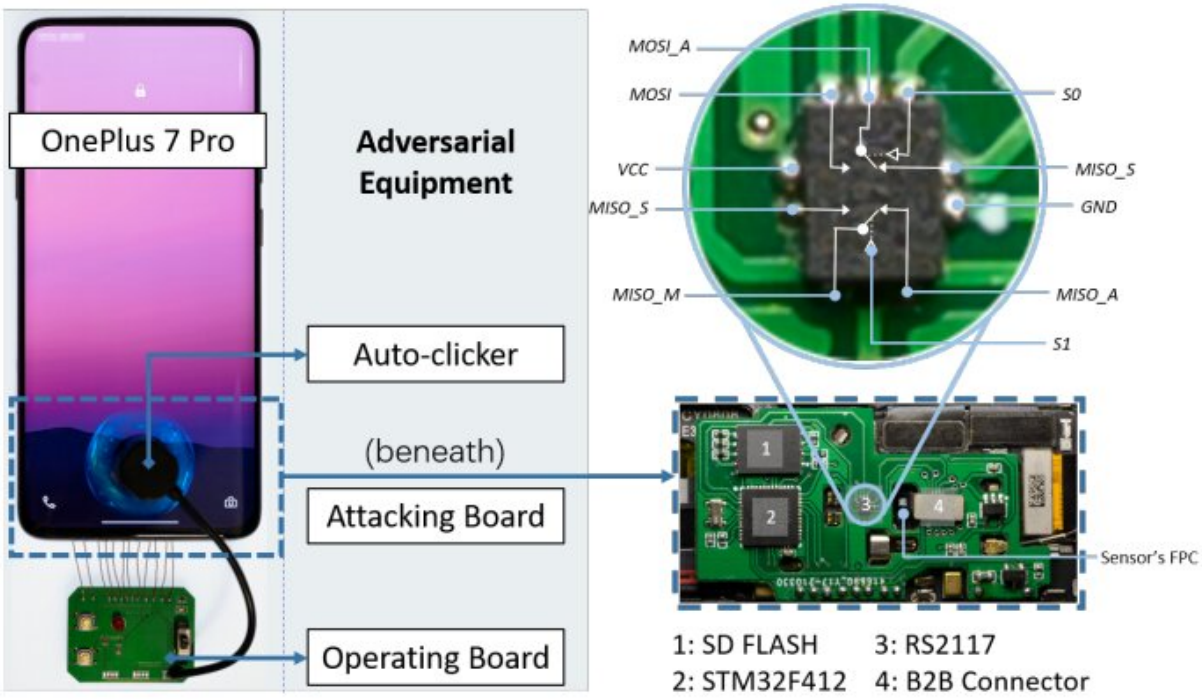
Brute-force test attack bypasses Android biometric defense

May 22 2023, by Peter Grad



Example of implementing automatic fingerprint bruteforce attack, which uses a suppressible attacking board, a hardware auto-clicker, and an optional operating board. Credit: *arXiv* (2023). DOI: 10.48550/arxiv.2305.10791

Chinese researchers say they successfully bypassed fingerprint authentication safeguards on smartphones by staging a brute force attack.

Researchers at Zhejiang University and Tencent Labs capitalized on vulnerabilities of modern smartphone fingerprint scanners to stage their break-in operation, which they named BrutePrint. Their findings are published on the *arXiv* preprint server.

A flaw in the Match-After-Lock feature, which is supposed to bar authentication activity once a device is in lockout mode, was overridden to allow a researcher to continue submitting an unlimited number of fingerprint samples.

Inadequate protection of biometric data stored on the Serial Peripheral Interface of fingerprint sensors enables attackers to steal fingerprint images. Samples also can be easily obtained from academic datasets or from biometric data leaks.

And a feature designed to limit the number of unsuccessful fingerprint matching attempts—Cancel-After-Match-Fail (CAMF)—has a flaw that allowed researchers to inject a checksum error disabling CAMF protection.

In addition, BrutePrint altered illicitly obtained fingerprint images to appear as though they were scanned by the targeted device. This step improved the chances that images would be deemed valid by fingerprint scanners.

All Android devices and one HarmonyOS (Huawei) device tested by researchers had at least one flaw allowing for break-ins. Because of tougher defense mechanisms in IOS devices, specifically Apple iPhone SE and iPhone 7, those devices were able to withstand brute-force entry attempts. Researchers noted that iPhone devices were susceptible to CAMF vulnerabilities, but not to the extent that successful entry could be achieved.

To launch a successful break-in, an attacker requires physical access to a targeted phone for several hours, a printed circuit board easily obtainable for $15, and access to fingerprint images.

Fingerprint databases are available online through academic resources, but hackers more likely will access massive volumes of images obtained through data breaches. Law enforcement agencies from 18 countries announced last month that they had shut down a major illegal marketplace for stolen identities. Genesis Market, which stocks digital fingerprints and other private digital data, was offering up to 80 million credentials for sale.

Biometric security is a leading security measure on digital devices. Fingerprint and facial recognition are considered preferable to passwords and PIN numbers since then are harder to fake, easier to use (no memorization required) and cannot be transferred among users.

But aside from the potential of cyberattacks such as BrutePrint, there are other problems surrounding fingerprint identification. Forged fingerprints and residual prints left behind on device screens are an entryway to abuse.

One unlucky drug dealer from Liverpool found out the hard way that fingerprints can be identified in unexpected ways. After posting a picture of himself holding a package of one of his favorite foods, Stilton cheese, in his hand, police spotted the photo, tracked his fingerprints and arrested him after linking the prints to crimes.

Biometrics has a grip on cinema, too. Movies such as "The Spy Who Dumped Me," "The Equalizer 2" and "Death Wish" humorously—and ghoulishly—show people using, and even cutting off, fingers from dead people to access phones.

Of course, that works only in Hollywood. Today's fingerprint scanners not only confirm skin patterns but also detect and require the presence of living tissue residing in the lower layers of skin as well as slight electric charges that run through the bodies of all of us, but only when we're alive… and our fingers are attached.

The Zhejiang University researchers said "the unprecedented threat" they uncovered requires bolstering of OS protections and greater cooperation between smartphone and fingerprint sensor manufacturers to address existing vulnerabilities.

More information: Yu Chen et al, BrutePrint: Expose Smartphone Fingerprint Authentication to Brute-force Attack, *arXiv* (2023). DOI: 10.48550/arxiv.2305.10791