Miercom

The leading edge in security information.

CrucialTec Heart Rate Monitoring (HRM) & Body Impedance Analysis (BIA)

The CrucialTec Heart Rate Monitoring (HRM) & Body Impedance Analysis (BIA) provides anti-spoofing protection for fingerprint recognition sensors on leading mobile devices and operating systems.

The CrucialTec HRM and BIA solution was recently evaluated by Miercom for the performance of its biometric anti-spoofing fingerprint solution. Eight different mobile phone models were locked using fingerprints from both male and female users, ranging for age twenty to fifty years old. Each participant had their fingerprint copied using multiple methods. The fake fingerprints were used in an attempt to unlock the mobile phone by spoofing the default print scanner sensor. Any successful exploit methods and vulnerable phone models were recorded. The CrucialTec HRM and BIA solution was then introduced and tested for its ability to detect the same set of fake fingerprints. Fraudelent fingerprints were detected within two seconds.

> ***The CrucialTec HRM and BIA defeated fingerprint spoofing that was proven to compromise fingerprint sensors of the leading mobile device vendors and models.***

CrucialTec Anti-spoof Protection

Mobile Device Brand	Mobile Exploit (ME) Used	Detected by Default	Detected by CrucialTec
Google	ME 1	✗	✓
HTC	ME 2	✗	✓
Huawei	ME 3	✗	✓
iPhone	ME 4	✗	✓
Meizu	ME 5	✗	✓
Samsung	ME 6	⚠	✓

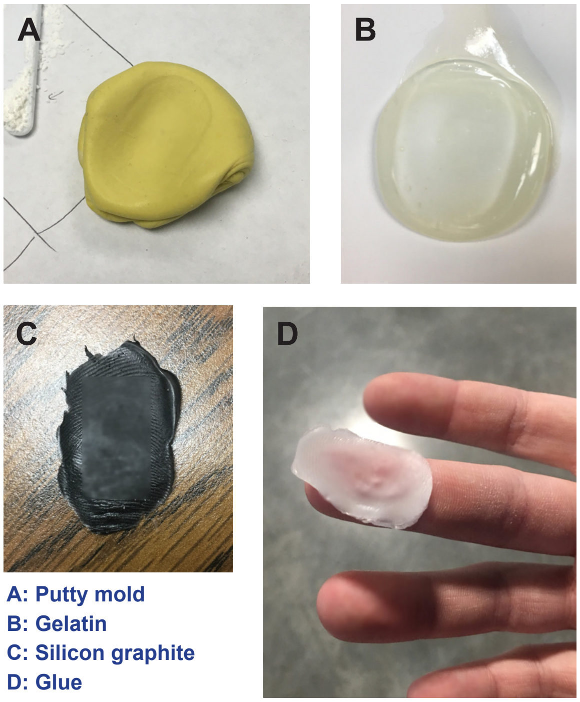
All brands were accessed using one of the six mobile exploit test methods of fingerprint spoofing. CrucialTec was able to detect and deny access for each mobile device with its novel HRM and BIA sensor module.

Copyright © 2017 Miercom

Fingerprint Spoofing

In order to trick each phone's default fingerprint scanning sensor, the forged fingerprint required two things: clarity and consistency. A mold or picture was taken of the finger being copied. Different approaches were taken to recreate the captured prints. A few notable methods are described below.

Glue was heated, applied to the finger, cooled and peeled as a thin printed copy of the person's finger. **Gelatin** mix is heated, poured into the putty mold of the finger and chilled to produce a hard fake fingerprint. **Silicon and graphite** were mixed to form a solution, poured into the putty mold and refrigerated until firm. **Conductive ink** was used to print a picture of the fingerprint on transparent, plastic sheets.



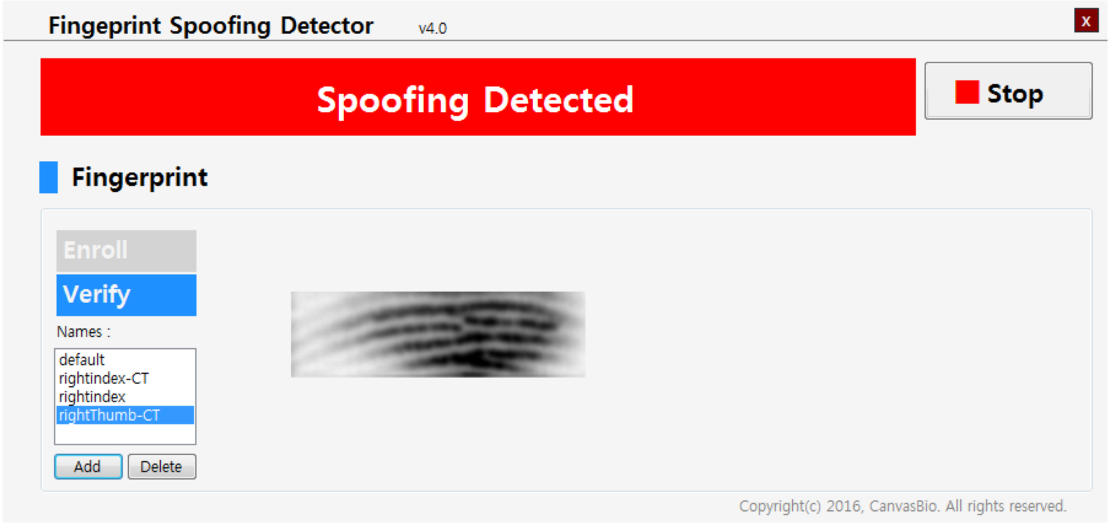
A: Putty mold
B: Gelatin
C: Silicon graphite
D: Glue

Without elaborating on which of these methods and other techniques worked the best, we were able to successfully falsify the fingerprint of each participant and gain access into a phone within seconds.

CrucialTec HRM & BIA Module

The CrucialTec module was placed on its proprietary test board and connected to a PC via USB. After installing a test program, each participant's actual fingerprint is enrolled. These fingerprints are then verified and used to test the fake fingerprint attempts. Test programs evaluated each fingerprint attempt using its HRM detection and BIA detection separately.

Each phone is tested side-by-side with the CrucialTec module to compare whether access was granted and, if not, how much time passed until detection.



Fingerprint Spoofing Detector v4.0

Spoofing Detected

Fingerprint

Names :

default
rightindex-CT
rightindex
rightThumb-CT

Copyright(c) 2016, CanvasBio. All rights reserved.

CrucialTec's combination of trackpad and fraud detection software was the only product successful in detecting fraudelent fingerprint entries attempting to match the real, verified fingerprints of each user.

Bottom Line

Mobile devices are increasingly used for business and bank transactions. Spoofing a fingerprint gives access to both personal and organizational data. An unlocked phone acts as a key to photographs, contacts, account numbers, payment accounts and confidential company files. While a fingerprint is a security measure, it can easily be exploited within seconds.

The CrucialTec solution provides two detection mechanisms: heart rate and body impedance. Its proprietary trackpad and corresponding software collect and record physiological data of each individual user. Fingerprint patterns and biometric measurements are used to verify the authorized user and to combat fraudelent physical access to the most popular mobile devices around the world. Securing mobile devices protects end users, networks and enterprises from malicious activity.

The CrucialTec Heart Rate Monitor and Body Impedance Analysis solutions were recently evaluated by Miercom for high-level detection of spoofed fingerprint access into mobile devices. CrucialTec's module combines these solutions into a comprehensive security measure against unauthorized phone access using heart rate and body impedance, unique to each individual. The Certified Secure certification is presented to CrucialTec in recognition of proven superior biometric performance as one of the most robust and secure anti-spoofing solutions tested.

About Miercom's Product Testing Services

Miercom has published hundreds of network and security product comparison analyses in prominant trade periodicals and other publications. Miercom's reputation as the leading independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

www.Miercom.com

Copyright © 2017 Miercom