

Schwere Zeiten für falsche Finger

Biometriker erhöhen die Sicherheit von Fingerabdruckscannern

Autor: Ralf Krauter
Erscheinungsdatum: 27. 1. 2006

MANUSKRIFT

Zahlen sie mit EC-Karte oder mit Fingerabdruck? Die Frage klingt ungewohnt, wird in manchem Edeka-Supermarkt aber bereits heute gestellt. Ein Sensor an der Kasse scannt das Rillenmuster auf der Fingerkuppe. Stimmt es mit einem der gespeicherten Datensätze überein, wird der fällige Betrag direkt vom Konto abgebucht – schnell und einfach. Und das ist auch bei tragbaren Computern Trumpf. Vor kurzem brachte ALDI den ersten Volks-Laptop mit biometrischer Erkennung auf den Markt. Passwort zum Einloggen? Überflüssig. Fingerauflegen genügt. Doch während Benutzer den gewonnenen Komfort genießen, sorgen sich Biometrie-Experten um die Sicherheit.

Fingerabdruckscanner haben der boomenden Biometrie-Branche im Jahr 2004 die Hälfte ihres Umsatzes beschert. Doch viele käufliche Sensoren, lassen sich mit gefälschten Fingerabdrücken täuschen. „Das Risiko von Betrügereien wird zunehmen“, prophezeit Professor Davide Maltoni von der Universität Bologna. „Deshalb müssen wir heute schon nach Lösungen suchen, die Fingerabdrucksensoren sicherer machen.“ Der italienische Informatiker hat in seinem Labor eine beachtliche Sammlung falscher Finger. Mehr als hundert Replikate aus Silikon, Latex und Gelatine haben Maltoni und seine Kollegen hergestellt, um für das EU-Projekt Biosec die Sicherheitslücken von Fingerabdrucksensoren zu untersuchen. Sein Fazit: „Professionelle Fälscher können die gängigen Scanner in fast 100 Prozent der Fälle hinters Licht führen.“

Um Betrügern das Leben zu erschweren, soll die nächste Sensorgeneration automatisch erkennen, ob ein Finger echt ist oder nicht. Mögliche Ansätze dazu gibt es viele. Nicht alle halten, was sie versprechen. „Die Lebenderkennung ist nach wie vor ein Problem“, bestätigt der Biometrie-Experte Henning Daum vom Fraunhofer-Institut für graphische Datenverarbeitung in Darmstadt. Die simple Idee etwa, anhand der Temperatur festzustellen, ob der aufgelegte Finger aus Fleisch und Blut ist, klingt bestechend. Doch wie warm ein Finger ist, schwankt je nach Person und Situation beträchtlich. Und ein Fingerabdrucksensor, der den Kunden am Bankautomat nach einer winterlichen Fahrradfahrt abweist, weil sein Zeigefinger zu kalt ist, taugt nicht für den Massenmarkt.

Vielversprechender ist da schon die Idee, mit zusätzlichen Elektroden die elektrischen Eigenschaften der Haut zu vermessen – ein Verfahren, das sich Infineon patentieren ließ. Andere Hersteller tüfteln an Geräten, die testen, ob der aufgelegte Finger durchblutet wird. Eines der derzeit sichersten Verfahren ist die Messung des Blutsauerstoffes: Bei der Pulsoximetrie wird der Finger von oben durchleuchtet. Je

nach Sauerstoffgehalt wird das einfallende Licht dabei unterschiedlich abgeschwächt. Gemeinsames Manko all dieser Verfahren: Sie lassen sich nicht ohne Aufwand in preiswerte handelsübliche Scanner integrieren.

Deshalb favorisiert Davide Maltoni aus Bologna mittelfristig eine andere Lösung. Er hat in einen kommerziellen optischen Fingerabdrucksensor eine elektronische Nase eingebaut, wie sie in der Lebensmittelüberwachung eingesetzt wird. Der zusätzliche Sensorchip riecht, ob ein Finger echt ist. „Wir messen das typische Geruchsmuster eines Fingerabdrucks und unterscheiden es vom charakteristischen Geruch anderer Materialien“, erklärt Maltoni. Bei einer Versuchsreihe mit 30 Studenten konnte er zeigen, dass das Konzept in der Praxis funktioniert. Die elektronische Nase erkannte professionelle Fälschungen in 9 von 10 Fällen. Ein bedeutender Fortschritt, findet Maltoni: „Verglichen mit herkömmlichen Scannern reduziert sich die Fehlerrate um 90 Prozent.“ Ähnlich gute Resultate mit handelsüblichen Scannern erzielte kürzlich auch die US-Forscherin Stephanie Schuckers von der Clarkson Universität in Potsdam, New York. Sie verwendete ebenfalls einen kommerziellen optischen Sensor, erweiterte dessen Mustererkennungssoftware aber um einen Algorithmus, der die Ausbreitung des Schweißes analysiert, der aus den Hautporen austritt. Bei Tests mit 60 falschen Fingern war auch hier nur noch einer von zehn Täuschungsversuchen erfolgreich.

Parallel zu ihrem riechenden Detektor arbeiten auch die italienischen Informatiker um Davide Maltoni an einem Ansatz, der allein auf verbesserte Software setzt: Sie wollen die Verformung der Fingerkuppenhaut unter die Lupe nehmen. Dazu muss die zu identifizierende Person ihren Finger auf der Sensoroberfläche drehen. Weil Haut besonders elastisch ist, ändert sich das Rillenmuster anders als bei einem Replikat. „Wenn das funktioniert, wäre es das Aus für falsche Finger aus Gummi und Kunststoff“, sagt Fraunhofer-Experte Henning Daum. Doch Praxistests stehen noch aus. Welches Verfahren am Ende das Rennen machen wird ist offen.

Henning Daum, der im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik seit Jahren Fingerabdruckscanner unter die Lupe nimmt, bewertet die neuesten Fortschritte deshalb zurückhaltend. „Man sollte die Kreativität der Fälscher nie unterschätzen“, warnt er. Denn wer könne schon ausschließen, dass ein neuartiges Material in ein paar Jahren auch einen riechenden Detektor austrickst? „Bis auf weiteres ist die Überwindungssicherheit bei Fingerabdrucksensoren eher gering“, resümiert Daum. Bei sensiblen Anwendungen sollten die Geräte deshalb immer durch weitere biometrische Erkennungssysteme ergänzt werden.