INVESTIGATION INTO PHYSICAL METHODS TO BYPASS FINGERPRINT SENSORS ON MOBILE DEVICES

PRIFYSGOL BANGOR UNIVERSITY

HARI ROBERTS SUPERVISOR DR. CAMERON C. GRAY

Introduction

In recent years, fingerprint sensors have been increasing in popularity[1] tremendously and in particular with smartphones. One reason that fingerprint sensors are so popular is that they increase security [2] because fingerprints are unique for each person and are hard to fake.

My aim with this thesis is to see how difficult it is to bypass a fingerprint sensor. This is to improve personal practise with the security of fingerprint sensors. I will gather relevant information and develop various methods to bypass a capacitive fingerprint sensor on a mobile device.

Experiment Design

There are four main experiments that I will conduct on a fingerprint sensor; [3]

- PVA glue in a wax mould
- PVA glue in chewing gum
- Gelatine in a clay mould
- An image of a fingerprint

One goal of this project was to create working artificial fingerprints with easy to find materials. This is to prove anyone could create working artificial fingerprints if they intended to.

Results

Only 2/15 experiments have worked. The success rate to bypass a mobile phones capacitive sensor is therefore 13.3%. This shows under the right circumstances, fingerprint sensors can be bypassed with an artificial fingerprint.

The two samples that did manage to bypass a capacitive sensor were PVA glue on a wax mould. Only this experiment managed to work out of the 4 conducted.

Future work

This project has only tested the different experiment on a capacitive sensor on an iPhone 5s. These experiments should be tested on other capacitive fingerprint sensors for example another mobile device or even a different device.

These experiments could have been conducted on different types of fingerprint sensors including an optical sensor and an ultrasonic sensor.

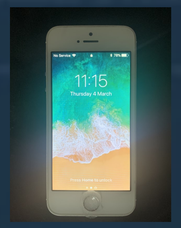
Experiment - PVA glue in a wax mould

Melting wax in a cup and pan.

Wax with a finger pressed into the mould.

Wax mould filled with PVA glue.

The artificial fingerprint made from PVA glue.



The device locked before pressing the fingerprint.

The unlocked phone after pressing the fingerprint.

References

[1] A. Ross and A. Jain, “Biometric sensor interoperability: A case study in fingerprints,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 3087, no. May, pp. 134–145, 2004, doi: 10.1007/978-3-540-25976-3_13.

[2] S. Hosseini, “Fingerprint vulnerability: A survey,” *2018 4th Int. Conf. Web Res. ICWR 2018*, no. December, pp. 70–77, 2018, doi: 10.1109/ICWR.2018.8387240.

[3] A. Wiehe and T. Søndrol, “Attacking Fingerprint Sensors,” *Gjøvik Univ. …*, pp. 1–26, 2004, [Online]. Available: http://www.skarderud.net/articles/attacking_fingerprint_sensors.pdf.