Fingerprint design issues on Android devices in spotlight

August 6 2015, by Nancy Owano

Image credit: Wikimedia.

Password leaked? Not the end of the world. Among the external patches and fixes, you can just change it. Fingerprints leaked? Not so good. These stay as your life's records. Small wonder that among presentations at the 2015 Black Hat security conference, one of the talks is particularly interesting: how attackers can steal fingerprints from Android phones.

A *ZDNet* report about the talk remarked : "Fingerprints might be commonplace in mobile payments and unlocking devices, but they have been used more in the past five years also for identity, immigration, and

for criminal records." Zack Whittaker in *ZDNet* reported that Tao Wei and Yulong Zhang, two researchers from FireEye, were at the conference to discuss various ways to extract user fingerprints.

Their presentation, "Fingerprints on Mobile Devices: Abusing and Leaking," reviewed current Android fingerprint frameworks. Tao Wei and Yulong Zhang said their goal at the presentation was to provide a security analysis of popular mobile fingerprint authentication/authorization frameworks and discuss the design problems.

The two Black Hat presenters had a sobering assessment of fingerprints as part of mobile devices. They remarked how it will be even "a disaster if the attackers can remotely harvest fingerprints in a large scale."

Those problems, they said, included "the confused authorization attack that enables malware to bypass pay authorizations protected by fingerprints and "pre-embedded fingerprint backdoors." The two researchers said they also aimed to provide suggestions for vendors and users to better secure the fingerprints.

If a device maker does not fully lock down the sensor, according to one explanation, a hacker may acquire a fingerprint image. Also, some devices' sensors are only guarded by "system" privilege instead of root, making the target easier, explained Whittaker. Once the attack is in place, he added, "the fingerprint sensor can continue to quietly collect fingerprint data on anyone who uses the sensor."

Sean Buckley in *Engadget* said that affected devices "simply don't do enough to lock down their fingerprint scanners, often leaving them at the mercy of higher level system privileges."

Matt Hanson in *TechRadar* had some good news to report about this :

For one, this, he said, should be "a relatively easy fix."

Adding encryption to fingerprint data on Android devices will keep the information secure, he said. Also, Hanson said that manufacturers were aware of the flaw and have started to update their software. Hanson also noted that Android does not yet officially support fingerprints.

Sean Buckley in *Engadget* similarly reported that device manufacturers were on the case: "notified vendors have already issued patches for the exploit."