Werden biometrische Sicherheitstechnologien die heutige IT-Sicherheitsdebatte vor neue Herausforderungen stellen?

Andreas Pfitzmann[1]

Kurzfassung

Eine Diskussion biometrischer Verfahren zur Identifizierung und Authentifizierung von IT-Nutzern in Vergangenheit, Gegenwart und Zukunft wirft grundsätzliche Fragen auf:

- Werden biometrische Verfahren – wie allgemein erwartet – in der Zukunft eher weniger unsicher sein als heute oder wegen der zunehmenden Verbreitung von Genomdatenbanken nicht eher unsicherer?
- Sind biometrische Verfahren mit dem Recht auf „Informationelle Selbstbestimmung“ vereinbar, sofern ihre Nutzung faktisch oder gar gesetzlich vorgeschrieben wird?
- Wie soll in der Zukunft eine Balance zwischen immer leichterem Zugriff auf Daten unseres Körpers (u.a. durch Genomdatenbanken oder Biometrie) und damit immer leichterer und weitergehender Überwachung in der physischen Welt und der weitgehend frei gestaltbaren (Un-)Überwachbarkeit in der digitalen Welt aussehen?
- Wollen wir die heute in der physischen Welt noch vorhandenen Unbeobachtbarkeitsräume in die digitale Welt verlagern oder soll es künftig keinerlei unbeobachtbares Handeln mehr geben?

Wer glaubt, diese Fragen kurzfristig, einfach und mit Gewissheit beantworten zu können, hat sie vermutlich nicht verstanden. Die IT-Sicherheitscommunity wie auch Innen- und Forschungspolitik sollten beginnen, sich mit ihnen auseinanderzusetzen.

1 Einleitung

Biometrische Verfahren zur Identifizierung und Authentifizierung von IT-Nutzern sollen bewirken, dass Unbefugte abgewiesen werden und Identitäts„diebstahl“ vermieden wird. All dies soll benutzungsfreundlich (nichts muss man sich merken, nichts wechseln, nichts mit sich herumtragen) und preiswert sein. Und natürlich sicher: Niemand wird zu Unrecht abgewiesen, kein Unbefugter hat eine realistische Chance, akzeptiert zu werden.

Solche biometrischen Sicherheitstechnologien gibt es heute höchstens in Ansätzen, aber da sie allgemein für wünschenswert gehalten werden, wird an ihrer Entwicklung fieberhaft gearbeitet. Soweit ich zurückdenken kann (im Gebiet Sicherheit und Datenschutz arbeite ich seit 1983) sind solcherart sichere biometrische Systeme jeweils für in zwei Jahren angekündigt. Nach mehr als zwei Jahrzehnten beginnt mir der Glaube daran zu schwinden.

[1] Lehrstuhl Datenschutz und Datensicherheit, Institut für Systemarchitektur, Fakultät Informatik, TU Dresden, 01062 Dresden, http://dud.inf.tu-dresden.de e-mail pfitza@inf.tu-dresden.de

Nun ist die Sicherheit biometrischer Systeme nicht der einzige offene Punkt für ihren erfolgreichen Einsatz. Fragen des Datenschutzes im Sinne „Informationeller Selbstbestimmung“, zumindest aber im Sinne von „nebenwirkungsfreiem Einsatz“ der Biometrie stellen sich und sind möglicherweise noch schwerer befriedigend zu beantworten als Fragen der Sicherheit. Schließlich ist, wegen der Fortschritte in der Medizin – u.a. Prüfung der persönlichen Medikamentenverträglichkeit im Rechner – der Aufbau großer Genomdatenbanken zu erwarten. Deren Auswirkungen auf biometrische Sicherheitstechnologien werden vermutlich erheblich sein.

Um die notwendige Diskussion etwas zu strukturieren, ordne ich sie auf der Zeitachse: Vergangenheit, Gegenwart und Zukunft stehen für die Aspekte Sicherheit, Informationelle Selbstbestimmung und unerwartete, zumindest bisher nicht diskutierte Wechselwirkungen. Schließlich wage ich als Ausblick mit aller Vorsicht wenige Ratschläge.

2 Vergangenheit

Dass einzelne biometrische Merkmale wie z.B. Fingerabdruck, Hand- oder Gesichtsgeometrie zur sicheren Identifizierung und Authentifizierung nicht ausreichen und auch mehrere Merkmale kombiniert nicht notwendigerweise sicher sind, ist seit Jahrhunderten bekannt. Sie glauben das nicht? Dann erinnern Sie sich bitte an „Der Wolf und die sieben Geißlein“ (oder schließen Sie Ihre IT-sicherheitsrelevante Bildungslücke: http://gutenberg.spiegel.de/grimm/maerchen/wolfgeis.htm).

Sie meinen, solche Verwechslungen über Artgrenzen hinweg sind schon lange Geschichte und kommen in der Neuzeit nicht vor. Leider falsch. Eine von einem Münchner Weltkonzern vor wenigen Jahren als sicher angepriesene Chipkarte mit biometrischer Erkennung von Fingerabdrücken konnte zur Freude einiger Teilnehmer eines vom CCC organisierten Feriencamps selbst einem Angriff mit Feriencampmitteln nicht widerstehen: Die Chipkarte konnte den Originalfinger und Flüssigheftpflaster, nachdem es in einem Fingerabdruck in einer Wachskerze erstarrt war, nicht auseinander halten. Auch eine Art Überschreitung von Artgrenzen.

Während den Wolf die Strafe für sein lügnerisches Tun unmittelbar ereilt, verkauft der Münchner Weltkonzern weiterhin biometrische Sicherheitstechnik. Nicht immer nimmt die Geschichte einen als gerecht empfindbaren Verlauf.

3 Gegenwart

Viele, wenn nicht alle biometrischen Größen verraten Eigenschaften desjenigen, der hier vermessen wird, die bei Gestaltung (und Normung) des Verfahrens möglicherweise noch

unbekannt sind. Schon vor 15 Jahren erzählte mir ein Forscher der GMD in Darmstadt, dass beispielsweise der tiefe Blick ins Auge auf die Netzhaut nicht nur hilft, Menschen zu unterscheiden, sondern auch am Montag bei Arbeitsantritt unbemerkt auszuwerten, wie tief sie am Wochenende ins Glas geschaut haben – wenn nicht noch Persönlicheres. Damals wurde so etwas nicht publiziert, da nicht im Interesse der Auftraggeber. In der Gegenwart aber steht es in den einschlägigen Studien, ist allerdings immer noch nicht im allgemeinen Bewusstsein, nicht einmal im Bewusstsein aller IT-Sicherheitsfachleute.

Schon gar nicht ist allen Sicherheitsfachleuten klar, dass derjenige, der ein biometrisches Verfahren einführen will, sich nicht nur der Aufgabe stellen muss, seine Sicherheit, sondern auch seine „Nebenwirkungen“ bzgl. medizinisch-sozialer Neugierde zu klären. Im Zweifelsfall hat bei biometrischen Systemen, für deren Benutzung ein faktischer Zwang besteht, der Systementwickler und –betreiber die Pflicht zu beweisen, dass die „Nebenwirkungen“ vernachlässigbar, zumindest aber vertretbar sind. Kann er dies nicht überzeugend, dürften solche Systeme illegal sein. Das kann dann manchem Hersteller, Betreiber oder Politiker so schwer im Magen liegen wie die Steine dem Wolf im Märchen.

Leider kann man bei biometrischen Verfahren auch nicht so leicht wieder von vorn beginnen wie bei der Kryptographie, ist das Kind erst mal in den Brunnen gefallen. Bei Kryptographie generiert man im Zweifelsfall einfach neue Schlüssel, nachdem das IT-System gehackt oder auch nur mit einer (wenn nicht einigen hundert) Sicherheitslücken versehen am Internet betrieben worden war. PINs und Passwörter können ebenfalls leicht getauscht werden, während dies beispielsweise bei Fingerkuppen auf wenig Akzeptanz stoßen dürfte. Biometrie ist also nicht nur durch ihre Datenschutzrelevanz, sondern auch im Hinblick auf ihre Sicherheit extrem fehler-intolerant. Im Gegensatz dazu hat die Zahl der Fehler in weit verbreiteten Systemen entgegen allen Ankündigungen und Versprechungen in den letzten Jahren eher zu- als abgenommen und wird in der überschaubaren Zukunft keinesfalls klein genug sein, um nur noch alle 8 Jahre einen sicherheitsrelevanten schwerwiegenden Fehler zu erleben. Das müsste sie aber, damit die 10 Finger für ein normales Leben ausreichen.

4 Zukunft

Die immer schnellere und preiswertere Analyse des menschlichen Genoms, verbunden mit seinem zunehmenden Verständnis eröffnet die Hoffnung auf eine persönliche Medikamentenverträglichkeitsprüfung im Rechner statt langwieriger Tests von Medikamenten auf allgemeine Verträglichkeit. Langwierige Tests halten für manche Kranke hochwirksame Medikamente auf Zeit vom Markt fern, die Forderung nach allgemeiner Verträglichkeit tut dies gar auf Dauer.

Und trotz aller Tests ruft die Einnahme bei manchen immer noch teils schwere Nebenwirkungen hervor. Allein dieser Aspekt einer im engeren Sinne persönlichen Medikation dürfte dazu führen, dass auf „freiwilliger Basis“ innerhalb der nächsten Jahrzehnte nahezu vollständige Genomdatenbanken zumindest des zahlungskräftigeren Teils der Weltbevölkerung aufgebaut werden. Dies wird dramatische und weitgehend unkontrollierbare Auswirkungen auf den faktisch erreichbaren Datenschutz haben, da auf Genomdatenbanken nicht nur von Forschern vermeintlich anonymisiert zugegriffen werden kann (vermeintlich, weil leicht deanonymisierbar), sondern auch ein leicht nutzbarer Bezug zwischen Genomdatensatz und Mensch vorhanden sein muss:

- Der Mensch will leichten Zugriff auf sein eigenes Genom haben, da ihm dies im medizinischen Alltag Vorteile bringt.
- Nach der Entwicklung neuer Therapien möchte man natürlich kurzfristig alle betroffenen Genomträger erreichen.

Der Datenschutz wird solche Genomdatenbanken nicht verhindern können – und er sollte es nach meiner persönlichen Meinung auch gar nicht versuchen. Menschen, die wegen eines eher geringen Kundenrabattes persönliche Daten weitergeben und in deren Verarbeitung einwilligen, werden dies, wenn ihnen eine effektivere (und preiswertere, so die Ankündigungen der Pharmaindustrie) medizinische Behandlung winkt, sowohl für sich wie auch vor allem für ihre Kinder tun. Auch und gerade vorsichtige Menschen werden dies wollen.

Was bedeutet dieser absehbare Trend für biometrische Sicherheitstechnologien? Einerseits spitzen Genomdatenbanken die in Kapitel 3 beschriebenen Datenschutzprobleme extrem zu. Andererseits untergraben Genomdatenbanken möglicherweise die Sicherheit aller biometrischen Verfahren, zumindest aber solcher, bei denen nicht *erworbene*, sondern *ererbte* Merkmale vermessen werden. Diese ererbten Merkmale sind durch das individuelle Genom determiniert, so dass sie bei Kenntnis des individuellen Genoms möglicherweise genügend effizient hergeleitet und dann (bio)technisch nachgebildet werden können.

Sind Fingerabdrücke ererbte Merkmale, dann müsste biometrische Fingerabdruckerkennung nicht nur den ererbten Abdruck, sondern insbesondere die durch das praktische Leben verursachten Abweichungen durch Verletzungen etc. messen. Heutige Verfahren kennen diese Differenzierung nicht, sondern messen nur die „Summe“.

Mir sind zu Wechselwirkungen zwischen biometrischen Sicherheitstechnologien und Genomdatenbanken keine Überlegungen, geschweige denn Untersuchungen anderer bekannt. Sie werden aber innerhalb weniger Jahrzehnte, wenn nicht Jahre zumindest für

solche biometrischen Verfahren nötig sein, die große Werte schützen oder massenhaft eingesetzt werden sollen.

Die wohlige Selbstzufriedenheit bezüglich Biometrie „hat es schon in den letzten Jahrzehnten nicht funktioniert, wird es vielleicht auch in den nächsten zwei Jahren nicht funktionieren, so werden wir doch zumindest mittelfristig spürbare Fortschritte bezüglich der Sicherheit und Kosten unserer Systeme erzielen“ könnte also nicht nur kurzfristig immer mal wieder durch „In-den-Brunnen-Fallen“ gestört werden, sondern gerade auch langfristig durch weit verfügbare Informationen aus Genomdatenbanken.

5 Ausblick

Biometrische Verfahren sind, sowohl was ihre kurz- und langfristige Sicherheit angeht, als auch im Hinblick auf ihre „Nebenwirkungen“ bzgl. dem Offenbaren medizinischer Daten bei weitem nicht so untersucht und stabil, dass mir ein massenhafter, flächendeckender Einsatz verantwortbar erscheint. Er wird teils aus politischen, teils aus wirtschaftlichen Gründen, teils aus purer Bequemlichkeit trotzdem versucht werden. Manche möglichen Überraschungen habe ich skizziert.

Diese zu erwartenden Überraschungen aus dem Bereich Biometrie zusammen mit den vermutlich explosionsartig anwachsenden Genomdatenbanken und ihren Anwendungen werden die heute noch vorhandenen Freiräume der Unbeobachtbarkeit in der physischen Welt zunehmend verkleinern, wenn nicht gar auslöschen. Möglicherweise werden sich Menschen künftig in der physischen Welt nicht mehr bewegen können, ohne mit jedem einzelnen Schritt personenbezogen auswertbare Spuren zu hinterlassen.

In der digitalen Welt ist es bisher genau umgekehrt: Heute sind die Spielräume für Unbeobachtbarkeit dort sehr gering – auch wenn das unpersönliche Internet Unbeobachtbarkeit vorgaukelt. Die Forschung der letzten 24 Jahre hat zwar Verfahren hervorgebracht, die eine weitgehende Unbeobachtbarkeit in der digitalen Welt ermöglichen, die bisher aber nur sehr wenig eingesetzt werden. Sollen wir als Gesellschaft auf Räume des unbeobachtbaren Handelns künftig verzichten? Können wir das, ohne den Menschen als autonomes Wesen weitgehend auszulöschen? Oder könnte und sollte die digitale Welt künftig der Ort des weitgehend unbeobachtbaren Handelns werden? Gibt es dazu langfristig Alternativen?

6 Ein Dankeschön

Für Diskussion, Kritik und Verbesserungsvorschläge danke ich Mike Bergmann, Katrin Borcea, Rüdiger Dierstein, Marit Hansen, Stefan Köpsell, Thomas Kriegelstein, Antje Schneidewind und Andreas Westfeld.