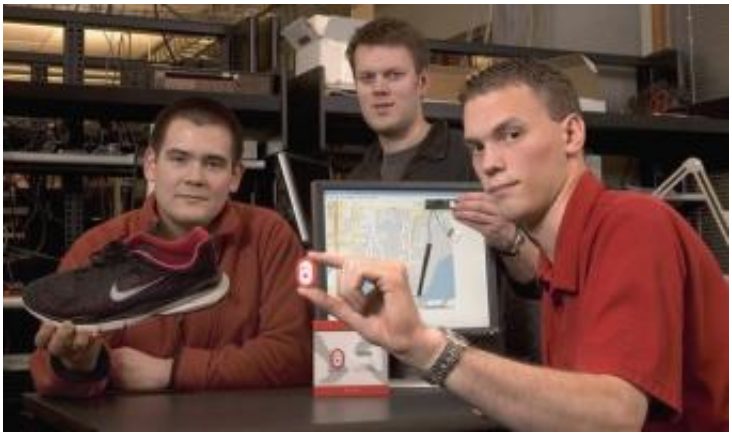
Nike+iPod Sport Kit raises privacy concerns

November 30 2006



Yoshi Kohno, Carl Hartung and Scott Saponas (l-r) with devices they built to pick up on the Nike+iPod. Credit: Mary Levin, UW News and Information

This holiday season, gift-givers may unwittingly give their favorite athlete a workout accessory that can double as a tracking device. Researchers in computer science and engineering at the University of Washington say there are serious privacy breaches posed by the gadget, which is marketed to runners but may be equally attractive to stalkers and thieves.

"It is easy for someone to use the Nike+iPod as a tracking device," says Scott Saponas, a doctoral student in computer science and lead author of a technical report posted online at www.cs.washington.edu/research/systems/privacy.html on Nov. 30. "It's an example of how new gadgetry can erode our personal privacy."

The researchers suggest that people who own a Nike+iPod Sport Kit turn it off when they're not exercising so that it stops emitting signals.

Saponas is an avid runner and had originally bought the device to use in his workouts, before he started wondering about potential security risks. Now, he and his colleagues have built a range of low-cost devices that use information from his Nike+iPod to monitor his whereabouts. Other researchers on the report are UW graduate students Jonathan Lester and Carl Hartung, and Yoshi Kohno, assistant professor of computer science and engineering.

Since its August release, retailers have sold more than 450,000 Nike+iPod Sport Kits, according to industry publication AppleInsider. The $29 item consists of two parts. One piece is a chip the size of a dinner mint that acts as a pedometer, which runners slip into their shoe. The other piece is a receiver that fits into an iPod Nano and stores information beamed from the person's foot. After their workouts, high-tech runners can upload the data and use a Nike software program to track their distance, speed and calories burned.

But it turns out that the sensor in the shoe emits a signal detectable by any compatible receiver within a range of up to 60 feet, long after the workout has ended. The researchers concocted a variety of homemade devices able to pick up the sensor's unique signature. The simplest connects a receiver from the Nike+iPod kit to a laptop's serial port, and the screen displays each device in range. A more sophisticated system uses a matchbox-sized computer with wireless Internet access to record multiple users' whereabouts, send the information to a central server, plot people's locations using GoogleMaps and alert the person doing the tracking with an e-mail or text message. All use the receiver sold with the kit, and each was built for less than $300.

The technical report describes possible scenarios. A thief could track

when people enter or leave their homes. A jealous boyfriend could track a woman's movements, or compare them with the movements of a suspected rival. And although a receiver only picks up the signal when a person is within range, a stalker could hide receivers near a home, a gym and a restaurant, for example, to closely monitor his or her target's movements.

Researchers report that it took them about 10 minutes to figure out how to decode a receiver's unique tag and a few hours to write the code that interprets the sensor data. They estimate that an electronics hobbyist could build a system in a few hours, or at most a weekend. And if somebody posted sensor-scanning code on the Internet, it would be easy for others to build copycat devices.

The team tested the technology to track each other's movements and those of colleagues in the UW computer-science building. Ethical concerns prevented them from trying the device on unsuspecting targets. But because the signal can be picked up silently by any number of receivers, they say there's no way to know whether this spying technique has already been put into practice.

Though it has an off switch, the sensor is sold with the power on. Most users likely wouldn't bother to remove the gadget and turn the power off after each workout. Nike's online documentation reads: "Most Nike+iPod runners and walkers can just drop the sensor in their Nike+ shoes and forget about it."

The report suggests a number of ways the company could have made the device more secure using standard techniques from modern cryptography.

"There's a bigger issue here," says Kohno, the senior author on the paper. "When people buy a toaster, they know it's probably not going to blow

up when they plug it in. But when they buy a consumer device like the Nike+iPod kit, they have no idea whether the device might enable someone to violate their privacy. We need to change that."

Source: University of Washington