Venenscanner akzeptiert Wachsattrappe

Chaos Computer Club trickst biometrisches Verfahren simpel aus

Zwei Hacker haben mit wenig Aufwand Finger- und Handvenenscanner ausgetrickst. Mit einem Raspi-Kameramodul im Händetrockner konnten sie sogar unbemerkt Venen-Aufnahmen machen, mit denen sie biometrische Zugangssysteme täuschten.

Von Arne Grävemeyer

Biometrische Venenerkenner scannen das individuelle Muster der verzweigten Venen eines Fingers oder einer Hand. Anhand dieser Muster können sich Personen authentifizieren, etwa an Geldautomaten oder bei der Zutrittskontrolle zu Hochsicherheitsbereichen. Zwei Sicherheitsforscher haben im Dezember auf dem 35. Chaos Communication Congress in Leipzig live demonstriert, wie sie mit einer Handattrappe aus Wachs ein PalmSecure-System von Fujitsu täuschen konnten. Ebenso war es ihnen gelungen, Venenscanner des zweiten großen Anbieters Hitachi zu überlisten.

Wie die beiden Hacker Jan Krissler alias Starbug und Julian Albrecht berichten, besorgten sie sich zunächst handelsübliche Venenscanner von Fujitsu und Hitachi und untersuchten, in welcher Form die gescannten Venenbilder auf diesen Systemen vorliegen. Sie erkannten, dass mit einfachen digitalen Spiegelreflexkameras, aus denen allerdings die Infrarotfilter entfernt werden müssen, sehr gute Venenbilder geschossen werden können. Das ist möglich, da venöses Blut Infrarotlicht recht gut absorbiert und daher in Aufnahmen deutlich dunkel hervortritt. So gelangen mit Blitz oder angestrahlt von einem Infrarot-Handstrahler nutzbare Handvenen-Aufnahmen sogar aus fünf bis sechs Metern Entfernung. Die Hacker erzielten ebenfalls brauchbare Aufnahmen in einem Händetrockner, den sie mit Infrarot-LEDs und einem Raspberry-Pi-Kameramodul ausgerüstet hatten. „Dort halten die Menschen ihre gewaschenen Hände hinein und bewegen sie auf und ab – ideal für unsere Aufnahmen“, berichtet Albrecht.

Lasertoner anstelle von Blutgefäßen

Nun folgte die Herstellung einer Attrappe. In wenigen Bearbeitungsschritten erhöhten die beiden Sicherheitsforscher auf ihren Venenfotos den Kontrast und filterten Rauschen heraus. Mit einem einfachen Python-Programm standardisierten sie diesen Arbeitsschritt. Sie erkannten zudem, dass Lasertoner sehr gut von Venenerkennern aufgefasst wird, allerdings ließen diese sich nicht durch einen einfachen Papierausdruck täuschen. Am Ende einiger Versuche stand eine Gießform aus Silikon, in die der Venenausdruck eingelegt und mit einer dünnen Schicht hellroten Bienenwachses abgedeckt wird. Mit derartigen Attrappen kommen die Hacker nach eigener Aussage an neuesten Hardware-Software-Systemen von Fujitsu PalmSecure auf Erkennungsraten von über 95 Prozent. Die reine Herstellungszeit für eine Handattrappe schätzen sie auf 15 Minuten. Mit vergleichbaren Fingerattrappen hatten sie auch Erfolg an Fingerscannern wie VeinID von Hitachi. Hier wird der aufgelegte Finger zur Erkennung mit einer LED-Reihe von hinten durchleuchtet.

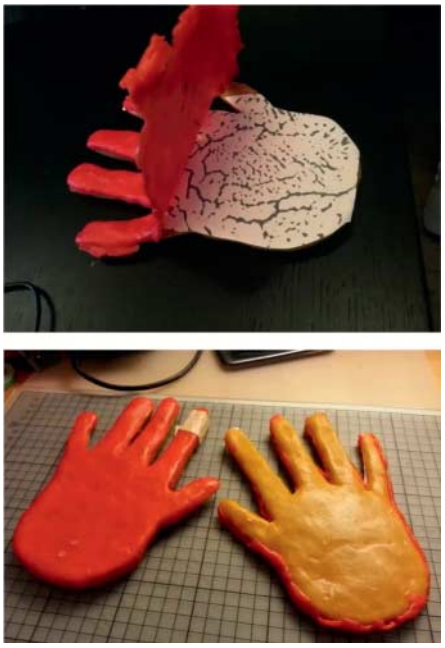

Bild: CCC

In wenigen Minuten gemacht: Ein Venenmuster aus dem Laserdrucker wird in einer Silikongießform mit einer rötlichen Wachsschicht überzogen.

Ihren Hack demonstrierten Krissler und Albrecht vor der Veröffentlichung auch direkt den Herstellerunternehmen. „Wir sind dem CCC aufgrund seiner offenen Kommunikation sehr verbunden“, sagt Fujitsu-Pressesprecher Michael Erhard. Allerdings gibt man sich bei Fujitsu in Deutschland überzeugt, dass es mit dem gezeigten Verfahren nicht möglich ist, eine nach Herstellerempfehlungen implementierte PalmSecure-Installation zu umgehen. Das gelinge nur „unter Laborbedingungen“ in seltenen Fällen. Insbesondere die Möglichkeit des unbemerkten „Venenklaus“ in einem Händetrockner hält man für unrealistisch. Immerhin: Man werde die Erkenntnisse in die kontinuierliche Weiterentwicklung der Fake Object Detection der Venenerkennung einfließen lassen.

Und was ist mit Lebenderkennung, also der Kontrolle, ob das biometrische Merkmal zu einem lebenden Menschen gehört? Die Hacker haben davon nichts bemerkt, obwohl ihre Attrappen keinen Blutfluss simulieren und das dargestellte Venenmuster auch nicht dreidimensional ist. Sie sehen daher einige Möglichkeiten für die Hersteller, ihre Venenerkennung gegen einfache Wachsattrappen abzusichern. Und das wäre sicherlich auch angebracht, denn schließlich finden biometrische Venenerkenner Einsatz als Zugangssysteme nicht nur für Laptops, sondern auch für Hochsicherheitsbereiche an Flughäfen und in Krankenhäusern, in Kernkraftwerken und Banken. Auch der BND setzt im neuen Berliner Hauptquartier Handvenenscanner an den Biometrieschleusen ein. Ein weiteres verbreitetes Einsatzfeld der Venenscanner ist die Kundenidentifikation an Geldautomaten beispielsweise in Japan, Brasilien, Russland, der Türkei und Polen. „Wir haben uns längst einmal einen Praxistest in Polen vorgenommen“, kündigt Krissler an. *(agr@ct.de)* c't