PHYS.ORG

Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards

October 18 2011

It's a pattern that no doubt repeats itself daily in hundreds of millions of offices around the world: People sit down, turn on their computers, set their mobile phones on their desks and begin to work. What if a hacker could use that phone to track what the person was typing on the keyboard just inches away?

A research team at Georgia Tech has discovered how to do exactly that, using a smartphone accelerometer—the internal device that detects when and how the phone is tilted—to sense keyboard vibrations and decipher complete sentences with up to 80 percent accuracy. The procedure is not easy, they say, but is definitely possible with the latest generations of smartphones.

"We first tried our experiments with an iPhone 3GS, and the results were difficult to read," said Patrick Traynor, assistant professor in Georgia Tech's School of Computer Science. "But then we tried an iPhone 4, which has an added gyroscope to clean up the accelerometer noise, and the results were much better. We believe that most smartphones made in the past two years are sophisticated enough to launch this attack."

Previously, Traynor said, researchers have accomplished similar results using microphones, but a microphone is a much more sensitive instrument than an accelerometer. A typical smartphone's microphone samples vibration roughly 44,000 times per second, while even newer phones' accelerometers sample just 100 times per second—two full orders of magnitude less often. Plus, manufacturers have installed security around a phone's microphone; the phone's operating system is programmed to ask users whether to give new applications access to most built-in sensors, including the microphone. Accelerometers typically are not protected in this way.

The technique works through probability and by detecting pairs of keystrokes, rather than individual keys (which still is too difficult to accomplish reliably, Traynor said). It models "keyboard events" in pairs, then determines whether the pair of keys pressed is on the left versus right side of the keyboard, and whether they are close together or far apart. After the system has determined these characteristics for each pair of keys depressed, it compares the results against a preloaded dictionary, each word of which has been broken down along similar measurements (i.e., are the letters left/right, near/far on a standard QWERTY keyboard). Finally, the technique only works reliably on words of three or more letters.

For example, take the word "canoe," which when typed breaks down into four keystroke pairs: "C-A, A-N, N-O and O-E." Those pairs then translate into the detection system's code as follows: Left-Left-Near, Left-Right-Far, Right-Right-Far and Right-Left-Far, or LLN-LRF-RRF-RLF. This code is then compared to the preloaded dictionary and yields "canoe" as the statistically probable typed word. Working with dictionaries comprising about 58,000 words, the system reached word-recovery rates as high as 80 percent.

"The way we see this attack working is that you, the phone's owner, would request or be asked to download an innocuous-looking application, which doesn't ask you for the use of any suspicious phone sensors," said Henry Carter, a PhD student in computer science and one of the study's co-authors. "Then the keyboard-detection malware is turned on, and the next time you place your phone next to the keyboard and start typing, it starts listening."

Mitigation strategies for this vulnerability are pretty simple and straightforward, Traynor said. First, since the study found an effective range of just three inches from a keyboard, phone users can simply leave their phones in their purses or pockets, or just move them further away from the keyboard. But a fix that puts less onus on users is to add a layer of security for phone accelerometers.

"The sampling rate for accelerometers is already pretty low, and if you cut it in half, you start to approach theoretical limitations that prevent eavesdropping. The malware simply does not have the data to work with," Traynor said. "But most phone applications can still function even with that lower accelerometer rate. So manufacturers could set that as the default rate, and if someone downloads an application like a game that needs the higher sampling rate, that would prompt a permission question to the user to reset the accelerometer."

In the meantime, Traynor said, users shouldn't be paranoid that hackers are tracking their keystrokes through their iPhones.

"The likelihood of someone falling victim to an attack like this right now is pretty low," he said. "This was really hard to do. But could people do it if they really wanted to? We think yes."

More information: The finding is reported in the paper, "(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers," and will be presented Thursday, Oct. 20, at the 18th ACM Conference on Computer and Communications Security in Chicago.

Provided by Georgia Institute of Technology

Citation: Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards (2011, October 18) retrieved 24 April 2024 from https://phys.org/news/2011-10-iphone-spiphone-smartphones-accelerometer-track.html