5 ways hackers 'beat' fingerprint scanner

Fingerprint scanners are a good defense against hackers, but that doesn't mean they can't be broken.

Fingerprint scanners are a good defense against hackers, but that doesn't mean they can't be broken. In response to the proliferation of devices that support fingerprint scanning, hackers are improving the techniques to unlock this defense line.

Here are some ways that hackers can 'beat' the fingerprint scanner.

How can hackers "take down" fingerprint scanners?

1. 1. Use masterprint
2. 2. Collect unsecured images
3. 3. Use fake fingerprints
4. 4. Exploiting software vulnerabilities
5. 5. Reuse the leftover fingerprint section

1. Use masterprint

Just like a physical multipurpose lock can open any lock, masterprint can also pass fingerprint scanners.

Hackers can use masterprint to access devices that use poor scanning. Reliable scanners will block masterprint, but an inferior scanner (found in mobile phones, for example) may not be very rigorous. Thus, masterprint is an effective way for hackers to infiltrate devices with poor defensive capabilities.

How to avoid attacks with masterprint

The best way to avoid this type of attack is to use a reliable fingerprint scanner. Masterprint exploits the inaccurate scanner to confirm identity.

Before putting too much faith in the fingerprint scanner, do some research on it. Ideally, find False Acceptance Rate (FAR) statistics - Rate of tolerance. The FAR percentage is an opportunity for an unapproved fingerprint to have access to the system. The lower this percentage, the more likely the fingerprint scanner you are using will detect the masterprint.

2. Collect unsecured images

If hackers hold your fingerprint image, that means they hold the key to entering the fingerprint scanner you are using. People can change passwords, but fingerprints do not. The permanence of fingerprints makes them a valuable tool for hackers who want to bypass the fingerprint scanner.

Unless you are a very famous or influential person, the hacker will easily get everything you touch to create a masterprint from your fingerprint. It is likely that hackers will target devices or scanners in the hope that contains your raw fingerprint data.

For a scanner to identify you, it needs a basic image of the fingerprint. During the setup process, you provide a fingerprint template for the scanner and it will save the image to memory. Then, the scanner will 'recall' this image every time you use it, to ensure the fingerprint on the finger is scanned in the same way as the sample fingerprint provided during the setup process.

Unfortunately, some devices or scanners save this image without encryption. If hackers have access to memory, they can take photos and collect your fingerprint details easily.

How to avoid this attack?

To avoid this type of attack, consider the security of the device you use. A reliable fingerprint scanner encrypts image files to prevent bad guys from getting your biometric information.

Check the fingerprint scanning technique used to see if it stores the fingerprint image properly. If you find that the device doesn't save fingerprint images safely, you should stop using it immediately. You should also consider deleting the image file so that hackers cannot copy it.

3. Use fake fingerprints

If hackers cannot get an unsecured fingerprint image, they can choose to create a fake fingerprint instead. This trick involves holding target fingerprint templates and re-creating them to defeat the scanner.

A few years ago, The Guardian reported on how a hacker used to replicate the fingerprint of the German defense minister!

There are many different ways for hackers to turn collected prints into a physical fingerprint. They can make a wax or wooden copy of a hand, print it on a special paper, use silver ink, and then use it on a scanner.

How to avoid this attack?

Unfortunately, this is an attack that you cannot directly prevent. If a hacker intends to invade the fingerprint scanner you're using and they find ways to get your fingerprints, you can't do anything to prevent them from creating a fake model.

The key to defeating this attack is to prevent getting fingerprints in the first place. You don't have to wear gloves all the time as a criminal, but it's good to be aware of places where your fingerprint details might leak. Recently, there have been many reports of leaking sensitive information databases, so this is worth considering.

Be sure to provide your fingerprint details only for reliable devices and services. If an inferior security service violates the database and does not encrypt the fingerprint image, hackers will take advantage of this to attack the fingerprint scanner you are using.

4. Exploiting software vulnerabilities

Some password managers use fingerprint scanning to identify users. Although this is useful in helping keep passwords safe, the effectiveness also depends on the security of the password management software. If the program is not effective against attacks, hackers can exploit this vulnerability to get fingerprint information.

This issue is similar to the security upgrade at the airport. Metal detectors, security personnel and cameras are located everywhere to observe every corner of the airport. However, if there is a long-forgotten 'back door' that allows bad guys to sneak in, all of those additional security measures won't help!

Recently, **Gizmodo.com** reported a vulnerability to Lenovo devices, in which a fingerprint-enabled password manager has hard-coded password (a plain text password inside the source code). If a hacker wants to have access to the password manager, he can pass the hard-coded password scanner, making the scanner useless!

How to avoid this attack?

Usually, the best way to avoid this type of attack is to buy popular products and get positive feedback from users. Although there are exceptions (for example, a big name like Lenovo has been attacked, as mentioned above).

Thus, even if you only use hardware manufactured by reputable brands, it is still important to keep the security software up to date to fix any problems found later.

5. Reuse the leftover fingerprint section

Sometimes, a hacker doesn't need to do any advanced techniques to get fingerprints. They just need to use the remainder from the previous fingerprint scan to bypass the security layer.

You leave your fingerprints on objects when using them and fingerprint scanners are no exception. Any sample harvested from the scanner is guaranteed to be similar to the unlocked fingerprint pattern. This situation is like forgetting the key in the lock after opening the door.

Even then, a hacker may not need to copy fingerprint samples from the scanner. The smartphone detects fingerprints by emitting light on the finger, then recording how the light shines back into the sensor. **Threatpost.com** reported on how hackers could trick this scanning method into accepting residual fingerprints.

Researcher Yang Yu tricked a smartphone fingerprint scanner into accepting the remaining fingerprint, by placing a fuzzy reflective surface on the scanner. The reflective surface trick the scanner into believing that the leftover fingerprint is a real finger and allows phone access.

How to avoid this attack?

This way of avoiding attacks is very simple. Please wipe the device surface after fingerprint scanning! The scanner retains fingerprints after you use them and the best way to ensure safety is to clean it. Doing so will prevent hackers from using the device you own to fight against yourself.

Although fingerprint scanners are a useful tool, they are not absolutely safe! If you are using a fingerprint scanner, be sure to take safety measures with it. Fingerprints are the key to all the scanners you use, so be careful with your biometric data.

Wish you find a suitable solution!

on tips and guides. Thank you for reading and for following us regularly.