Überwindungsszenarien für biometrische Systeme

Stefan Hein
Markus Mahrla

18. Oktober 2004

Inhaltsverzeichnis

1 Präambel **4**

2 Einführung **5**

3 Angriffsmöglichkeiten **7**
- 3.1 Benutzer . . . 7
- 3.2 Aufnahme des biometrischen Merkmals . . . 8
- 3.3 Verbindungen zwischen bestimmten Komponenten . . . 9
- 3.4 Datenerfassung . . . 10
- 3.5 Speicherort . . . 10
- 3.6 Administrator . . . 11
- 3.7 Benutzer, Policy Management, Portal . . . 11
- 3.8 Portal . . . 12
- 3.9 Hardware . . . 12
- 3.10 Software und Firmware . . . 12
- 3.11 Verbindungen zwischen Komponenten allgemein . . . 12

4 Spezielle Szenarien **14**
- 4.1 Fingerabdruck . . . 14
- 4.2 Gesichtsgeometrie . . . 18
- 4.3 Schnittstellen zwischen Sensor und verarbeitenden System . . . 19

5 Gegenmaßnahmen **20**
- 5.1 Lebenderkennung / Life-Test . . . 20
- 5.2 Smardcards . . . 22
  - 5.2.1 Template on Card . . . 23
  - 5.2.2 Match on Card . . . 23
  - 5.2.3 Sensor on Card . . . 23

5.2.4 System on Card 24

6 Schlussbemerkungen 26
6.1 Eigenschaften unterschiedlicher Authentifikationssysteme 26
6.1.1 Verlust 26
6.1.2 Diebstahl 27
6.1.3 Weitergabe 27
6.1.4 Änderbarkeit 27
6.2 Fazit 28

Kapitel 1

Präambel

Diese Ausarbeitung zum Thema „Überwindungsszenarien für biometrische Systeme" befasst sich mit den Möglichkeiten Sicherheitsmechanismen von biometrischen Systemen zu umgehen, zu überlisten oder anzugreifen. Aufgrund der zunehmenden Verbreitung von biometrischen Systemen gilt es diesen Punkt in der Zukunft mehr Beachtung zu schenken. Heutzutage bieten immer mehr Firmen Komplettlösungen an, die hohe Benutzerfreundlichkeit und zugleich ein hohes Sicherheitsniveau versprechen. Bei genauerer Betrachtung wird jedoch auffällig, dass sich diese beiden Aspekte in der Realität häufig widersprechen.

Kapitel 2

Einführung

Spricht man von biometrischen Sicherheitssystemen muß man sich zunächst im Klaren sein, dass es zwei Arten der Anwendung von Biometrie in diesem Bereich gibt. Man unterscheidet hier zwischen *Identifikation* und *Verifikation*. Bei der I dentifikation dient ein biometrisches Merkmal dazu, einen 1:N Vergleich durchzuführen, d.h. ein Merkmal einer zu identifizierenden Person mit N in einer Datenbank gespeicherten Merkmalen zu vergleichen, um dessen Identität zu ermitteln. Bei der Verifikation hingegen wird ein 1:1 Vergleich durchgeführt, d.h. es werden zwei Templates eines biometrischen Merkmals miteinander verglichen. Stimmen beide zu einem gewissen Grade überein wird angenommen, dass die Person tatsächlich die ist, für die sie sich ausgibt. Ein Angreifer verfolgt demnach unterschiedliche Ziele, je nachdem ob er eine Identifikation vermeiden möchte oder sich Zutritt zu einem gesicherten Bereich mit Hilfe einer erfolgreichen Verifikation verschaffen möchte. Man spricht von Negatividentifikation, wenn es darum geht aus einer Menge von Personen mit Hilfe eines biometrischen Identifikationsverfahren bestimmte z.B. verdächtige Personen herauszufiltern, von denen man beispielsweise über biometrisches Ausgangsmaterial in Form eines Fotos oder Fingerabdruckes verfügt. Ein potentieller Angreifer versucht hier, seine Merkmale möglichst unkenntlich zu machen bzw. zu verfremden. Mit einem präparierten Finger, einer neuen Barttracht oder ähnlichem lassen sich biometrische Merkmale sehr gut verstecken, mit dem Hintergrund eine Nichterkennung möglich zu machen. Bei der Verifikation ist das Angriffziel hingegen der Versuch ein Matching mit einer autorisierten Person zu erreichen. Der Angreifer hat hier die Absicht, möglichst gut ein bestimmtes biometrisches Merkmal zu imitieren, um sich unerlaubt Zutritt zu einem mit Hilfe von Biometrie gesicherten Bereich zu verschaffen.

Hautsächlich befasst sich diese Arbeit jedoch mit Szenarien biometrische Verifikationssysteme zu überwinden. Dabei soll im Vordergrund stehen, dass sich der Angreifer möglichst unbemerkt Zutritt zu gesicherten Systemen verschafft. Die Ausübung von phy-

sischer Gewalt auf ein biometrisches Sicherheitssystem ist auch auf nichtbiometrische übertragbar und soll somit weniger Thema dieser Ausarbeitung sein. Es bleibt an dieser Stelle dem Leser überlassen, sich solche Szenarien vorzustellen, die alles in allem sicher in kurzer Zeit die Aufmerksamkeit von Security oder anderen Personen auf sich ziehen würden.

In der Literatur wird darüber hinaus von zwei Typen von Angreifern gesprochen. Der *Imposter* (Betrüger) ist jemand, der autorisiert oder nicht autorisiert, absichtlich oder unabsichtlich versucht, sich als jemand auszugeben, der zugangsberechtigt ist. Der *Attacker* (Angreifer) versucht hingegen das Biometrische System zu umgehen oder manipulieren, um sich oder jemand anderem Zutritt zu verschaffen oder registrierten Nutzern den Zutritt zu verwähren.

Bevor wir uns genauer mit den Angriffspunkten eines biometrischen Systems auseinandersetzen wollen, soll zunächst eine für uns intuitive Gliederung von Angriffsmöglichkeiten vorangestellt werden. Ein Überwindungsszenario ist die Ausübung von psychischer oder physischer Gewalt auf einen autorisierten Nutzer. Ist jemand leicht zu erpressen oder zu bestechen, eröffnet dies ein nicht zu unterschätzendes Angriffspotential. An zweiter Stelle sei das Überlisten der Sensorik durch Nachahmung eines Biometrischen Merkmals mit Hilfe von Bildern, Attrappen, Kopien etc. genannt. Ein anderer Weg ist, einen Angriff auf das System hinter der Sensorik durchzuführen. Mögliche Ziele sind hier die Datenkommunikation, Templatedaten, Policy Management und noch weitere, auf die noch ausführlicher eingegangen wird.

Kapitel 3

Angriffsmöglichkeiten

Dieses Kapitel setzt sich mit den Angriffspunkten eines biometrischen Systems auseinander. Dabei werden die einzelnen Komponten dahingehend untersucht, inwieweit der Angreifer sie zur Überwindung des Systems nutzen kann.

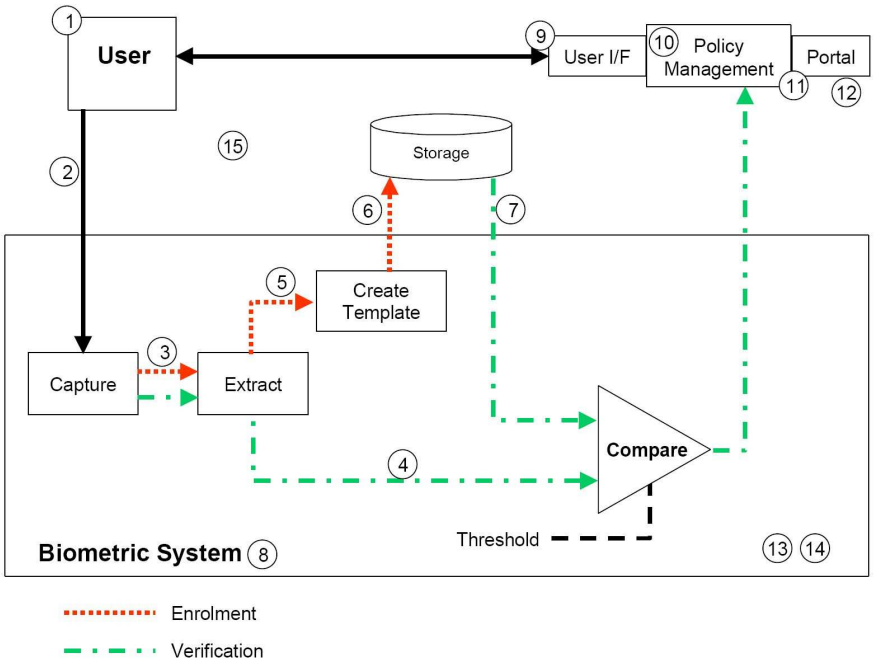

Abbildung 3.1: Angriffspunkte eines biometrischen Systems

3.1 Benutzer

Bei der Sicherheit eines biometrischen System muss immer berücksichtigt werden, dass ein Benutzer seine biometrischen Daten unwissentlich, unfreiwillig oder freiwillig zu Verfügung stellen kann. Man kann dabei unterscheiden, inwieweit der autorisierte Benutzer mitwirkt. So kann das biometrische Merkmal versteckt und unbemerkt aufgenommen werden; beispielsweise mittels Foto-, Video- oder Tonaufnahme. Durch eine Unachtsamkeit des Benutzers kann diese aber auch gestohlen werden. So zum Beispiel im Schlaf oder auch von einem unsicheren System, auf dem der Benutzer mit gleichem Merkmal ebenfalls eingerichtet ist. Die biometrischen Daten können aber natürlich auch durch Zwang oder Amputation gestohlen werden. Des weiteren kann der Benutzer sein biometrisches Merkmal bei der Einrichtung modifizieren und somit den Angriff erleichtern. Dies setzt ein grösseres Mitwirken des autorisierten Benutzer bei der Überwindung des Systems voraus. Letztendlich kann der Benutzer seine Daten freiwillig zur Verfügung stellen und den Angriff erheblich erleichtern.

3.2 Aufnahme des biometrischen Merkmals

Die Aufnahme des biometrischen Merkmals ist eine sehr empfindliche Stelle für das biometrische System. Wurde diese Stelle erfolgreich überwunden, gelangt der Angreifer meistens zum Ziel. Die Angriffe kann man je nach Aufwand unterscheiden. Kein Aufwand hat der Angreifer, wenn dieser sein eigenes, unverändertes Merkmal präsentiert. Dabei kann es bei einer zu hohen FAR zu einen Übereinstimmung kommen. Der Angreifer kann sich bei der Verifikation ein zufälligen Benutzer wählen oder einen Benutzer, bei dem er weiss, dass er eine hohe FAR besitzt. Bei der Identifikation erhöhen sich die Chancen des Angreifers erheblich, da es wesentlich mehr Möglichkeiten zur Übereinstimmung gibt. Denkbar ist natürlich auch, dass der Angreifer sich für einen Benutzer ausgibt, dessen biometrisches Merkmal sehr ähnlich zu seinem ist; so bei Verwandschaftbeziehungen oder im Idealfall bei Zwillingen. Woran ebenfalls zu denken ist, dass bei biometrischen Merkmalen, die man mehrmals besitzt, einige Versuche ohne nennenswerten Aufwand durchgeführt werden können. Dies ist beispielsweise bei den Fingerabdrücken der Fall. Dort hat der Angreifer die Möglichkeit alle zehn Finger ohne grossen Aufwand durchzuprobieren. Der Angreifer kann natürlich auch mit ein bisschen Mehraufwand versuchen sein biometrischen Merkmal zu modifizieren, um seine Chancen auf Erfolg zu erhöhen. So können dynamsiche Merkmale wie Stimme oder Unterschrift verändert oder angepasst werden, ebenso wie statische Merkmale wie Gesicht oder Hand. Etwas schwieriger und mit mehr Aufwand verbunden, aber dafür erfolgsversprechender, sind die künstlichen

Merkmale. Dabei wird versucht das biometrische Merkmal so gut wie möglich nachzubauen oder nachzuahmen. Beispielhaft sind hier der Silikonfinger, die Gesichtsmaske oder die Tonbandaufnahme. Bei diesem Vorgehen muss aber bereits ein biometrisches Merkmal vorliegen, um dieses nutzen zu können. Dabei können Rückstände von Merkmalen helfen, wie der latente Fingerabdruck auf dem Fingerabdruckscanner. Bei der Aufnahme des biometrischen Merkmals ist zu beachten, dass wenn die Anzahl der Wiederholungen nicht beobachtet werden, Angriffe mit leichten Veränderungen wiederholt werden können und der Angreifer so sukkzessiv das Ziel erreicht (hill-climbing attack).

3.3 Verbindungen zwischen bestimmten Komponenten

Leitungen zwischen Komponenten stellen immer ein Risiko dar, abgehört zu werden. Hierbei und an vielen anderen Stellen muss aber unterschieden werden, dass dies auch für nichtbiometrische Systeme gilt, und dies kein Nachteil von Biometrie bedeutet. Im Einzelnen sollen hier vor allem die Verbindungen zwischen den Komponenten Aufnahme und Extraktion sowie Speicherung/Extraktion und Vergleich betrachtet werden. Zwischen diesen Komponenten kann der Angreifer versuchen autorisierte Templates abzufangen und diese dann für seinen Angriff weiterbenutzen. Ebenso kann er versuchen sein Template einzufügen und somit diese Komponenten umgehen.

3.4 Datenerfassung

Das biometrische System kann bereits überwunden worden sein, bevor es überhaupt aktiv wurde. Bei der Erfassung der biometrischen Daten kann es schon zu Angriffen beziehungsweise zu Vorbereitungen für Angriffe gekommen sein. So ist es denkbar, dass ein autorisierter Benutzer bewusst ein schwaches Merkmal einrichtet hat, um einen Angriff zu erleichtern. So könnte der Benutzer bei ausreichenden Fachkenntnissen sein Verhalten entsprechend modifizieren oder die Qualität seines Merkmals durch Störeinflüsse aus der Umwelt verschlechtern. Ebenso könnte er bei der Einrichtung unbemerkt ein künstliches Merkmal verwenden und dieses den Angreifern überlassen. Diese benutzen dann einfach das künstliche Merkmal bei der biometrischen Aufnahme wieder. Auch ist daran zu denken, dass bei der Erfassung der Daten die Personen unter Umständen nicht vor Ort sind und auf Fotos, Videos etc. zurückgegriffen werden muss. So zum Beispiel bei der Identifikation von Terroristen an Flughäfen. Ebenso muss daran gedacht werden,

dass auch Fehler des Administrators gemacht werden können und es zu Fehlern bei den biometrischen Daten vor der Speicherung kommt.

3.5 Speicherort

Besonderer Beachtung kommt der Speicherung der biometrischen Daten zu. Hierbei muss jedoch unterschieden werden, um welches System es sich handelt. So ist der heimische PC anders zu betrachten als der Server im Internet. Generell kann man jedoch sagen, dass der Angreifer versuchen könnte sein biometrisches Merkmal abzuspeichern oder mit einem gültigen auszutauschen. Ebenso könnte er Templates löschen oder modifizieren, um dies unter Umständen für seinen Angriff zu nutzen. Wie erfolgreich die Angriffe sind hängt sicherlich von dem Grad der Verschlüsselung ab. Liegt keine oder nur eine geringere Verschlüssung vor, könnten biometrische Daten gestohlen und für Angriffe benutzt werden. Unter Umständen ist es denkbar, dass biometrische Daten von anderen gleichen biometrischen Systemen gestohlen und auf dem anversierten System eingesetzt werden.

3.6 Administrator

Eine nicht abschaltbare Fehlerquelle stellt der Administrator des Systems dar. Hierbei können alle Fehler zum Nachteil der Sicherheit gemacht werden, die vorstellbar sind. Der Administrator könnte beispielsweise falsche Schwellwerte einstellen, falsche Systemrechte vergeben oder Passwörter zu einfach gewählt haben. Vorstellbar ist auch, dass auf bestimmte Situationen nicht adäquat oder falsch reagiert wird und so Angriffsversuche unbeobachtet bleiben. Dies könnte eventuell zum Erfolg führen (z.B. hill-climbing Attacke) oder von anderen genutzt werden. Offensichtlich ist, dass es bei einem feindlichen gesinnten oder bestechlichen Administrator eine Fülle von Angriffsmöglichkeiten bestehen.

3.7 Benutzer, Policy Management, Portal

Für jedes biometrische System muss es ein nichtbiometrisches Alternativsystem geben, da es gewisse Umstände gibt, die Biometrie nicht zulassen. So zum Beipiel kann es vorkommen, dass es Benutzer gibt, die für das Fingerabdrucksystem nicht geeignet sind, weil Merkmale fehlen oder unzureichend vorhanden sind. So bei 2-4% der deutschen Bevölkerung. Möglich ist auch, dass bei vorrübergehenden Krankenheiten oder Verletzungen das biometrische System nicht genutz werden kann. Ebenso kann das biometrische System

von einigen Benutzern schlichtweg abgelenht werden. Gründe hierfür sind beispielsweise Hygiene, Misstrauen oder Unwohlsein bei der Aufnahme des Merkmals. Für all diese Benutzer muss es ein entsprechendes nichtbiometrisches System mit gleicher Sicherheit geben, um diese nicht auszuschliessen. Ein Alternativsystem musss ebenso vorhanden sein für den Fall eines Systemausfalls. Mögliche Angriffspunkte liegen auch dann vor, wenn Risiken vom Managment falsch eingeschätzt werden und diese gezielt ausgenutzt werden könnnen. Ebenso kann auf erkannte Attacken inadäquat reagiert werden.

3.8 Portal

Das Portal stellt einen weiteren Angriffspunkt dar. Dort kann der Angreifer mit Hilfe eines autorisierten Benutzers Zugang erlangen. Dabei kann es sich um einen logischen oder physischen Zugang handeln. Bei einem physischen Zugang kann der Benutzer beispielsweise die Tür offen lassen oder den Angreifer Huckepack nehmen. Beiden Zugängen ist gleich, dass mit Zwang sich Zugang verschaft werden kann. Natürlich kann bei physischen Zugängen versucht werden diese gewaltsam zu öffnen.

3.9 Hardware

Hardware ganz allgemein kann Ziel eines Angriffes sein. Dabei kann der Angreifer versuchen die Hardware zu umgehen, deaktivieren oder modifizieren. Schwachstellen von Hardware können allgemein bekannt sein und ausgenutzt werden. Ebenso muss beachtet werden, dass Hardwarekomponenten altern und sich die Funktionalität unter Umständen herabsetzt. Auch sind bestimmte Komponenten der Witterung ausgesetzt.

3.10 Software und Firmware

Wie auch bei der Hardware kann der Angreifer versuchen die Software zu umgehen, zu deaktivieren oder zu modifizieren. Hierbei sind genügend Beispiele von nichtbiometrischen Systemen aus den Medien vorhanden. So muss man an dieser Stelle wieder betonen, dass dies nicht unbedingt einen Angriffspunkt der Biometrie darstellt.

3.11 Verbindungen zwischen Komponenten allgemein

Im Allgemeinen kann man sagen, dass bei allen Verbindungen zwischen Komponenten ein Angriffspunkt vorliegt. Angreifer könnten immer probieren Daten abzufangen oder einzufügen. Je nach Grad der Datencodierung und Erreichbarkeit der Leitungen kann sich dies einfach oder schwierig gestalten.

Kapitel 4

Spezielle Szenarien

Im folgenden Kapitel möchten wir anhand einiger spezieller Beispiele aufzeigen, welche Möglichkeiten existieren, schon mit einfachen praktischen Mitteln biometrische Systeme zu überlisten. Im Vordergrund sollen hierbei einfache Fingerabdruckscanner stehen, wie sie häufig auch für den Heimanwender angeboten werden. Neben dieser doch recht etablierten Möglichkeit Biometrie in Sicherheitssystem einzusetzen, sollen auch Überwindungsszenarien der Gesichtsgeometrie kurz Erwähnung finden. Im Falle der privaten Nutzung ist es im Besonderen relevant, auch die Schnittstellen (z.B. USB) zwischen Scannereinheit und verarbeitenden System (hier der PC oder Laptop) näher zu beleuchten.

4.1 Fingerabdruck

Der Fingerabdruck kann auf eine lange Geschichte zurückblicken, ist er doch vor allem in der Kriminalistik bei forensischen Untersuchungen ein altbekanntes und bewährtes Mittel, Personen zu identifizieren. Im Laufe der Jahre können Polizeibehörden weltweit ihre Verbrecherkartei mit diesem unverwechselbaren biometrischem Merkmal ausstatten. Die Hauptgründe für seine Erfolgsgeschichte in der Kriminalistik sind, dass fast jeder Mensch auf der Erde einen einzigartigen Fingerabdruck besitzt und diesen bei direkter Berührung mit Gegenständen auf denselbigen hinterlässt. Förderlich für seine Akzeptanz in biometrischen Sicherheitssystemen ist die Tatsache, dass relativ schnell ein Abbild des Fingers erstellt werden kann und die Analyse von markanten Linienbilder, den sog. Minuzien mit elektronischen Hilfsmitteln heute kein Problem mehr darstellt. Die langen Erfahrungen mit dem Fingerabdruck als Identifikationsmerkmal führen dazu, dass die Industrie heute hardware- sowie softwareseitig sehr günstige Komplettlösungen auf den Markt bringen kann. Mit diesem beispielsweise in einer Computermaus integrierten Sicherheitsmecha-

nismus, lässt sich heute schon der heimische PC oder Laptop vor unbefugtem Zugriff schützen. Ein hier am Institut unter Laborbedingungen durchgeführter Versuch [3] zeigt jedoch, dass diese Geräte in vielen Fällen nur unzureichenden Schutz bieten.

In der Praxis haben sich heutzutage drei Typen von Sensoren etabliert. Man unterscheidet hier

- kapazitiv
- optische
- thermische

Sensorik. Kapazitive Sensoren bestehen aus einer Matrix von Kondensatoren, die durch Auflegen eines Fingers Kapazitätsänderungen unterworfen sind. Diese Änderungen sind abhängig vom jeweiligen Abstand zur Haut. Betrachtet man nun diese Ladungsänderungen und bringt sie mit der Geometrie eines Fingers in Einklang, erhält man ein gutes Abbild eines Fingerabdrucks.

Bei Optischen Sensoren wird lediglich ein fotografisches Bild des Fingers mit Hilfe einer Kamera erstellt.

Thermische Sensoren nutzen die minimalen Temperaturunterschiede zwischen den Fingerlinien, genauer zwischen den Erhebungen (Hills) und den Tälern (Valleys) und erzeugen eine Wärmebild des aufgelegten Fingers.

Wie bei anderen biometrischen Systemen besteht eine Möglichkeit eines potentiellen Angriffsversuchs darin, dass biometrische Merkmal zu kopieren bzw. nachzuahmen. Wie weiter oben bereits erwähnt besitzen die Finger die Eigenschaft, bei Berührung mit Gegenständen natürliche Fettrückstände sog. Latenzbilder zu hinterlassen. Diese Eigenschaft lässt sich in vielerlei Hinsicht für einen Angriff nutzen. Die intuitivste Variante stellt in unseren Augen die Nachbildung des Fingers aus Material wie zum Beispiel Silikon oder Gelatine dar. Sie setzt natürlich das Vorhandensein eines guten Referenzabdrucks als Vorlage voraus. In der Praxis erwiesen sich die kapazitiven Sensoren mit diesem Täuschungsversuch als sehr anfällig. Hier zeigte sich auch, dass es in vereinzelten Fällen sogar möglich ist, das System mit bereits auf dem Sensor befindlichen Latenzfingerabdrücken zu überlisten. Die Reaktivierung dieser Fingerabdrücke gelang beispielsweise mit Hilfe von Klebeband oder etwas Folie und wahlweise mit Graphitpulver (siehe Abbildung 4.1). Ein einfaches Auflegen unter leichtem Druck ermöglichte hier den Zutritt. Erstaunlicherweise reichte in machen Situationen ein leichtes Anhauchen des Sensors und das System erkannte den Angreifer als autorisierten Nutzer. Eine etwas abenteuerliche Variante ist der Versuch, den Sensor mit einer mit Wasser befüllten Plastiktüte zu überwinden. Die sich zwischen

Tüte und Sensor bildende erhöhte Luftfeuchtigkeit führte zunächst zu Kapazitätsschwankungen im Sensor und in Folge zu einer Verifikation anhand des Latenzfingerabdrucks. (siehe Abbildung 4.1)

Abbildung 4.1: Latenzfingerabdruck mittels Graphitpulver und Wasser

Optische Sensoren erweisen sich als weniger feuchtigkeitssensibel. Sie bieten insbesondere auch gute Möglichkeiten Mechanismen für eine Lebenderkennung zu integrieren. Im Allgemeinen sollten ausgereifte optische Verarbeitungssysteme die Reaktivierung von Latenzbildern abwehren können. Diese Systeme erkennen zum Beispiel, ob es sich um ein 3D-Objekt eines Fingers handelt oder nur eine Nachahmung mit Hilfe einer planen Folie.

Zusätzlich können bei Fingerabdrucksystemen natürlich auch Replay-Attacken zum Angriffserfolg führen. Sie finden weiter unten noch gesonderte Erwähnung.

An dieser Stelle soll der Artikel „Biometrie und Sicherheit" von Manfred Bromba [4] nicht unerwähnt bleiben. Er zeigt auf, dass die Nachahmungsversuche von Fingerabdrücken in der Realität weitaus schwieriger zu realisieren sind, als es den Anschein hat. Der Autor weist auf die Qualität von Latenzfingerabdrücken hin, die sich unter Laborbedingungen und in der Praxis sehr stark unterscheidet. Viele Publikationen, die Biometrik als unsichere Systeme entlarven wollen, berücksichtigen hier nach Meinung Brombachs nicht, dass es in der Praxis weitaus schwieriger ist, wirklich saubere somit brauchbare Latenzfingerabdrücke zu erhalten. Sie stellen letztlich in vielen Fällen die Grundvoraussetzung für einen Angriffsversuch dar. Brombach definiert Sicherheit u. a. als Risikomaß eines erfolgreichen Angriffs, welches von folgenden Faktoren abhängt:

- die Wahrscheinlichkeit, dass sich jemand zu einem Angriff entschließt
- die Wahrscheinlichkeit, dass jemand bis zum Arbeitsplatz vordringt
- die Wahrscheinlichkeit, dass der Angreifer bei der Suche nach einem qualitativ brauchbaren Latenzfingerabdruck erfolgreich ist

- dass er ihn geeignet kopieren kann
- dass die Authentifikation gelingt.

Um einen Angriff erfolgreich durchführen zu können, müssen alle Schritte erfolgreich sein. Die Sicherheit hängt somit also grob vom Produkt der Einzelwahrscheinlichkeiten ab.

Viele Systeme bieten heutzutage darüber hinaus eine Latenzbild-Detektion an. Die Software macht sich hierbei den Umstand zu nutze, dass es selten gelingt, den Finger zweimal genau identisch zu platzieren. Ein Latenzfingerabdruck besitzt jedoch genau diese Eigenschaft. Zeigt ein Vergleich zwischen dem Abbild der letzten Verifikation und dem des aktuellen Fingerabdrucks eine signifikante Ähnlichkeit, verweigert das System den Zutritt und verhindert somit einen potentiellen Angriff. In einigen Ausarbeitungen findet man diesbezüglich den Hinweis, den Sensor nach jedem Gebrauch zu putzen, um den Latenzabdruck zu entfernen. Brombach hingegen stellte fest, dass sich bereits nach 5-maligem Auflegen des Fingers kein brauchbarer Fingerabdruck mehr rekonstruieren lässt. Abbildung 4.2 verdeutlicht dies anhand eines ID-Mousesensors. Vergisst der Nutzer einmal den Sensor zu reinigen, liegen einem potentiellen Angreifer somit relativ gute Latenzbilder des autorisierten Nutzers vor.

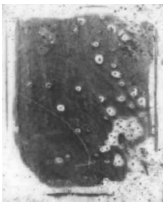

Abbildung 4.2: Latenzfingerabdruck auf einer Maus

Dieses Beispiel verdeutlicht, dass es doch sehr unterschiedliche Meinungen über die praktische Verwendung von Biometrischen Systemen gibt.

4.2 Gesichtsgeometrie

Schon seit Beginn der Menschheitsgeschichte nutzen wir intuitiv das biometrische Merkmal Gesicht, um Personen zu identifizieren. Ist es doch das Merkmal, dass für jedermann leicht erkennbar ist. Welche Leistungen hier das menschliche Gehirn im Bereich Mustererkennung vollbringt, wird erst dann deutlich, wenn man versucht ein Gesichtserkennungssystem in Hard- bzw. Software zu implementieren. Hier muss vor allem versucht

werden zu abstrahieren, d.h. sich auf die wesentlichsten Merkmale der Gesichtsgeometrie zu beschränken. Die Lage und Proportionen von Augen, Nase, Ohren und Mundwinkel stehen dabei im Vordergrund. Diese Daten lassen sich heutzutage mit modernen Bildverarbeitungssystemen gut auswerten. Die Notwendigkeit der Beschränkung macht es jedoch zunächst Angreifern relativ leicht, solche Systeme zu attackieren. Dabei hängt der Angriffserfolg vom eingesetzten Bildaufnahme- und Auswerteverfahren ab. Kamerasysteme, die im optisch-sichtbaren Bereich arbeiten lassen sich beispielsweise schon leicht durch ein auf die Lichtverhältnisse angepasstes Foto eines autorisierten Nutzer überlisten. Gelingt es dem Angreifer in den Besitz eines digitalen Fotos zu gelangen, sind solche „Optimierungen" mit aktuellen Bildbearbeitungsprogrammen kein Problem mehr. Es fällt sogar leicht, mehrere verschieden bearbeitete Fotos auszudrucken und diese dem biometrischen System zu präsentieren. Der Einsatz eines Laptops bietet zusätzlich die Möglichkeit, zur Darstellung des Fotos das Display zu benutzen und ggf. vor Ort das Bild hinsichtlich Helligkeit, Kontrast, Größe etc. anzupassen. Selbst wenn das Sicherheitssystem über eine Lebenderkennung verfügt, ist die Überwindung mit Hilfe eines vorgespielten Videostreams denkbar.

4.3 Schnittstellen zwischen Sensor und verarbeitenden System

Eine weitere Angriffsmöglichkeit besteht darin, die Software oder Hardware des Sicherheitssystems direkt zu attackieren. Hier sollen wiederum Heimanwendungen wie Laptop oder Desktop-PC im Vordergrund stehen. Größere Sicherheitssysteme, wie sie in Banken oder anderen Sicherheitsbereichen installiert sind, werden in der Regel zusätzlich durch Sicherheitspersonal und Kameras bewacht, sodass sich niemand unbemerkt an den Systemkomponenten zu schaffen machen kann. Natürlich sind aber auch hier Szenarien beispielsweise mit Hilfe eines Computervirus oder ähnlichen Programmen denkbar, die ein Restrisiko nicht ausschließen lassen. Relativ leicht zugängliche Sicherheitskomponenten, wie beispielsweise ID-Mouse, USB-Anschluss und Laptop können ein Sicherheitsrisiko darstellen. An dieser Stelle seien sog. USB-Sniffer erwähnt, die als Software- sowie als Hardwareversionen zur Verfügung stehen. Sie ermöglichen es, den USB-Datenverkehr zwischen einem Gerät (z.B. Sensoreinheit in Form einer ID-Mouse) und verarbeitenden System (z.B. Laptop) zu belauschen. Software-Sniffer klinken sich zwischen USB- und Geräte-Treiber direkt ins Betriebssystem ein und können beispielsweise mit Hilfe eines Virus auf den PC gelangen. Handelt es sich um einen unerfahrenen Nutzer, der beispielsweise den PC oder Laptop überwiegend mit Administratorrechten gebraucht, so ist es

kein schwieriges Problem ein solches „Spionageprogramm" einzuschleusen, welches den USB-Datenverkehr loggt und ihn über das Internet zur weiteren Analyse an den Angreifer schickt. Mit etwas Erfahrung lassen sich somit relativ leicht biometrische Daten ausspionieren und für einen späteren Angriff zum Beispiel mit einer Replay-Attacke missbrauchen. Etwas auffälliger ist der Einsatz von Hardware-Sniffern. Diese Geräte werden direkt an das USB-Kabel zwischen Sensor und USB-Anschluss angeschlossen. Sie arbeiten im Grunde ähnlich wie Software-Sniffer sind jedoch in Sachen Auffälligkeit und Bedienbarkeit unterlegen.

Ein weiteres Angriffszenario ist der vollständige Austausch der Sensoreinheit mit einer vom Angreifer präparierten Version. Der einfache Gebrauch von USB-Geräten im Besonderen das Anschließen bzw. Entfernen, ermöglicht dies relativ einfach zu bewerkstelligen. Moderne Sicherheitssoftware sollte einen solchen Austausch jedoch registrieren und entsprechend darauf reagieren können.

Kapitel 5

Gegenmaßnahmen

Der folgende Abschnitt soll sich mit Mechanismen beschäftigen, die verhindern sollen, biometrische Systeme mit einfachen Mitteln zu überwinden. Aufgabe eines biometrischen Systems ist es heutzutage nicht nur die Merkmale der autorisierten Nutzer zu beurteilen, sondern auch deren zweifelsfreie Herkunft zu überwachen. Ein in den Medien häufig auftauchender Begriff ist die sog. Lebenderkennung (engl. Life-Test). Darüber hinaus soll in diesem Kapitel auch auf SmardCards eingegangen werden. Sie stellen zwar keine direkte Gegenmaßnahme gegen Angriffe dar, sind jedoch ein wirksames Konzept, um die Sicherheit biometrischer Systeme erheblich zu steigern.

5.1 Lebenderkennung / Life-Test

Was bedeutet Lebenderkennung? Folgende Definition nach [7] soll hier zunächst die Begrifflichkeit klären:

„Unter Lebenderkennung wird die Überprüfung verstanden, ob die jeweiligen biometrischen Merkmale von einem lebenden Organismus und nicht von einer künstlichen Fälschung erzeugt wurden."

Dieser Test ist im Übrigen kein integraler Bestandteil eines biometrischen Algorithmus. Denkt man jedoch an die heutigen Möglichkeiten biometrische Merkmale auszuspionieren, ist er in modernen Sicherheitssystemen nicht mehr wegzudenken. Beispielsweise macht die zunehmende Verbreitung von teilweise auch immer kleiner werdenden Digitalkameras (Bsp. Handykamera) es heutzutage zum Kinderspiel, mehrere Fotos von einer Person unbemerkt aufzunehmen und für die Zwecke einer Verifikation mittels Gesichtserkennung zu missbrauchen. Sicherheitssysteme mit Lebenderkennung sind dennoch nicht unüberwindbar. Wie im vorherigen Kaptitel bereits dargestellt, reicht in manchen Fällen

etwas Kreativität aus, um dem System eine lebende Person vorzugaukeln. Der Erfolg hängt natürlich von der Komplexität der Überprüfung ab. Werden mehrere Merkmale geprüft, die ein lebender Organismus vorweisen muss, wird es für den Angreifer erheblich schwieriger ein brauchbares Imitat zu erstellen. Aktuelle Verfahren zur Lebenderkennung machen sich gewisse Eigenschaften der Haut, sowie Bewegungen beispielsweise in Gesicht und Auge zu nutze. Zu den typischen Hauteigenschaften gehören Farbe, elektrische Leitfähigkeit, Reflexionsverhalten und Wärmeabstrahlung. Die Überprüfung auf elektrische Leitfähigkeit lässt sich gut in Fingerabdrucksensoren oder Handgeometriesscannern integrieren; Hautreflexion und Farbe sind auch ohne weiteres bei Gesichtserkennungssystemen realisierbar. Die Temperaturunterschiede der Haut können mit Hilfe einfacher Infrarotabtastung analysiert werden. Die Tatsache, dass wir unser biometrisches Merkmal nie in vollständige Ruhe versetzen können, macht es der Lebenderkennung möglich, kleinste Bewegungen zu registrieren, die auf einen lebenden Organismus schließen lassen. So können Bewegungen von Lippen, Augenlidern und Kopf hilfreich beim Unterscheiden von lebenden Personen und Gesichtsattrappen sein. Bei der Iriserkennung ist bekannt, dass sich durch Helligkeitseinfluss die Pupille erweitert. Dieser Effekt und andere Eigenschaften wie die Wölbung der Augen sind hilfreiche Indizien, um künstliche Augen von echten zu differenzieren. Durch Algorithmen der Mustererkennung lassen sich auch mit Hilfe von Methoden der Signalverarbeitung durch Tonband aufgenommene Stimmen von autorisierten Nutzern entlarven. Ein in der Medizin eingesetztes Verfahren, dass ebenfalls in Fingerabdrucksystemen Anwendung findet ist die Pulsoxymetrie. Durchleuchtet man einen Finger mit rotem und infrarotem Licht, lassen sich Pulsschlag und Blutzirkulation nachweisen. Der Grund dafür ist, dass sauerstoffreiches Blut mehr Licht dieser Wellenlänge absorbiert als sauerstoffarmes.

Dass diese wie auch andere Verfahren teilweise große Akzeptanzprobleme haben, wird deutlich, wenn beispielsweise die durch Pulsoxymetrie oder Iriserkennung gewonnen Daten für andere Zwecke verwendet werden. Hämoglobingehalt sowie Pulsfrequenz können beispielsweise Hinweise über den Gesundheitszustand eines Nutzers geben. Ein Irisscan kann unter Umständen sogar Spekulationen auf ernsthafte Erkrankungen anregen. Lebenderkennung muss sich somit Vorwürfen den strengen Datenschutzrichtlinien in Deutschland nicht gerecht zu werden, erwehren. Neben dem Akzeptanzproblem hat Lebenderkennung auch mit weiteren Problemen zu kämpfen. Zum einen ist sie heute noch relativ teuer und teilweise aufwendig zu integrieren, zum anderen verlängert deren Einsatz die Gesamtverifikationsphase um einen nicht unbeachtlichen Anteil der eigentlichen Verifikationsdauer.

5.2 Smardcards

Smardcards werden von vielen als der neue Trend proklamiert. Sie sind nicht größer als die weit verbreiteten Chipkarten, die heutzutage jeder in seiner Brieftasche vorfindet und bieten Vorteile, die dem Nutzer die Akzeptanz von biometrischen Sicherheitssystemen erleichtern könnte. Im Laufe der Zeit wurden mehrere Systeme entwickelt, die jedoch alle die zwei Verifikationsmethoden Besitz und biometrisches Merkmal kombinieren. Die Grundidee ist, dass sich ein Template eines biometrischen Merkmals (meist der Fingerabdruck) auf der Smardcard befindet, welches dem Besitzer zuzuordnen ist und bei der Überprüfung herangezogen wird. Der Besitzer wird nur dann als autorisiert eingestuft, wenn das Smardcardexemplar mit dem bei der Prüfphase erstellten Template übereinstimmt. Ein entscheidender Vorteil ist, dass das Template nicht in einer zentralen Datenbank abgelegt wird, sondern auf der Smardcard gespeichert ist und der Nutzer somit im ständigen Besitz seines Templates ist. Selbst bei Verlust oder Diebstahl kann einem Missbrauch mit einer Kartensperrung begegnet werden. Auch eine Kompromittierung von biometrischen Merkmalen ist eher unkritisch zu betrachten, da ohne den Besitz der Smardcard und dem sich darauf befindlichen Template kein Verifikationsversuch gelingen wird. Auf den Chips der Smardcards können natürlich noch weitere Nutzerdaten hinterlegt werden. Diese Vielseitigkeit dehnt nicht nur das Anwendungsspektrum erheblich aus, sondern erhöht auch merklich den Komfort der Handhabung. So ist es beispielsweise nicht mehr erforderlich, Eingaben wie Anwender-ID oder ähnliches während der Überprüfung zu leisten. Einige Firmen, die solche Smardcards herstellen werben damit, dass ihr Card-System in naher Zukunft viele der im Umlauf befindlichen Identifikationsmittel und auch Karten aus dem Bereich „elektronic-cash" vereinen könnte. Personalausweis, Reisepass, Führerschein, Krankenkassekarte, Bank- und Kreditkarten sind nur einige Beispiele, die die möglichen Einsatzbereiche von Smardcards beschreiben.

Im Folgenden soll kurz auf die unterschiedlichen Smardcard-Systeme eingegangen werden, die sich in den letzten Jahren etabliert haben.

5.2.1 Template on Card

„Template on Card"-Systeme zeichnen sich dadurch aus, dass Smardcards lediglich als Speicherort für biometrische Referenztemplates dienen. Das Enrolement sowie die Verifikation erfolgt mit externen Geräten, zum Beispiel mit Hilfe eines PCs oder eines Smardcard-Readers mit integriertem Sensor. Da bei diesem System biometrische Daten an Fremdgeräte übertragen werden, ist ein Restrisiko durch Kopieren bzw. Ablauschen der Daten nicht auszuschließen. Der erste Schritt dieses Restrisiko zu minimieren bestand darin, die Templatedaten verschlüsselt abzuspeichern. Mehr Sicherheit bieten Chipkarten

mit integrierten Kryptoprozessoren. Sie erlauben es eine sichere Verbindung zum Lesegerät aufzubauen, um somit eine Ablauschen der Templatedaten zu verhindern.

5.2.2 Match on Card

Bei „Match on Card"- Systemen handelt es sich um Chipkarten mit integrierten Matchingprozessor. Über den Umweg einer externen Sensoreinheit ist es möglich, den Matchingalgorithmus auf der Smardcard auszuführen. Controllereinheit und Speicher sind ebenfalls Bestandteile dieser Technologie. Sie stellen somit eine sicherere Alternative zu den bereits beschriebenen „Template on Card"- Systemen dar, denn das Template verlässt bei diesem Verfahren die Smardcard nicht, kann somit auch nicht ohne weiteres abgefangen werden.

5.2.3 Sensor on Card

Wie der Name vermuten lässt, werden Smardcards mit integrierter Sensoreinheit als „Sensor on Card" - System bezeichnet. Anders als bei der „Match on Card" - Variante wird der Verifikationsprozess jedoch außerhalb durchgeführt. Neben dem Komfort seinen eigenen Fingerabdrucksensor mitzuführen, eröffnet das Übertragen von Templatedaten zum externen Matchingprozessor wiederum Raum für einen Angriff auf biometrische Daten.

5.2.4 System on Card

„System on Card" - Systeme stellen zurzeit das sicherste Verfahren dar, biometrische Verifikation mit Hilfe einer Chipkarte durchzuführen. Smardcards dieser Variante vereinen alle Vorteile der oben vorgestellten Systeme. Heute ist es möglich Mikrotechnologie zur Erfassung und Speicherung der biometrischen Daten sowie deren Verarbeitung und Ausgabe auf einer Chipkarte unterzubringen. Da der Anwender weder sein biometrisches Merkmal noch sein Referenztemplate weitergeben muss, bietet dieses System einen optimalen Schutz und sollte auch geltenden Datenschutzbestimmungen gerecht werden. Der Einsatz von „System on Card" gestaltet sich darüber hinaus als außerordentlich flexibel, da vor Ort keine zusätzliche Hardware installiert werden muss.

Abbildung 5.1: System on Card

Mobile Kleingeräte (Abbildung 5.1), die ohne größeren Installationsaufwand eingesetzt werden können, machen teurer Umbauten an vorhandenen Sicherheitssystemen überflüssig und ermöglichen biometrische Verifikation für unterwegs. In Zukunft werden auch Merkmale wie Gesicht, Iris, Stimme etc. ihre Verwendung in „System on Card" - Systemen finden.

Kapitel 6

Schlussbemerkungen

6.1 Eigenschaften unterschiedlicher Authentifikationssysteme

Betrachtet man die Möglichkeiten biometrische Systeme zu überwinden, sollte man ebenso alternative Authentifikationssysteme betrachten. Somit kann man Vor- und Nachteile der jeweiligen Systeme besser beurteilen und feststellen, ob ein besserer Schutz überhaupt möglich ist. Wie in den vorigen Kapitel bereits erwähnt, muss man besonders darauf achten, inwieweit die Schwachstelle dem System anzulasten ist oder es für alle gilt. Somit ist es sinnvoll sich mit den Eigenschaften der Systeme zu beschäftigen, die zu den Möglichkeiten der Überwindung führen. Die betrachteten alternativen Systeme sind hier Wissen, wie Passwort oder PIN, und Besitz, wie Schlüssel oder Ausweis.

6.1.1 Verlust

Angefangen mit der Eigenschaft Verlust hat die biometrische Identifikation einen gewissen Vorteil. Das Passwort kann schnell vergessen werden und es muss eine Möglichkeit geben ein Neues zu beantragen. Hierbei muss der Benutzer erneut authentifiziert werden, um zu prüfen, ob er wirklich berechtigt ist ein neues Passwort zu erhalten. Beim persönlichen Besitz kommt es vor, dass der Gegenstand verloren geht und der Finder in der Lage wäre diesen Gegenstand zu benutzen. Bei Biometrie ist es jedoch kaum möglich sein Authentifikationsmittel zu verlieren und stellt somit mehr Sicherheit zur Verfügung.

6.1.2 Diebstahl

Ebenso wie der Verlust ist auch der Diebstahl möglich. Hierbei kann das Passwort ausspioniert oder die Zugangskarte gestohlen werden. Beides kann anschließend für den autorisierten Zugang benutzt werden. Bei dem biometrischen Merkmal gestaltet sich dies jedoch schwieriger, so dass auch hier mehr Sicherheit gewährleistet ist.

6.1.3 Weitergabe

Eine andere Möglichkeit Sicherheitssysteme zu überwinden besteht darin, dass autorisierte Benutzer ihr Authentifikationsmittel, also Schlüssel, Passwort oder biometrisches Merkmal weitergeben. Bei der biometrischen Identifikation nutzt dies jedoch noch nichts, da das Merkmal in entsprechender Form weiterverarbeitet werden muss. Bei den anderen Verfahren ist dies jedoch einfacher. So kann recht einfach das Passwort weitererzählt oder der Schlüssel verliehen werden.

6.1.4 Änderbarkeit

Die Änderbarkeit bei der biomtrischen Identifikation ist etwas problematischer als bei den Anderen. So kann beispielsweise bei Vergessen des Passwortes ein Neues eingerichtet werden. Nach der Aktivierung des neuen Passwortes existiert der gleiche Schutz wie vorher mit dem Alten. Bei der Authentifikationart Besitz verhält es sich ähnlich. Verliert jemand sein Schlüssel zur Wohnung, kann das Schloss ausgewechselt werden und der alte Schlüssel ist unbrauchbar. Auch hier erhält man die gleiche Sicherheit zurück. Wird ein biometrisches Merkmal gestohlen besteht die Gefahr, dass es zur Überwindung des biometrischen System eingesetzt werden kann. Bei biometrischen Merkmalen, die am menschlichen Körper mehrmals auftauchen, wie zum Beispiel die Finger, könnte ein anderes jedoch gleiches Merkmal benutzt werden. Bei Merkmalen, die nur einmal am Körper existieren, besteht diese Möglichkeit nicht und die Gefahr eines Angriffes mit diesem Merkmal ist vorhanden. Dabei besteht nicht nur für dieses System ein erhöhtes Risiko, sondern womöglich auch für andere Systeme, auf diesen der Benutzer sich mit gleichen Merkmal eingerichtet hat. Hinzukommt, dass das biometrische Merkmal normalerweise ein lebenlang besteht und die Problematik bei erneuter Benutzung des Merkmals bestehen bleibt.

6.2 Fazit

Unter allen vorgestellten Möglichkeiten biometrische Systeme zu überwinden, kann man feststellen, dass viele Überwindungsmöglichkeiten auch für nichtbiometrische System gelten. Lässt man die gleichen Überwindungsmöglichkeiten weg und betrachtet nur die jeweilige Authentifikationsart, kann man, wie im vorigen Kapitel, sich an den Eigenschaften orientieren, welche Authentifikationsart Vor- und Nachteile in Bezug auf die Überwindung mit sich bringt. Gerade das letzte Kapitel hat gezeigt, dass Biometrie andere Vor- und Nachteile gegenüber Nichtbiometrie hat. Daher muss für ein System entschieden werden, inwiefern Biometrie alleine oder in Kombination mit anderen eingesetzt werden soll. Dabei muss natürlich der Aufwand in einem entsprechenden Verhältnis zum Nutzen stehen. Auch die Kosten haben hier einen entscheidenen Anteil. Leider geben Firmen ihr Wissen und ihre Erfahrung mit der Überwindung von Biomtrie nicht preis, um keine Schwachstellen zu veröffentlichen oder dem Firmenimage zu schaden. Dadurch ist es kaum möglich sichere Aussagen für die Praxis zu tätigen. Zusammenfassend kann man jedoch sagen, dass Biometrie immer einer gezielten Einsetzung und Nutzung bedarf und nicht die Lösung für alle Probleme darstellt.

Literaturverzeichnis

[1] UK Government Biometrics Working Group. Biometric Device Protection Profile (BDPP). Draft Issue 0.82. Semptember 2001.

[2] Common Criteria Biometric Evaluation Methodology Working Group. Biometric Evaluation Methodology Supplement (BEM). Version 1.0. August 2002.

[3] Thalheim, Krissler,Ziegler. Biometric Access Protection Devices and their Programs Put to the Test.
http://www.heise.de/ct/english/02/11/114/ , November 2002.

[4] Manfred Bromba. Biometrie - Fragen und Antworten.
http://www.bromba.com/faq/biofaqd.htm , Oktober 2004.

[5] Christian Paulsen. Risikoanalyse von biometrischen Systemen.
Diplomarbeit , August 2003

[6] Astro Datensysteme AG. BioSmardCard. White Paper Version 3.02.

[7] Brigitte Wirtz. Datenschutz und Datensicherheit, 1999.