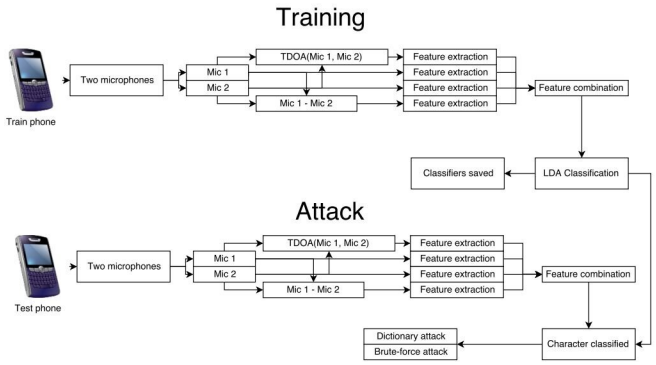
When smartphone finger taps can lead to side channel attack

7 June 2019, by Nancy Cohen



Attack pipeline. Credit: arXiv:1903.11137 [cs.CR]

You type, hacker deciphers, your password is doomed. That is the grim scenario being discussed in a paper that is now on arXiv. "Hearing your touch: A new acoustic side channel on smartphones," is by authors Ilia Shumailov, Laurent Simon, Jeff Yan and Ross Anderson.

What goes on in the theft process in this manner? Short and simple, sound waves emanating from your typing on a phone are decoded. They evaluated the effectiveness of the attack with 45 participants on an Android tablet and an Android smartphone.

Buster Hein in *Cult of Mac* said with sound waves traveling through the screen and the air to the phone's mic, the algorithm predicts where certain vibrations come from.

The researchers said, "by recording audio through the built-in microphone(s), a malicious app can infer text" as the user enters it on his or her device. The team successfully recovered 27 out of 45 passwords on a phone, and 19 out of 27 passwords on a tablet, via typing vibrations.

They designed a machine-learning algorithm able to decode vibrations for keystrokes. *The Washington Post*: "Among a test group of 45 people across several tests, the researchers could correctly replicate passwords on smartphones seven times out of 27, within 10 attempts. On tablets, the researchers achieved better results, nailing the password 19 times out of 27 within 10 attempts."

Really, a hacker can steal your password just by listening to you type? Ian Randall in *Daily Mail* had more about this "machine-learning algorithm." He said it was built to try to match each vibration to a particular point on the devices' screen where the users had touched the on-screen keyboard while typing or entering a password.

The authors themselves explained what was going on: "When a user taps the screen with a finger, the tap generates a sound wave that propagates on the screen surface and in the air. We found the device's microphone(s) can recover this wave and 'hear' the finger's touch, and the wave's distortions are characteristic of the tap's location on the screen."

The result: by recording audio through the built-in microphone, a malicious app can infer text as the user enters it on his or her device.

For their experiment, they used phones and a tablet. There were 45 participants in a real-world environment. And, when they say real-world, they really mean real-world:

"We conducted the experiments outside of the lab environment in order to simulate real- life conditions more closely, thereby improving the validity of the study."

The participants performed in three different places: 1) in a common room, where people chat and occasionally a coffee machine makes some drink

with loud sounds; 2) in a reading room where people type or speak in a semi-loud voice; and 3) in the library where there are a lot of clicking sounds from laptops. All three places had ambient noise coming in from windows left open.

What did the authors recommend as safeguards and solutions?

The authors said, "Mobile devices may need a richer capability model, a more user-friendly notification system for sensor usage and a more thorough evaluation of the information leaked by the underlying hardware."

Elsewhere in the discussion, they explored various options, and one of them was to offer "a properly-engineered PIN entry facility, which when called by one application would temporarily blank, and/or introduce noise into, the microphone channel seen by other apps. This approach should logically be extended to other sensors that can be used to harvest PINs via side-channels such as the accelerometer, gyro and camera."

They also mentioned for the OS to introduce timing jitter, or decoy tap sounds, into the microphone data stream. This would hinder an attacker aiming to identify tap locations.

"As the taps themselves are pretty unnoticeable for humans, this should not disturb applications that run in the background and collect audio with user consent."

At the application level, they said, "an app might itself introduce false tap sounds into the device, in order to jam and confuse any hostile apps that happen to be listening." Tactical jamming, they said, was a low-cost countermeasure.

More information: Hearing your touch: A new acoustic side channel on smartphones, arXiv:1903.11137 [cs.CR]
arxiv.org/abs/1903.11137

Research poster: www.cl.cam.ac.uk/~is410/Poster … ing_touch_poster.pdf

APA citation: When smartphone finger taps can lead to side channel attack (2019, June 7) retrieved 20 June 2019 from https://techxplore.com/news/2019-06-smartphone-finger-side-channel.html