students carried out the tests in Stevens labs, assisted by Stevens alumnus Yan Wang Ph.D. '15, now a professor at Binghamton University.

"This was surprising, even to those of us already working in this area," says Chen, a multiple-time National Science Foundation (NSF) awardee. "It may be easier than we think for criminals to obtain secret information from our wearables by using the right techniques."

The Stevens team outfitted 20 volunteers with an array of fitness wristbands and smart watches, then asked them to make some 5,000 sample PIN entries on keypads or laptop keyboards while "sniffing" the packets of Bluetooth low energy (BLE) data transmitted by sensors in those devices to paired smartphones.

"There are two kinds of potential attacks here: sniffing attacks and internal attacks," explains Chen. "An adversary can place a wireless 'sniffer' close to a key-based security system and eavesdrop sensor data from wearable devices. Or, in an internal attack, an adversary accesses sensors in the devices via malware. The malware waits until the victim accesses a key-based security system to collect the sensor data."

After capturing accelerometer, gyroscope and magnetometer data from

the devices and using it to calculate typical distances between and directions of consecutive key entries, Chen's team developed a backward-inference algorithm to predict four-digit PIN codes.

"These predictions were assisted by the standardized layout of most PIN pads and keyboards—plus the knowledge that nearly all users will hit 'enter' as their final significant hand motion after entering a code," she notes.

While some devices proved more secure than others, the algorithm's first guess succeeded an astonishing 80 percent of the time, on average. Within five tries, its accuracy climbed to 99 percent on some devices.

"Further research is needed, and we are also working on countermeasures," concludes Chen, adding that wearables are not easily hackable—but they are hackable.

A paper on the new research, *Friend or Foe? Your Wearable Devices Reveal Your Personal PIN*, received the Best Paper Award at the ACM Conference on Information, Computer and Communications Security (ASIACCS) in Xian, China in May.

More information: Friend or Foe?: Your Wearable Devices Reveal Your Personal PIN, DOI: 10.1145/2897845.2897847 , dl.acm.org/citation.cfm?doid=2897845.2897847
PDF:
personal.stevens.edu/~ychen6/papers/Friend%20or%20Foe_Your%20Wearable%20Devices%20Reveal%20Your%20Personal%20PIN.pdf

Provided by Binghamton University

Citation: Your smartwatch is giving away your ATM PIN (2016, July 6) retrieved 25 April 2024 from https://phys.org/news/2016-07-smartwatch-atm-pin.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.