

Mit 3-D-Fingermodell und Gelatine

Biometrische Systeme überlisten

Biometrische Systeme dienen der Bequemlichkeit (Passwortsatz) oder der Sicherheit (Zugangskontrolle). Dass diese Systeme aber nicht so sicher sind, wie von den Herstellern behauptet, hat der Chaos Computer Club (CCC) in einem Beitrag seiner Clubzeitschrift „die datenschleuder“ (Ausgabe 80) am Beispiel von kapazitiven Fingerabdruckscannern dokumentiert.

Diese Technik ist am weitesten verbreitet und funktioniert so: Der Sensor besteht aus einer regelmäßigen Anordnung (Array) von winzigen Kondensatoren, die die Kapazitätsänderung beim Berühren des Sensors messen. Das aufgenommene Bild wird dann zur Verarbeitungseinheit übertragen, dort mittels Bildverarbeitungsalgorithmen aufbereitet. Um solche Systeme zu überwinden, braucht man laut „datenschleuder“ lediglich einen Abdruck des Fingerbildes einer berechtigten (eingelernten) Person.

Da die Haut mit einer schützenden Fettschicht überzogen ist, hinterlässt der Finger praktisch überall Abdrücke seines Rillenmusters, also auch auf dem Sensor selbst. Solche Rückstände bezeichnet man als Latenzabdruck. Gelingt es, diesen zu reaktivieren, kann man dem Rechner vortäuschen, ein berechtigter Nutzer melde sich gerade an. Dazu verändert man die Kapazität der Kondensatoren, auf denen sich die Fettrückstände der Haut befinden.

Eine Möglichkeit, dies zu tun, ist, durch Anhauchen zusätzliche Feuchtigkeit einzubringen – eine andere, feinen Graphitstaub aufzutragen, der an den Rückständen haften bleibt und somit die Änderung der Kapazität bewirkt.

Da die Hersteller um dieses Problem wissen und die Erkennung solch einer Latenzbildreaktivierung relativ einfach zu erkennen ist, sind die meisten Systeme so nicht mehr zu täuschen. Abhilfe schafft hier normales Klebeband. Wird das am Fett haftende Graphitpulver mit Klebeband abgezogen und leicht versetzt wieder aufgelegt, funktionieren die Algorithmen zur Latenzbilderkennung nicht mehr. Auf die gleiche Art und Weise können auch Abdrücke von anderen Gegenständen genommen und dem System als echte Finger vorgespielt werden. Besonders gut eignen sich hierfür glatte Flächen wie z.B. Glas oder Hochglanzpapier.

Aber auch wenn man nur im Besitz eines Fingerabdruckbildes (z.B. aus der Datenbank des BKAs o.ä.) ist, gibt es Möglichkeiten der Überwindung. Hierbei kommen Techniken des Platinenätzens zum Einsatz. Zur Herstellung einer dreidimensionalen Fingerabdruckattrappe druckt man das Fingerbild in Originalgröße mit einem Laserdrucker (600 dpi oder besser) auf Folie aus. Diese wird auf den Fotolack einer handelsüblichen fotostrukturierbaren Leiterplatte gelegt und mit einer UV-Quelle bestrahlt. Nach dem Entwickeln und Ätzen existiert eine Negativ-3D-Form der Fingerfläche.



Die ID Mouse von Siemens gehorcht nur dem Besitzer des eingespeicherten Fingerabdrucks. Foto: Siemens AG

Für die Fertigstellung der Fingerattrappe muss die Form noch mit einer möglichst hautähnlichen Substanz ausgefüllt werden. Gelatine scheint sich hierfür besonders gut zu eignen, da Konsistenz und Wasseranteil ähnlich wie bei einem echten Finger sind. Die Attrappe wird dann auf dem Sensor plziert. Wenn man gut gearbeitet hat, wird man vom System als berechtigter Benutzer akzeptiert.

Siemens sieht die Biometrie als eine Brücke zwischen Komfort und Sicherheit, wobei die Sicherheit biometrischer Produkte gegenüber PINs und Passwörtern deutlich höher sein kann. In verschiedenen Medien wird über erfolgreiche Angriffe auf biometrische Systeme berichtet. Hierbei handelte es sich um Laborversuche, die mit realen Bedingungen wenig gemein haben. [1]

[1] www.fingertip.de/index/index.html

Stellungnahme von Siemens zum Thema unter www.designbytechnology.de/index/

Der Chaos Computer Club ist unter der Internetadresse www.ccc.de erreichbar. Dort können auch ältere Ausgaben der Datenschleuder nachbestellt werden.

Lauschen im Festnetz

Es gibt eine Vielzahl an Möglichkeiten, einen normalen ISDN- oder Analog-Anschluss abzuhören oder zu überwachen.

- bei einer Dreierkonferenz
- durch die Rückruf-Funktion bei Abwesenheit
- Gebührenbetrug durch Eingriff in die TK-Anlage
- oder ganz klassisch mit Wanzen

Beispiel Nr. 1: Sie telefonieren mit einer Person und schalten, für diese unbemerkt, eine Dreierkonferenz. So kann ein Dritter ohne Probleme mithören und mitschneiden, ohne dass die angerufene Person davon Kenntnis erlangt.

Beispiel Nr. 2: Sie rufen einen Bekannten an und dieser ist nicht da. Sie haben aber schon lange den Verdacht, dass Herr XYZ keine Lust mehr hat, mit Ihnen zu telefonieren und deshalb einfach nicht den Hörer abnimmt.

Dank der Rückruf-Funktion können Sie den Herrn überführen: Sie geben, während das Telefon noch klingelt, die Tastenkombination *10# ein und legen auf. Sobald der telefonunlustige Bekannte ein Telefonat mit einer anderen Person führt und den Hörer wieder auf die Gabel drückt, werden Sie per Klingelzeichen informiert. Er ist also tatsächlich zuhause.

Beispiel Nr. 3: Viele Telefon-Verteilerkästen befinden sich in den Kellern von Wohnhäusern. Dort kann man mit einigem technischen Aufwand die Leitung „umklemmen“ und so auf Ihre Kosten telefonieren. Allerdings ist diese Sicherheitslücke bekannt und soll angeblich nicht mehr angreifbar sein.

Beispiel Nr. 4: Im Internet gibt es Bauanleitungen für Wanzen. Der Lauscher muss jedoch unbemerkt in Ihre Wohnung eindringen und dort die Wanze aktivieren.

Soweit die Möglichkeiten, die sich Otto Normal-Verbrecher zunutze machen kann. Die staatlichen Stellen haben seit der neuen TKÜV, der Telekommunikations-Überwachungsverordnung vom 29. 1.2002/www.bmwi.de, weit mehr Möglichkeiten, an Informationen zu gelangen.

Das Bundeskriminalamt z.B. kann „Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung mittels Auskünften oder Anfragen bei öffentlichen und nicht-öffentlichen Stellen erheben.“ (TKÜV) Was dabei unter diesen „Stellen“ zu verstehen ist, bleibt offen.

Die Telekommunikationsanbieter sind nach der neuen Verordnung dazu verpflichtet, Schnittstellen zu schaffen, um den Strafverfolgungsbehörden Auskünfte über Verbindungsdaten geben zu können. Gespeichert werden diese Daten in Zukunft bis zu einem halben Jahr.

Quelle: www.freenet.de/mobil/handy/rund/ratgeber/imsicatcher/06.html