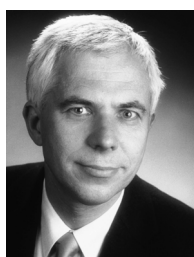


Eine ironische Anleitung für Meinungsbildner

Über die Unbrauchbarkeit der Biometrie

Sie sind als Autor auf der Suche nach einem spannenden Thema für eine medienwirksame Publikation? Dann empfehlen wir Ihnen, sich doch einmal mit Fälschungen biometrischer Charakteristika zu beschäftigen. Wenn das Thema für Sie von Interesse ist, finden Sie hier einige wertvolle Hinweise, wie Sie mit minimalem Aufwand und ohne allzu komplexe Detailrecherchen einen hohen publizistischen Aufmerksamkeitswert erzielen können. Der Erfolg ist garantiert und es gibt auch keine Nachwirkungen wie etwa ein ruiniertes Ruf oder gar die Gegendarstellung eines „angesäuerten“ Biometrieherstellers.



Von Dr. Manfred Bromba,
München

Der Einfachheit halber veranschaulichen wir unsere Empfehlungen am Beispiel der Fingerabdruckerkennung und betrachten dazu einige mehr oder weniger erfolgreiche Publikationen aus den Medien zum Thema „Wie überliste ich ein Fingerprint-System“. Alles was Sie brauchen, ist ein geschickter Umgang mit Informationen, insbesondere durch gezielte Verallgemeinerungen und passendes Weglassen – etwa durch nicht sofort durchschaubare Vernachlässigung von Zusammenhängen.

Und so wird es gemacht:

Schritt 1: Sie suchen sich eine konkrete biometrische Anwendung heraus. Denn es ist sehr wichtig, dass der Empfänger Ihrer Botschaft sich vorstellen kann, worum es geht und dass er auch selbst betroffen sein könnte. Deshalb: Keine Nischenanwendungen oder Anwendungen, die erst vor kurzem eingeführt wurden!

Schritt 2: Nun müssen Sie demonstrieren, wie leicht die biometrische Anwendung auszutricksen ist. Natürlich wissen Sie, dass ein kompletter Betrugversuch aus mindestens drei Hürden besteht, die alle zu überwinden sind.

Hürde 1: Sie müssen eine passende Fingerabdruckkopie etwa in Form eines Latenzbildes auftreiben

Hürde 2: Sie müssen diese in eine materielle Form bringen, die es gestattet, nicht als Plagiat erkannt zu werden

Hürde 3: Sie müssen das System dazu bringen, den nachgemachten Fingerabdruck zu akzeptieren

Da die Beschaffung von unbeabsichtigt hinterlassenen Fingerabdrücken leichter gesagt als getan ist, arbeiten Sie am besten mit einem ganz legalen Trick: Sie nehmen Ihren eigenen Abdruck oder den eines Freundes. Vorteil: Durch

Wahl einer passenden Oberfläche und mehrere Versuche lässt sich die Qualität von Fingerabdrücken „kooperativer Opfer“ perfekt optimieren. Empfohlen wird außerdem das vorherige Eincremen der Finger, um eine ausreichende Haltbarkeitsdauer des Abdrucks zu gewährleisten.

Ganz wichtig ist die Oberfläche. Sie muss glatt und sauber sein, hochglänzend und eben – denn sonst könnten etwa beim Abfotografieren Verzerrungen entstehen und die Erkennungschancen vermindert werden. Natürlich muss die Oberfläche zu einem viel genutzten Allerweltsgegenstand gehören, denn Sie haben jetzt mit einem Glaubwürdigkeitsproblem zu kämpfen. So könnte jemand auf die Idee kommen, dass Ihre Methode genauso sexy ist, wie das Duplizieren des eigenen Haustürschlüssels. Denn niemand kommt auf die Idee, dass Schlüssel generell unbrauchbar sind, nur weil man sie beim Schlüsseldienst nachmachen lassen kann. Natürlich könnten Sie an dieser Stelle verschweigen, woher der Fingerabdruck kommt. Aber das ist nicht erforderlich: Jeder Mensch mit einem Minimum an Fantasie kann sich vorstellen, dass das Ganze ähnlich einfach auch mit einem fremden Finger funktioniert. Denn Ihr Vorteil ist, dass außer der Kriminalpolizei und denen, die es tatsächlich einmal versucht haben, zur Zeit wahrscheinlich (noch) niemand wirklich weiß, wie (wenig) aussichtsreich dieses Unterfangen ist.

Hürde 2 ist da schon wesentlich einfacher zu nehmen. Denn hier haben Sie den unbezahlbaren Vorteil, dass Ihnen honorarige Institutionen wie der Chaos Computer Club die Arbeit bereits abgenommen haben. Sie können ruhigen Gewissens auf deren Anleitung [1] im Internet verweisen. Unklug wäre es an dieser Stelle allerdings, zu tief in die Hintergründe einzusteigen. Das könnte Sie erheblich an Glaubwürdigkeit kosten. So interessieren sich nur Wissenschaftler (also nicht Ihre Zielgruppe) dafür, wie viele Wochen jemand braucht, um etwa ein zu Ihrem Fingerprintsensor passendes Kopierverfahren auszutüfteln und wie viele Tage jemand braucht, um dieses Verfahren soweit zu beherrschen, dass der Kopiervorgang etwa innerhalb einer Stunde gelingt. Auch die Zahl der erfolglosen Versuche ist hier belanglos. Denn wenn einmal ein Versuch erfolgreich war, dann ist

die Hoffnung berechtigt, dass es erneut (sofort) klappen wird. Sonst würde ja auch kein vernünftiger Mensch Lotto spielen.

Hürde 3. Jetzt wird es ernst, Sie müssen Ihre Fingerkopie dem Sensor präsentieren. Um den Erfolg Ihres Projekts nicht zu gefährden, haben Sie natürlich schon bei der Auswahl der biometrischen Anwendung darauf geachtet, dass diese Präsentation ohne Beobachtung durch andere Personen stattfinden kann. Da ja nicht-digitale Kopien nie so perfekt wie das Original sein können, sollte Ihre Anwendung auch so ausgesucht sein, dass beliebig viele Authentifizierungsversuche erlaubt sind, damit Sie den richtigen Auflagewinkel, den richtigen Auflagebereich relativ zur Fingerführung des Sensors und den richtigen Auflagedruck in der zur Verfügung stehenden Zeit treffen. Für den wahrscheinlichen Fall, dass es nicht schon beim ersten Mal klappt, hat der Anbieter des biometrischen Systems hoffentlich daran gedacht, den vom Sensor aufgenommenen Fingerabdruck auf einem Display bildlich darzustellen. Denn ohne Feedback kann ein Fälschungsversuch doch recht mühselig werden.

Textbeispiele zur Orientierung

1. Bald ein Volk ohne Daumen? [3]. Dieser Beitrag in der Süddeutschen Zeitung aus dem Jahre 1998 gehört zu den frühesten, aber leider weniger gelungenen Beispielen. Er zeigte ein Schreckensszenario von Fingerprintrutzern, denen die Daumen abgeschnitten wurden, um damit am Automaten anderer Leute Geld abzuholen. Zwar hat dieser Artikel kurzzeitig einige Hersteller von Fingerprintsensoren aufschrecken können, fand aber beim großen Publikum keine größere Resonanz. Grund: Zu früh, zu übertriebene Darstellung.

2. Matsumoto [4]: Sehr erfolgreicher Beitrag eines Mathematikers, der einmal handwerklich tätig sein wollte und dies zur internationalen Bestürzung auch erfolgreich bewerkstelligte. Genial: Diese Veröffentlichung kam zu einer Zeit voller Hype, in der selbst von manchen Sensorherstellern noch die Marketingbotschaft in die Welt gesetzt wurde, man könne keine Finger nachmachen. Damit war die Wirkung umso einschlagender. Der Verfasser vermied es auch erfolgreich, auf frühere Quellen seiner Versuche hinzuweisen: So wurde 1922 vom berühmten Kriminalisten Robert Heindl in seinem Buch „System und Praxis der Daktyloskopie und der sonstigen technischen Methoden der Kriminalpolizei“ (De Gruyter, Berlin 1922) darauf verwiesen, dass R. Austin Freeman bereits 1907 in seinem Kriminalroman „The Red Thumb Mark“ eine High-Tech-Methode zum Kopieren von Fingerabdrücken auf Gelatinefolie präsentierte, die auch heute noch sehr gut mit den meisten Fingerabdrucksensoren zusammenarbeiten würde.

3. c't 2002 [5]: Perfekt gemachte Fälschungsversuche in einem Test von Fingerprintsensoren für PC-Anwendungen. Waren so gut, dass sogar der Chefredakteur von „heise Security“ hinterher im Fernsehen verkündete, seinen PC nicht

mit Fingerprint schützen zu wollen. Es wurden fast alle hier gemachten Empfehlungen umgesetzt: „kooperative Opfer“, gutes Timing, keine unnützen Angaben über den Fälschungsaufwand, fehlerhafte Testprodukte.

4. c't 2007 [6,7]: In diesem zweiten Test konnte das hohe Niveau des ersten Beitrags nicht gehalten werden. Schlecht: Die Autoren geben zu, dass sie einige Fingerprintsysteme nur schwer „überlisten“ konnten. Unverzeihlich: Der Beitrag erwähnt, dass nicht-kooperative Opfer, also der Realfall, die Situation für den Fälscher deutlich erschweren. Aber wenigstens hat man diesen Fall nicht weiter untersucht.

5. Plusminus [8]: Dieser Beitrag setzt die Tradition biometriespezifischer Fälschungsthemen im öffentlich-rechtlichen Fernsehen mit einer Demonstration fort, wie sich ein biometrisches Bezahlsystem überrumpeln lässt. Gut gemacht: kooperatives Opfer, kein überflüssiges Wort zum Fälschungsaufwand, keine unnütze Information, welche Maßnahmen dem Fälscher sonst noch die Arbeit schwer machen könnten. Weniger geschickt der Abschluss des Beitrags, in dem es heißt: „Edeka Südwest teilt uns auf Anfrage schriftlich mit, man sehe ‚keinen Handlungsbedarf‘. Die bestehenden Sicherheitsvorkehrungen seien, ‚wie unsere Erfahrungen gezeigt haben, vollkommen ausreichend‘. Der verwendete Scanner sei ‚sogar für die Verwendung durch amerikanische Regierungsbehörden freigegeben‘ und werde ‚weltweit (...) im Sicherheitsbereich von ca. 200 Mio. Personen genutzt‘. Mit anderen Worten: Man kann auch Sicherheitsbehörden mit diesem Trick „leimen“. Spätestens hier könnte dem einen oder anderen Leser der Gedanke kommen, warum der Autor „gegen den Rest der Welt“ Recht haben sollte und ob dieser nicht irgend etwas übersehen haben könnte.

Über unseren Autor:

Dr. Manfred Bromba ist Geschäftsführer der Bromba GmbH und Biometrieberater. Kontakt: www.bromba.com

[1] „Starbug“; „Wie können Fingerabdrücke nachgebildet werden?“; 09. Oktober 2004; https://www.ccc.de/biometrie/fingerabdruck_kopieren.xml

[2] Kent, J.: „Malaysia car thieves steal finger“; <http://news.bbc.co.uk/1/hi/world/asia-pacific/4396831.stm>

[3] Maresch, M.: „Bald ein Volk ohne Daumen?“; Süddeutsche Zeitung v. 1998-01-31

[4] Matsumoto, Tsutomu; „Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies“; ITU-T workshop on security, Seoul; May 2002.

[5] Thalheim, L.; Krissler, J.; Ziegler, P.-M.: „Körperkontrolle“; c't 11/2002, S 114-123

[6] Heinz, B.; Krißler, J.; Rütten, C.: Fingerspitzengefühl – Fingerabdrucksysteme im Test. c't 12/2007, S 98-101.

[7] Krißler, J.; Rütten, C.: Feine Linien – Wie leicht sich Fingerabdrucksensoren austricksen lassen. c't 12/2007, S 102-103

[8] Fingerprint-System überlistet, WDR, plusminus, Dienstag, 27. November 2007, 21:50