SySS
THE PENTEST EXPERTS.

IT SECURITY KNOW-HOW

Philipp Buchegger

HACKING FINGERPRINT READERS WITHOUT MAKING A MESS

Using tin foil instead of human skin

November 2018

Schaffhausenstraße 77, 72072 Tübingen, Germany

+49 (0)7071 - 40 78 56-0

info@syss.de

www.syss.de

1 Introduction

Hacking fingerprint sensors as biometric authentication mechanisms has been possible for many years [1]. The challenge is getting a neat copy of the fingerprint. As yet, the actual fake fingerprint has been created with a skin-like material like wax, wood glue or silicone. With a scientific view on the used sensors of mobile devices, laptops and burglar alarm, just using tin foil should do it.

2 Fingerprint Sensors

How do fingerprint sensors work? They use matrix of tiny plate capacitors which sense the change of the surrounding dielectric material. A dielectric is an electrical insulator that can be polarized by an applied electric field. But wait, aluminium is a metal which can conduct currents! That is correct, but the surface of tin foil consists of aluminium oxide which is an excellent insulator. So, we just need to get the material into the right shape.

In order to make the fake fingerprint work in the real world, it is measured for similarity up to a specific threshold. By applying more (erroneous) information to the device, the threshold is lowered. For example, when learning new fingerprints, it is possible to use to different fingers and save it as one fingerprint on the device. After successful training, both fingers can be used to unlock the device.

This means that our copy only has to be close to the original and give similar results to the sensor. Since the dielectric constants of human skin and tin foil differ by more than a factor of 6 (70 vs. 10.8), only the relative capacity changes matter.

3 Creating the Fake Fingerprint

An adequate photograph can be taken with a decent smart phone camera (the images shown in this paper were taken with an iPhone 5S of 2013). The processing of the image to a high-contrast and inverted image was handled with built-in graphic utilities of a Windows XP system. Since custom PCBs (polychlorinated biphenyls) can be ordered online from several services, you do not need to etch and process a PCB by yourself anymore. Fingerprints, however, are not part of the normal PCB layout, thus processing and etching the PCB was performed manually in this proof of concept. We used a laser printer with 1200 dpi resolution on a clear film. For better contrast, two copies of the printed clear film were put on top of each other. The PCB was developed manually, the etching was done with a self-built computer-controlled etching machine with human visual control.

Figure 1: Fingerprint on an Apple iPhone 6S

In order to get a good result onto the PCB, the fingerprint has to be idealized, i.e. the texture needs to be coarse enough for the ferric chloride to react in order to remove the copper.

The image has to be inverted for the photoresist and mirrored, so that the created sample represents a copy of the original. Tin foil offers the advantage that the opposite site can also be used. In case an excellent digital version of the fingerprint exists (for example, as done by governments with their fingerprint sensors at the border), creating such a sample should not be a big deal.

When extracting the partial fingerprint directly from the sensor, only a fragment will be necessary to unlock the device since only this certain part of the fingerprint is needed for authentication.

Figure 2: Digitally processed fingerprint

The copy of the fingerprint should have the same dimensions as the original. We managed to get a working copy at our first try. In most cases, a fingerprint has to be edited manually because even on plain and clean surfaces such as glass, not all areas of a fingerprint will be perfect. Editing the master fingerprint took approximately one hour.

Figure 3: Etched fingerprint

Figure 4: Fingerprint on tin foil

A pipe wrench with some foam material was used to apply enough pressure. After several tries, even pressing with fingers also works.

4 Conclusion

Creating fake fingerprints does not have to end up in a complete mess. It is possible to create fingerprint samples from a solid master sample without glue or graphite spray. Aluminium foil or tin foil has the advantage that it can be given the desired shape by simply pressing.

After two evenings of intensive work, we successfully unlocked all tested smartphones and laptops. This technique works for all iOS and Android devices with fingerprint sensors or on laptops requiring a fingerprint for Windows Hello.

The following devices were successfully tested: Apple iPhone 5S, Apple iPhone 6, Apple iPhone 6S, Google Nexus 5X, Samsung Galaxy S5 Mini, Samsung Galaxy S6 Edge, Samsung Galaxy S7 Edge, HP Elitebook X360, Apple MacBook Pro (2018).

References

[1] Starbug, Chaos Computer Club hackt Apple TouchID, https://www.ccc.de/updates/2013/ccc-breaks-apple-touchid, 2013 1

THE PENTEST EXPERTS

SySS GmbH 72072 Tübingen Germany +49 (0)7071 - 40 78 56-0 info@syss.de

WWW.SYSS.DE