Authentifizierung durch Sprache
Potenziale und Grenzen biometrischer Systeme

Andreas Wolf und Joerg Tacke

VOICE.TRUST AG
Landshuter Allee 12-14
80637 München
aw@voicetrust.de, jt@voicetrust.de

Zusammenfassung: Biometrie ist in aller Munde. Spätestens seit den nach dem 11. September 2001 erhobenen Forderungen nach mehr und besseren Personenkontrollen rufen Politik und Wirtschaft verstärkt nach biometrischen Lösungen. Was ist aber überhaupt Biometrie? Allheilmittel oder Teufelszeug? Wie zuverlässig sind biometrische Lösungen? Welche Probleme können mit ihnen gelöst werden? Welche nicht? Wofür ist Biometrie besonders gut geeignet? Alle diese Fragen sollen mit diesem Artikel am Beispiel der Benutzerverifikation durch Sprache angesprochen werden.

1 Einleitung

Spätestens seit den Ereignissen am 11. September 2001 und den danach erhobenen Forderungen nach möglichst lückenloser Überwachung sensibler Orte sind biometrische Methoden in starkem Maße in das Blickfeld der Öffentlichkeit gerückt. Auch die Bundesregierung, Innenministerien der Länder und Betreiber sicherheitskritischer Einrichtungen wie etwa Flughäfen und Atomkraftwerke untersuchen, wie man Biometrie zur Absicherung öffentlicher Interessen verwenden kann.

Was ist in diesem Kontext überhaupt unter Biometrie zu verstehen? Wie funktioniert sie? Welche Merkmale kann man in technischen Systemen auswerten? Was kann Biometrie überhaupt leisten? Wo liegen ihre Grenzen? Abschnitt 3 will mithelfen, über diese Fragestellungen zu diskutieren. Dabei möchten die Autoren insbesondere ihre Erfahrungen aus der Arbeit für die VOICE.TRUST AG, einem Hersteller für sprachbasierte Authentifizierungstechnik, einbringen.

Um die Einsatzmöglichkeiten der Biometrie beurteilen zu können, ist es notwendig, biometrische Systeme als Authentifikationssysteme zu identifizieren, mit denen die Identität von Personen festgestellt oder überprüft werden kann. Wir ordnen in Abschnitt 2 die Biometrie in die Gesamtheit der Authentifikationssysteme ein und vergleichen sie mit anderen Authentifikationsprinzipien.

Am Beispiel der Benutzerverifikation durch Sprache wird in Abschnitt 4 die Funktionsweise eines typischen biometrischen Systems erläutert. Abschnitt 5 skizziert typische Einsatzszenarien für Sprachverifikation und die Probleme, die bei Einführung und Betrieb von Biometrielösungen häufig auftreten. Abschnitt 6 bewertet die durch biometrische Systeme

typischerweise erreichbare Zuverlässigkeit in Bezug auf Sicherheit (=Security) und Verfügbarkeit und ordnet diese Angaben in das Rahmenwerk der Common Criteria (CC) als internationalem Standard für IT-Security ein.

Das Papier schließt in Abschnitt 7 mit einer zusammenfassenden Bewertung und einem Ausblick auf das, was wir möglicherweise künftig von der Biometrie erwarten dürfen.

2 Authentifizierungstechniken

Authentifizierungssysteme sind häufig Bestandteil von Lösungen zum Access Control Management (ACM), die Komponenten zum Authentifizieren und Autorisieren von Benutzern, zum Auditing und zur Rechte-Administration beinhalten. Die Authentifizierung eines Benutzers umfasst die Überprüfung (*Verifikation*), in manchen Fällen auch die Feststellung seiner Identität (*Identifizierung*). Sie ist jedenfalls klar abgegrenzt von der Feststellung eventueller Berechtigungen, die aufgrund der überprüften Identität für den Zugriff auf bestimmte Ressourcen zum Beispiel in IT-Systemen erteilt werden können (*Autorisierung*). Auf dem Markt erhältliche biometrische Systeme können mit unterschiedlicher Präzision sowohl Identifizierung als auch Verifikation durchführen. Identifizierung ohne aktive Mitwirkung des Betroffenen ist durch biometrische Techniken überhaupt erst möglich, man denke etwa an die auf einigen Flughäfen derzeit in Erprobung befindlichen Gesichts-Scanner.

Authentifikationsverfahren können in drei Klassen unterteilt werden. Sie fragen geheimes *Wissen* des Benutzers ab, überprüfen den *Besitz* von speziellen, schwer zu fälschenden Dingen oder verwenden *persönliche Eigenschaften* des Benutzers für seine Identifizierung oder Verifikation. Letztere sind die biometrischen Verfahren.

Um sich gegenüber einem Bankautomaten oder Computersystem zu identifizieren, werden heutzutage hauptsächlich Mechanismen wie Passwort und PIN (*Wissen*) oder Chipkarten (*Besitz*) verwendet. Hier besteht des Problem des *Vergessens* bzw. des Verlusts. Biometrische Verfahren, die auf individuellen Charakteristika des Menschen (*Sein*) beruhen, haben demgegenüber den Vorteil, dass diese nicht ohne weiteres gestohlen oder ausgespäht werden können. Häufig sind biometrische Authentifizierungsmechanismen darüber hinaus komfortabler zu bedienen. Damit können sie zu einer besseren Datensicherheit beitragen. Viele biometrische Merkmale sind der Natur der Dinge nach bereits *öffentlich zugänglich*. Wir hinterlassen unsere Fingerabdrücke auf allen Dingen, die wir berühren, das Gesicht und die Irisringe einer Person sind in der Regel ständig sichtbar. Diese Eigenschaften biometrischer Merkmale führen einerseits zu einer Reduktion der mit Verlust oder Kompromittierung verbundenen Gefährdungspotenziale, bringen aber andererseits neue Risiken mit sich. Wie bei allen Sicherheitstechniken, so muss auch hier die Entscheidung für den Einsatz der einen oder der anderen Technik nach vorheriger Analyse der vorhandenen zu schützenden Güter und ihrer Bedrohungen getroffen werden.

Typische Einsatzbereiche liegen in der Zugangs- oder Zugriffskontrolle. Doch auch bei der Abgabe von Willenserklärungen, z. B. im Zusammenhang mit der digitalen Signatur, können biometrische Verfahren zur Freischaltung eines privaten Schlüssels dienen. Für Verfahren nach dem Signaturgesetz ist zur Zeit geregelt, dass biometrische Merkmale

zusätzlich zu einer Identifikation des Inhabers durch Besitz und Wissen nutzbar sind (§16 Abs. 2 SigV) [Va03].

3 Biometrie

Zunächst sollte kurz die Frage erläutert werden, worum es sich bei Biometrie und Biometrik handelt. Anfang des 20. Jahrhunderts wurde unter Biometrie (engl.: biometrics) die Entwicklung statistischer Methoden für die Biologie verstanden. Der Einfluss des Wetters auf die Ernteerträge, die Wirksamkeit medizinischer Therapien oder die Auswirkungen von Wasserverschmutzungen auf den Fischbestand sind nur einige Beispiele für traditionelle biometrische Fragestellungen. In jüngerer Zeit wird der Begriff nun auch für Methoden gebraucht, die sich mit der Identifikation von Personen mit Hilfe biologischer Merkmale beschäftigen. Bei Verwendung der Bezeichnung Biometrik soll meist der Aspekt der Automatisierung hervorgehoben werden. Biometrie ist ursprünglich die Wissenschaft und Technologie von der Messung und der statistischen Analyse biologischer Signale. Biometrik ist das automatisierte Messen von spezifischen Merkmalen eines Lebewesens [Me03].

Biometrische Verfahren können in passive und aktive Verfahren unterteilt werden. Passive Verfahren sind solche, bei denen *offensichtliche* Merkmale des Benutzers ohne aktive Mitarbeit der Person herangezogen werden, wie Gesicht, Iris, Retina, Fingerabdruck, Ohr, Handgeometrie, Körpergeruch oder Struktur der DNA. Aktive Verfahren sind solche, bei denen der Benutzer zu ihrer Durchführung nicht nur präsent sein, sondern auch aktiv mitwirken muss, wie sprachbasierte Verfahren, Schriftanalyse und Schreibverhalten, Tastaturanschlagsrhythmus oder Ganganalyse. Außerdem unterteilt man biometrische Verfahren nach der Veränderlichkeit des verwendeten Merkmals in statische und dynamische. Zu den statischen zählen etwa Iris- und Fingerabdruckscan. Unterschrifts-, Sprach- oder Ganganalyse sind dynamische Verfahren. Diese Klassifizierung ist mit gewisser Toleranz zu beurteilen, da sich z. B. durch Gewichtszunahme oder Verletzungen auch Fingerabdrücke in gewissem Umfang verändern. Hierzu siehe auch [Ot03]. Eine Übersichtsdarstellung heute gebräuchlicher biometrischer Verfahren ist in Abbildung 1 angegeben.

Die Themen Akzeptanz, Datenschutz und Peripheriekosten bestimmen den Grad der Einsetzbarkeit der Verfahren. So hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) folgendes als Kriterium für biometrische Systeme festgelegt: Bei biometrischen Verfahren sollte grundsätzlich ausgeschlossen sein, dass ohne Kenntnis der Betroffenen von diesen ein biometrisches Merkmal technisch erfasst wird. Vielmehr muß in jedem Fall die willentliche Mitwirkung des Nutzers erfolgen. Dies gilt sowohl für die Referenzdatenerfassung als auch für die spätere Überprüfung des biologischen Merkmals des Betroffenen. Eine aktive Mitwirkung des Nutzers macht das Verfahren zudem transparenter, baut daher unberechtigte Ängste ab und leistet damit einen positiven Beitrag zur Akzeptanz des Systems bei. Wegen Verletzung des Rechts auf informationelle Selbstbestimmung sind daher grundsätzlich solche Installationen abzulehnen, bei denen z. B. beim bloßen Passieren einer bestimmten Stelle für die Betroffenen unerkennbar biometrische Merkmale erfasst werden [DS03].

Verfahren	Erläuterung	Vor-/Nachteile
Handgeometrie	Geräte erfassen die Abmessungen der Finger und die Dicke der Hand oder liefern auch ein Venenbild.	Vorteil: schon seit mehr als zehn Jahren im Einsatz. Nachteil: Die geometrischen Abmessungen von menschlichen Händen unterscheiden sich nicht genügend. Nachteil Peripheriekosten. Zusätzlicher Sensor für Lebenderkennung notwendig. Userunterstützung nur mit zusätzlichem Medium möglich.
Retina	Die Struktur des Augenhintergrundes wird mittels eines ungefährlichen Laserstrahls abgetastet	Vorteil: theoretisch sehr fälschungssicher, relativ einfache Lebenderkennung. Nachteil: Peripheriekosten, Ängste der Benutzer, die Augen mittels Laser abtasten zu lassen. Userunterstützung nur mit zusätzlichem Medium möglich.
Iris	Die Farbverläufe im nahen Infrarotbereich (NIR) der Iris werden analysiert	Vorteil: theoretisch sehr fälschungssicher und niedrige Falscherkennungsraten von bis zu 1 zu 1.000.000. Nachteil: Peripheriekosten. Erfolgreiche Imposter-Tests der jüngsten Vergangenheit zeigen, dass die theoretische Fälschungssicherheit nicht unbedingt umgesetzt werden kann. Zusätzliches Verfahren für Lebenderkennung notwendig. Userunterstützung nur mit zusätzlichem Medium möglich.
Fingerabdruck	Fingerabdrücke sind von Mensch zu Mensch unterschiedlich und eignen sich hervorragend zur physiologischen Erkennung	Vorteil: bei zusätzlicher Lebenderkennung sehr fälschungssicher und niedrige Falscherkennungsraten von bis zu 1 zu 1.000.000; fortgeschrittene Datensatz-Standardisierung. Im Bankenbereich beruhen schon heute 68 Prozent der Biometrie-Anwendungen auf dem Fingerabdruckverfahren. Nachteil: durch den allgemein bekannten Einsatz bei der Polizei bei der Verbrecherjagd große Hemmnisse bei den Benutzern hinsichtlich der Persönlichkeitsrechte. Für Lebendtest zusätzlicher Sensor notwendig. Userunterstützung nur mit zusätzlichem Medium möglich.
Gesicht	Erkennung erfolgt auf den persönlichen Gesichtsmerkmalen	Vorteil: völlig berührungsfrei. Standards für Datensätze in der Erarbeitung. Nachteil: umfangreiche Datensätze erfordern schnelle und teure Systeme. Da das System auch zur Erkennung und Identifikation von Personen in der Öffentlichkeit angewandt werden kann, gibt es auch datenschutzrechtliche Probleme. Userunterstützung nur mit zusätzlichem Medium möglich.
Unterschrift	Erkennung der charakteristischen Unterschriftenmerkmale wie Dynamik des Schreibstiftes	Vorteil: wird vom Benutzer akzeptiert. Nachteil: Problem der Trennung variabler und invarianter Teile bei der Erkennung, hoher Zeitbedarf Userunterstützung nur mit zusätzlichem Medium möglich.
Stimme	Spektralanalyse eines (meist vorbestimmten) gesprochenen Wortes	Vorteil: Weltweit 1 Mrd. Festnetztelefone und 1 Mrd. Handys vorhanden. Somit nicht notwendigerweise zusätzliche Peripherie notwendig. Wird vom Benutzer akzeptiert. Kostenvorteil. Für Online-Hilfe und Lebendtest keine zusätzliche Technologie notwendig. Nachteil: Direkte, gleichlaute Stimmen oder dominante Geräusche nahe am Mikrofon führen zur Abweisung. Vorteil der vorhandenen Hardware korrespondiert mit deren Vielfalt (Cross-Channel-Problem)

Abbildung 1: Übersicht über heute gebräuchliche biometrische Verfahren.

4 Sprache als biometrisches Merkmal

Vom Verstehen des Gesprochenen einmal abgesehen, setzt ein Dialog Mensch-Maschine voraus, dass die sprechende Person von einem System erkannt und somit als Dialogpartner akzeptiert wird. So ist es bereits in einigen Unternehmen gängige Praxis, die Verwaltung ihrer Rechnernetzwerke durch eine Stimmerkennung zu unterstützen: Hat ein berechtigter Nutzer sein Passwort vergessen, ruft er eine bestimmte Nummer an. Er wird mit einem Computer verbunden, der ihn zum Nachsprechen von einzelnen Begriffen oder ganzen Sätzen auffordert. Anhand von bei der Erstanmeldung des Benutzers (Enrollment) gespeicherten Daten, den so genannten biometrischen Templates, kann der Rechner die betreffende Person verifizieren und ihr dann ein neues Passwort mitteilen.

Dass ein solches System funktioniert, verdanken wir den physiologischen Gegebenheiten des Menschen. Die Sprachorgane sind nämlich so komplex aufgebaut, dass sich ihre Anatomie und damit die Stimme selbst von Person zu Person deutlich unterscheidet. Der Klang, den wir beim Sprechen erzeugen, besteht aus einem Spektrum von Frequenzen, das sich je nach gesprochenem Laut verändert. Der Klang, der durch das Strömen der Luft durch die Stimmlippen im Kehlkopf entsteht, heißt Stimme. Dieses Signal aber wird durch

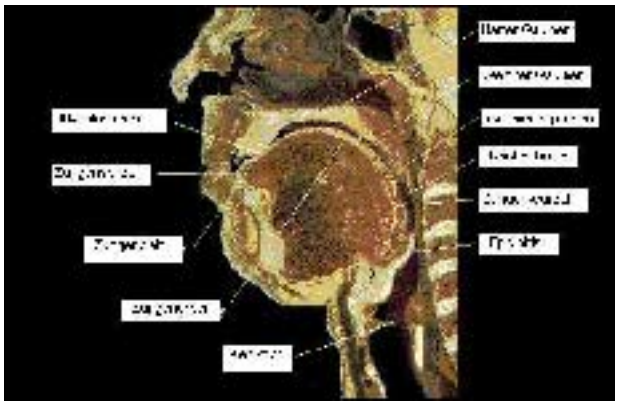


Abbildung 2: Schematischer Aufbau des menschlichen Sprachtraktes.

Resonanzen in Mundhöhle, Kehle und Nase charakteristisch verändert. Jeder Teil des Vokaltraktes lässt sich durch charakteristische Resonanzfrequenzen beschreiben. Auch die Anordnung, Form und Maße von Zunge, Kiefer, Lippen und Gaumen beeinflussen das Frequenzspektrum als Filter und Artikulatoren. Da diese Resonanzen dazu tendieren, das Frequenzspektrum der menschlichen Sprache zu *formen*, werden sie *Formanten* genannt. Was wir also von jemand anders hören, ist technisch gesehen Sprache, unabhängig von textlichem Inhalt. Die folgenden Abbildungen mögen einen Eindruck von der Komplexität der menschlichen spracherzeugenden Organe vermitteln.

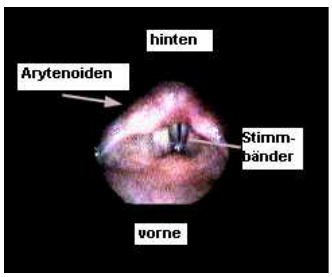


Abbildung 3: Ansicht der Stimmbänder [Co02].

Verhältnismäßig einfach erscheint da der Sensor zur Stimmerkennung: Ein Mikrofon wandelt das akustische Signal in ein elektrisches, eine nachgeschaltete Einheit macht daraus ein Bitmuster für die Verarbeitung im Computer. Die auf dem Rechner laufende Software ermittelt nun innerhalb des Frequenzmusters stabile Parameter (stabil bezieht sich darauf, dass diese trotz Erkältungen, Stimmungen, Umgebungseinflüssen, Stress etc. relativ unverändert bleiben), durch welche sich die Stimme des Sprechers mittels eines mathematischen Modells beschreiben lässt. Bei dieser Modellierung werden zunächst die Pausen

aus der gesprochenen Sequenz geschnitten. Das verbliebene Sprachmaterial wird in Abschnitte von 30 ms Dauer *blind segmentiert*. Dann werden die Formanten (siehe oben) errechnet. Mittels der *Pole-Filtered-Cepstrum* Methode wird das Cepstrum[1], welches die Stimmbandfrequenz von den Vokaltraktresonanzen trennt, bestimmt. Die Effekte, die der Übertragungskanal dem eigentlichen Sprachsignal hinzugefügt hat, werden durch Inversfilter eliminiert.

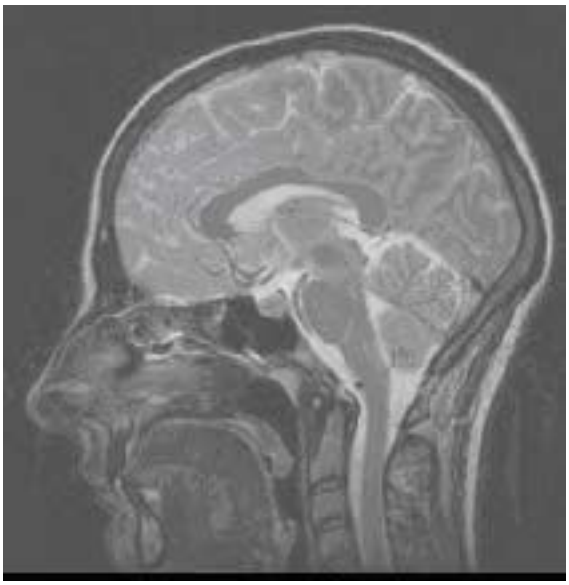
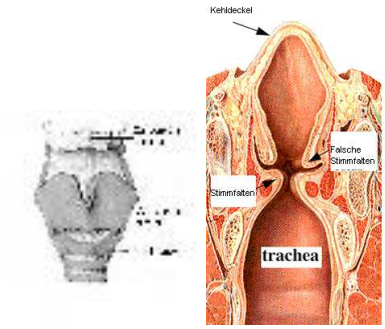


Abbildung 4: Querschnitt des menschlichen Kopfes und Halses [Co02].

Bei einer Verifikation wird das so aus den Registrierungsdaten gewonnene biometrische Template mit dem aus der aktuell vorliegenden Sprachäußerung erzeugten verglichen. Zur Reduktion der Fehlerquoten können mehrere Entscheidungsverfahren gleichzeitig angewendet werden. Gebräuchlich sind das *Hidden Markov Model* (HMM) und auch das *Neural Tree Network*, bei dem nicht nur die absoluten Werte der Parameter benutzt werden, sondern zusätzlich beurteilt wird, wie sich diese von denen anderer Personen unterscheidet [DHP99]. Die Methode des autoregressiven Modellierens ermöglicht ausreichend genaue Frequenzschätzungen anhand von kurzen Datensätzen. Verglichen mit der Fast Fourier Transformation erwies sich diese Methode als besser geeignet.

[1] Cepstrum wird mittels Fast Fourier Transformation die inverse Fouriertransformierte eines zuvor logarithmierten Spektrums berechnet, um die Anregungsparameter der Rohschallerzeugung von den Übertragungseigenschaften des Ansatzrohres besonders hervorzuheben. Daraus lassen sich in Grenzen wiederum der Grundton von Sprachschall und die Filtereigenschaften des Ansatzrohres ermitteln.



(a) außen (b) innen

Abbildung 5: Ansicht des Kehlkopfes von außen und innen.

4.1 Textabhängige Verifikation

Im einfachsten Fall, der textabhängigen Sprecherverifikation, werden dem Prozess immer gleiche Worte oder Sätze zugrunde gelegt. Ein Benutzer spricht bei der Registrierung diese festen Wörter mehrfach auf, der Computer ermittelt daraus die oben beschriebenen Templates und hinterlegt diese Informationen in einer Datenbank oder als Dateien im Filesystem. Um sich zu identifizieren, wird eine Person dann aufgefordert, eben diese festgelegten Ausdrücke zu sprechen.

Wie alle biometrischen Systeme arbeitet auch die Stimmerkennung um so besser, je sorgfältiger die Registrierung durchgeführt worden ist. Ungünstige Umgebungsbedingungen, in diesem Fall dominante Hintergrundgeräusche, verschlechtern das Ergebnis ebenso wie undeutliche Aussprache und minderwertige Sensoren, wenn das System derartige Faktoren nicht analysieren und und die Registrierung verweigern kann. Erfolgt der Dialog mit dem System über eine Telefonleitung oder ein Mobiltelefon, beeinflusst auch die Qualität der Verbindung den Vorgang, da das übertragene Frequenzspektrum von der verfügbaren Bandbreite des Übertragungskanals abhängt. Der Frequenzgang des Mikrofons hat ebenfalls erheblichen Einfluss auf die Übertragungscharakteristik des Sprachsignals.

Wie alle Sicherheitssysteme ist auch dieses letztlich zu täuschen, wenn keine entsprechenden Vorkehrungen gegen mögliche Bedrohungen getroffen werden. Ein Angreifer könnte die Stimme einer berechtigten Person mitschneiden und dem System vorspielen. Eine solche Replay-Attacke sorgt in Spionagefilmen für Hochspannung, doch der Aufwand ist sehr hoch. Der Angreifer muss in den Besitz der Aufnahmen gelangen und außerdem direkten Zugang zum Mikrofon erhalten. Wie anspruchsvoll das sein kann, illustriert der Film *Sneakers - Die Lautlosen* mit Robert Redford von 1992.

Wer ein solches Unterfangen aber als machbar unterstellt, kann sein System durch den Lebend-Test absichern. Dem Sprecher werden willkürlich verschiedene Phrasen vorgegeben, die er jedoch bereits vorher registriert haben muß. Diese Phrasen muß er unverzüglich

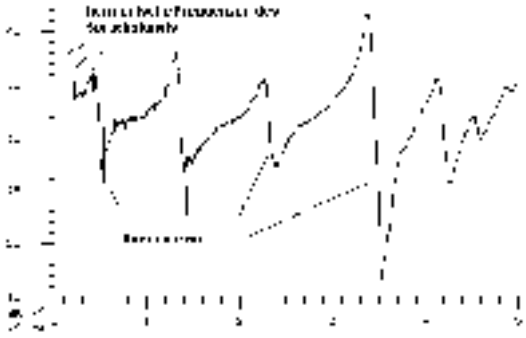


Abbildung 6: Harmonische und Resonanzfrequenzen als individuelle charakteristische Merkmale menschlicher Sprache.

nachsprechen. Es ist wenig wahrscheinlich, dass ein Angreifer die verlangte Sprachäußerung gerade mit der Stimme des richtigen Sprechers parat hat. Es sei denn, er hat sich in den Besitz des Templates, also des mathematischen Modells, für eben diese Worte gebracht. Dies könnte er jedoch nur nutzen, wenn er Zugang zur Sprecherverifizierungssoftware und deren Datenbank hat. Ein System zur Stimmresynthese anhand einer Spektralanalyse, wie es die Helden der *Mission Impossible*-Thriller einsetzen, ist reine Fiktion.

Selbst nach Aussage führender Hersteller von TTS-Systemen (TTS = text to speech), die davon ausgehen, dass zur Herstellung einer synthetischen Stimme nach dem Vorbild einer realen Person in mehreren Wochen gesammeltes Sprachmaterial von etwa 40 Stunden Umfang gewonnen werden muß, können solche Stimmen zumindest heute Sprachverifikationssysteme nicht erfolgversprechend angreifen.

4.2 Textunabhängige Verifikation

Die zweite Variante, die textunabhängige Sprecherverifizierung, erlaubt es, das gesamte Vokabular zu nutzen. Hierzu muß der Sprecher aber das System mit viel Sprachmaterial trainieren, was entsprechend lange dauert. Die Analyse des Frequenzspektrums der zu identifizierenden Person ist in diesem Falle nicht aufwändiger, aber ungenauer, denn das gespeicherte Referenzmuster, also die mathematische Beschreibung der spezifischen Parameter von Sprachäußerungen, bezieht sich nicht auf ein *Wort*, sondern allgemein auf die *Sprache* einer Person. Es werden die gleichen Technologien verwendet wie auch bei der textabhängigen Variante.

Studien in europäischen Verbundprojekten zeigten, dass die aus Fehlerraten für falschpositive Identifikation und falsch-negative Ablehnung berechnete *gewichtete Fehlerquote* zehnmal so groß ist wie beim Abfragen immer gleicher Ausdrücke [Lu99]. Deshalb tendiert die Branche derzeit dazu, eher mit festgelegten Sprachformeln zu arbeiten, aber dafür mehrere abzufragen. Das vermindert das Risiko eines erfolgreichen Angriffs und senkt die Fehlerquote auf nahezu Null, wie der TÜV IT Essen im Oktober 2002 bestätigt hat. Mit Hilfe des Lehrstuhls für Wirtschaftsinformatik III der Friedrich-Alexander-Universität Er-

langen-Nürnberg wurde ein Test durchgeführt, bei dem 120.000 berechtigte Zugriffe und 130.000 Angriffe auf den VOICE.TRUST Server erfolgten. Bei den empirisch ermittelten Fehlerraten gab es eine Systemkonfiguration, bei denen die falsche Akzeptanz (FAR) wie auch die falsche Zurückweisung (FRR) gleich Null war [GT02]. Eine Zusammenfassung der Ergebnisse dieser Studie ist in Abildung 7 angeführt.

4.3 Spracherkennung

Spracherkennung (ASR) ist die sprachbezogene Anwendung, die neben der Sprachgenerierung heute bereits die breiteste Verwendung findet. Spracherkennung und Sprachverifikation haben einen vergleichbaren mathematischen Hintergrund. Während die Erkennung dazu dient, Gemeinsamkeiten von Phonemen und Phonemkombinationen unterschiedlicher Sprecher zu finden und auszunutzen, sucht die Verifikation gerade nach Unterschieden zwischen den einzelnen Sprechern bei der Aussprache der einzelnen Sprachbestandteile. Spracherkennung kann für die Verifikation zur Qualitätssteigerung eingesetzt werden. Wenn jede Sprachäußerung vor der Bearbeitung durch die Verifikation mit einem Erkenner behandelt wird, dann kann auf diese Weise sichergestellt werden, dass die vom Benutzer zu sprechenden Phrasen in ausreichend guter Qualität dem vorgegebenen Phrasentext entsprechen. Damit sind nachlässige oder vorsätzlich in minderwertiger Qualität durchgeführte Registrierungen, etwa mit Pfiffen oder dergleichen, nicht möglich.

5 Einsatzgebiete von Sprachauthentifizierungen

Sprachverifikationstechnologien haben ohne Kombination mit zusätzlichen Techniken und Verfahren Fehlerraten von drei bis fünf Prozent. Das ist für viele praktische Anwendungen zu viel. Durch die Anwendung des bisher erworbenen Erfahrungsschatzes kann man die erreichbare Fehlerrate bis auf Werte der Größenordnung von einer fälschlichen Akzeptanz auf zehntausend Ereignisse bei einer moderaten Rate von fälschlichen Zurückweisungen reduzieren. Damit eignen sich sprachbasierte Verfahren entsprechend der Definition des vom BSI herausgegebenen IT-Grundschutzhandbuches für Anwendungen mit geringem und mittlerem Schutzbedarf. Die erreichbare Funktionsstärke kann man, wie bei anderen Authentifizierungstechniken auch, durch Kombination verschiedener Verfahren, die sogenannte Mehr-Faktor-Technik, deutlich erhöhen.

5.1 Anwendungen

Sprachverifikationssysteme sind heutzutage überwiegend in auf IVR-Plattformen (interactive voice response) ablaufenden Telefonieapplikationen eingebettet. Als Standard zur Steuerung der Kommunikation des Verifikators mit dem Benutzer kommt zunehmend VoiceXML [W303] zum Einsatz. Anwendungen für lokale und mobile Systeme wie etwa PDA und Mobiltelefone sind in der Entwicklung. Für die nahe Zukunft sind auch leistungsfähige embedded Systeme zu erwarten.

Arbeitszeiterfassung. Ein Dienstleistungsunternehmen im Baugewerbe nutzt die Sprecherverifizierung zur mobilen Zeiterfassung. Der Mitarbeiter ruft mit einem Mobiltelefon von der Baustelle den Authentifizierungsserver an, nennt seinen Namen und sagt, dass

er entweder seine Arbeit beginnt oder beendet. Der Server überprüft, ob die angegebene Identität (claimed identity = Name) mit den registrierten, sprachbiometrischen Merkmalen übereinstimmt, ruft über die vom Mobilfunkprovider bereitgestellten *location based services* die Standortkoordinaten des Telefons ab und schreibt diese in die Zeiterfassung.

Web-Access. Ein Zugang zum Intranet oder Internet kann auch ohne die sonst übliche Passwortabfrage erfolgen. Anstelle des Passwortes gibt der Benutzer die Telefonnummer ein, unter der er erreichbar ist. Der Authentifizierungsserver überprüft die Zugangsberechtigung des Benutzers und ruft ihn unter der angegebenen Rufnummer zurück. Nach dem bereits beschriebenen Authentifizierungsprozeß bekommt der Benutzer Zugang zur gewünschten Site.

E-Commerce. Im Bereich E-Commerce gibt der Benutzer anstatt einer Kontoverbindung oder Kreditkartennummer seine Rückrufnummer ein. Der Authentifizierungsserver authentifiziert den Käufer, fragt ihn, ob er den Betrag in Höhe von *X* Euro überweisen will, und löst die finanzielle Transaktion aus, ohne daß Kontonummer oder Kreditkartennummer in der laufenden Internet-Session übertragen werden müssen.

5.2 Projektdurchführung

Den größten Einfluß auf die erfolgreiche Einführung eines biometrischen Systems hat die Definition sinnvoller und realistischer Ziele in der Anfangsphase des Projektes. Hier muß geklärt werden, was das System leisten soll und welche Sicherheitsanforderungen gestellt werden. Ist ein Lebend-Test notwendig? Ist bei der Authentifizierung eine Person anwesend, die eine solche Komponente dann optional werden ließe? Es muß geklärt werden, in welcher Umgebung das System zum Einsatz kommt, um die Einflußfaktoren zu berücksichtigen [MW02] und entsprechende Richtlinien für den Einsatz festzulegen. Versäumnisse in dieser Phase sind später nur mit erheblichem Aufwand oder gar nicht zu korrigieren.

Für Großanwendungen müssen die Anforderungen zu den folgenden Themenkreisen festgelegt werden.

- Dialoge: Wie soll der Dialogfluß der Anwendung gestaltet werden? Welche Stimme wird für die Rückmeldungen des Systems an den Benutzer verwendet? Wie passen sich die geplanten Dialoge in die vorhandene Unternehmenskultur ein?
- Telefonanlage: Welche Anforderungen bestehen bezüglich der Zuordnung der Rufnummern und Kanäle?
- E-Mail-Anbindung: Welche Events sollen per E-Mail weitergeleitet werden? Hier ist insbesondere die eventuelle Notwendigkeit der Verteilung von Sicherheitsfunktion zu beachten.
- Sicherheits- und funktionale Parameter: Festlegung der Anforderungen bezüglich der vom Administrator zu parametrisierenden Regelgrößen des Authentifikationsverfahrens und der verbundenen Systeme (Datenbanken, Zielplattformen, Managementsysteme, Webserver etc.) und der ergonomischen Gestaltung der Oberflächen.
- Implementierung: Bei Einsatz des Systems als Passwort Reset Automat müssen die zu bedienenden Systeme festgelegt werden. Es muß geklärt werden, wie das System mit den erforderlichen Rechten Zugang zu diesen Zielplattformen erhält.

- Challenge/Response als Lebendtest: Das für die Durchführung eines Lebendtests notwendige Challenge/Response-Verfahren muß bezüglich seiner Anforderungen definiert werden. Welche Challenges sollen wie generiert werden? Wie oft sollen diese Challenges benutzbar sein? Mit dieser Funktion kann die bislang noch nicht ausreichend untersuchte *Alterung* des Sprachtemplates adressiert werden, indem der Benutzer bei jeder erfolgreichen Authentifizierung aufgefordert wird, eine neue Challenge zu registrieren. Unter Alterung von biometrischen Templates versteht man in diesem Zusammenhang die Steigerung der Erkennungsfehlerquote, die durch zeitbezogene Veränderungen im biometrischen Muster, seiner Darstellung und dem Sensor verursacht wird [MW02]. Die sprecherbezogene Varianz ist Teil des Phänomens der *Templatealterung*. [Fu81] stellt dar, dass die Intra-Sprecher-Varianz 3-4 Monate nach der ersten Aufnahme zunimmt und sich dann stabilisiert. Die bisherigen Forschungsergebnisse legen eine regelmäßige Erneuerung der Templates nahe, wie sie durch das bereits beschriebene Challenge/Response-Verfahren unterstützt wird.
- Einbindung in den Helpdesk: Welche Berechtigung hat der Helpdesk? Welche Rollen werden von Helpdesk-Mitarbeitern übernommen? Welche Rechte erfordern diese Rollen?
- Statistiken: Welche Anforderungen werden an die zu führenden Statistiken bezüglich des Security Audits und betriebswirtschaftlicher Erfordernisse gestellt?
- Performance und Return on Investment (RoI): Welchen betriebswirtschaftlichen Anforderungen unterliegt das Projekt und wie ist die Performance des Projektes meßbar.
- Vertrauenskette: Um die Vertrauenskette zu den registrierten Templates verfolgen zu können, muß jederzeit nachvollziehbar sein, welcher Superuser welchen Benutzer registriert hat. Das kann beispielsweise dadurch gesichert werden, dass immer ein vertrauenswürdiger Superuser bei der Registrierung anwesend ist (Superuser Enrollment).
- Benutzermanagement: Sollen die Templates und Berechtigungen der User mittels einem GUI verwaltet werden können? Erfolgt das Benutzermanagement über eine bereits vorhandene Datenhaltung, etwa eines Verzeichnisdienstes?
- Benutzerdatenimport: Für große Anwendungen ist ein automatisierbarer Benutzerdatenimport unabdingbar. Es müssen Formate geklärt werden, insbesondere auch die Qualität der zentralen Benutzerverwaltung. Fehlerhafte Daten, mit deren Auftreten bei großen Datenmengen immer gerechnet werden muß, führen in der Regel zu erheblichen Anlaufschwierigkeiten eines Biometrieprojektes.
- Error-, Event- und Log-File-Formate: Die Anforderungen an die Formate der Fehlerdateien und deren Einbindung in Management-Systeme müssen geklärt werden.
- Wartung und Datenreplikation: Die Verfügbarkeit des Authentifizierungsdienstes ist durch geeignete Mechanismen gerade für große und verteilte Anwendungen abzusichern.
- Alarmfunktionen: Enstprechend den Sicherheitsanforderungen sind die Fälle der automatischen Benachrichtigung verantwortlicher und zuständiger Personen zu definieren.
- Intrusion Detection: Es ist zu definieren, wie unberechtigte Benutzer entdeckt und behandelt werden sollen. Es sollten Schnittstellen zu verwendeten speziellen Intrusion Detection Systemen (IDS) festgelegt werden.

- Auto Locking: Die automatische Sperrung eines Benutzers im Falle des Mißbrauchs seines Accounts kann etwa bei dreimaliger aufeinanderfolgender Abweisung aktiviert werden.
- Housekeeping: Abhängig von der erforderlichen Systemleistung muß verhindert werden, daß die Festplatte des Servers vollläuft. Auto Locking und Housekeeping sind zudem ein wirksamer Schutz gegen Denial of Service Attacks.

Die rechtzeitige Kommunikation mit den betroffenen Anwendern und Verantwortlichen wie Management und Betriebsrat sind ein wesentlicher Erfolgsfaktor. Insbesondere sind hier auch die rechtlichen Aspekte des Datenschutzes zu beachten [DS03]. Da dem Datenschutz mit der Zustimmung des Betroffenen prinzipiell Gewährleistung getragen wird, ist diese einfache und sichere Variante frühzeitig in Betracht zu ziehen. Wir konnten bei der Einführung von Systemen, bei denen Komfort und Nutzen für den Benutzer sehr hoch sind, keine Ablehnung, sondern im Gegenteil sehr bereitwillige Annahme des Systems beobachten.

Nach dem Durchlauf der Phasen Definiton, Evaluierung, Design, Legal Review, Einkauf, Rolloutplanung, Installation, Training, Test und Test-Review kann der eigentliche Rollout beginnen. Im Fall der Sprachauthentifizierung via Telefon ist der Rollout denkbar einfach. Da das System per Telefon im Dialog Anleitungen und Korrekturanweisungen gibt, also über eine integrierte Audio-Online-Hilfe verfügt und zudem dem Benutzer die Tätigkeit des Telefonierens geläufig ist, reicht z. B. eine kurze Mail mit der Aufforderung zur Durchführung der Registrierung und einer kurzen Beschreibung des Ablaufes für die Organisation des Registrierungsprozesses, der hauptsächlich die zeitliche Koordinierung zu regeln hat. Insbesondere entfällt die Installation, Wartung und Einführung von zusätzlicher Hard- und Software auf der Benutzerseite vollständig.

Wird ein Benutzer gesperrt, muß Ihm im Gegensatz zu Token-basierten Systemen (Smart-Card o. ä.) kein neues Device bereitgestellt werden, was regelmäßig zusätzliche Kosten für Bestellung, Lagerung, Wartung, Fehleranalyse etc. einspart. Der Benutzer wird einfach erneut zur Registrierung berechtigt oder das bestehende Template reaktiviert.

Hier leitet sich eine weitere Anwendung von sprachbasierten Authentifikationssystemen ab, die Freischaltung, Suspendierung, Sperrung oder Neuausgabe von Smart Cards bzw. den damit verbundenen PINs in Public Key Infrastrukturen. Da die Authentifizierung maschinell erfolgt, können diese Vorgänge mit einer Sprachauthentifizierung sicher durchgeführt werden.

6 IT-Sicherheit

Spricht man im Kontext von Authentifizierungslösungen über Sicherheit, so sind dabei neben der erreichbaren Funktionsstärke auch Datenschutz- und Akzeptanzthemen zu untersuchen.

Fehler bei biometrischen Systemen sind fälschliche Akzeptanz (FA) und fälschliche Zurückweisung (FR). Fälschliche Akzeptanz heißt, dass das System eine Person A, welche behauptet, die Person B zu sein, als Person B akzeptiert. Fälschliche Zurückweisung bedeutet, daß das System eine berechtigte Person A als nicht berechtigt zurückweist. Die

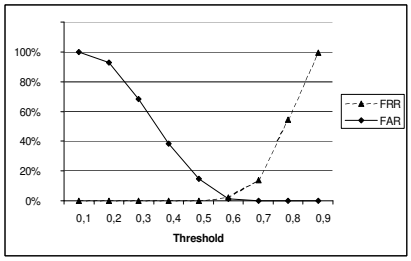
Fehlerquote der FA (FAR) beschreibt die Sicherheit eines Systemes, die Fehlerquote der FR (FRR) den Komfortlevel des Systems. Ein User muß bei einer niedrigen FRR nur selten mehrmals verifiziert werden. Während die FAR die primäre Sicherheit beschreibt, ist die FRR wichtig für die sekundäre Sicherheit eines biometrischen Systems. Ist der Komfort-Level eines Systems zu niedrig, ist die Motiviation der Benutzer hoch, dieses System zu umgehen oder absichtlich nicht ordnungsgemäß zu nutzen. Als Beispiel möge hier der Keil unter einer Hochsicherheitstür dienen, die aufgrund Ihrer schlechten Bedienbarkeit durch die Nutzer bedienungsfreundlich gemacht wurde.

Sprachbiometrische Systeme können nur Identitäten verifizieren, welche vorher registriert wurden. Sobald man wünscht, dass Personen ohne eine *claimed identitiy* authentifiziert werden sollen, muß die gesamte Datenbank durchsucht werden. Dieses 1:n-Suchproblem führt zu einer entsprechenden Erhöhung der Fehlerquoten wie auch des dafür notwendigen Zeitaufwandes. Je nach Gestaltung der Dialoge lässt sich die Authentifizierung innerhalb von 30 bis 60 Sekunden durchführen, wobei die Überprüfung der Stimme bei textabhängigen Sprachverifizierern dabei unter 10 Sekunden in Anspruch nimmt.

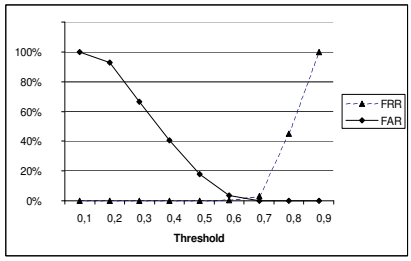
Bezüglich des flächendeckenden Einsatzes eines biometrischen Systems ist auch die Fehlerquote wichtig, die beschreibt, welcher Anteil an Personen nicht erfasst werden kann, die Failure to Enroll Rate (FER). Gleiche Bedeutung bezüglich der Sicherheit haben Systemintegrationsaspekte: Schutz der Templates durch Verschlüsselung, Schutz und Verschlüsselung der Rohdaten, Schutz vor Bedrohungen sowohl durch den Administrator bzw. Resourcenverantwortlichen als auch Schutz vor Gefahren, welche für alle Authentifikationssysteme gelten. Hierunter fällt auch der Schutz der Datenbank, damit Attribute nicht umbenannt oder Berechtigungen nicht verändert werden können.

Welches sind realistische Gefahren und wie kann man sich davor schützen? Am Beispiel des VOICE.TRUST Servers soll dies verdeutlicht werden. Das Unterschieben von Templates wird verhindert, indem eine Registrierung nur dann möglich ist, wenn ein als Superuser (zur Registrierung Dritter ermächtigter) Berechtigter positiv authentifiziert wird und sicherstellt, daß nur wirklich berechtigte und sicher identifizierte Personen als sie selbst registriert werden. Außerdem wird die Datenbank der Templates als auch die Kommunikation zwischen der verarbeitenden Software und der Datenbank durch Verschlüsselung geschützt. Je nach Schutzbedürftigkeit lassen sich Zeitstempel und ein Public Key Verfahren einsetzen. Das Täuschen des Systems durch Tonbandaufnahmen oder Ähnlichem (Replay Attack) wird durch einen Lebendtest verhindert. Dieser stellt sicher, daß der Benutzer zum Zeitpunkt der Authentifizierung lebend anwesend ist [Sc00], eine der wichtigsten Funktionen eines biometrischen Systems. In der Sprachauthentifizierung ist dies ohne einen Medienbruch möglich. Durch das Challenge/Response-Verfahren wird der Nutzer aufgefordert, willkürlich ausgewählte Phrasen zu wiederholen. Diese werden sowohl semantisch als auch biometrisch auf Richtigkeit überprüft. Die Sprachsynthese, also die künstlichen Spracherzeugung, ist beim heutigen Stand der Technik nicht in der Lage, einen Sprecher so zu imitieren, daß eine erfolgreiche Überwindung ermöglicht würde. Ein ernsthafter Angriff wäre die Registrierung einer künstlich erzeugten Stimme. Dies wird durch die Vertrauenskette des oben beschriebenen Superuser-Enrollments verhindert bzw. ist im Audit-fähigen und nicht löschbaren Admin-Log nachzuvollziehen. Jeder Angriff auf das System, auch durch Social Engineering, wird damit protokolliert.

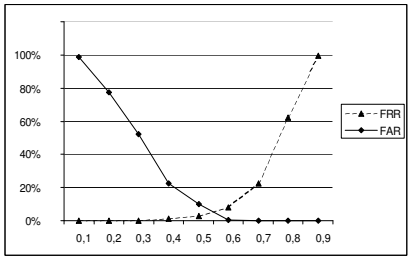
Die Sicherheit von biometrischen Systemen kann mittels der Common Criteria (CC, standardisiert als ISO/IEC 15408) evaluiert werden [CC00]. Die CC geben Herstellern und Anwendern eine Methodologie in die Hand, unter Benutzung objektiver Kriterien die Sicherheitseigenschaften von IT-Lösungen bewerten und vergleichen zu können. Speziell für die Bewertung biometrischer Systeme wurde unter Mitwirkung des BSI die Biometrics Evaluation Method [BEM02] erarbeitet. Für den bereits erwähnten VOICE.TRUST Server wurde entsprechend der in der BEM vorgeschlagenen Vorgehensweise bereits ein *Security Target* erstellt. Außerdem wurde in Zusammenarbeit mit dem TÜV-IT eine Vorstudie angefertigt, die insbesondere zum anzuwendenden Testverfahren Stellung bezieht. Die in dieser Studie nachgewiesenen Ergebnisse sind sehr vielversprechend. Details zu den erreichten FAR und FRR sind in der folgenden Abbildung 7 dargestellt.



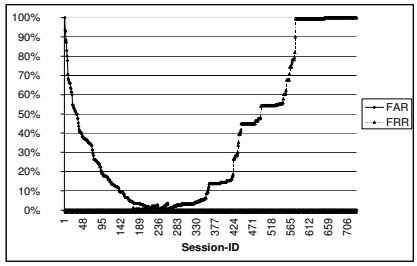
Fehlerraten auf dem Verifikationslevel1.



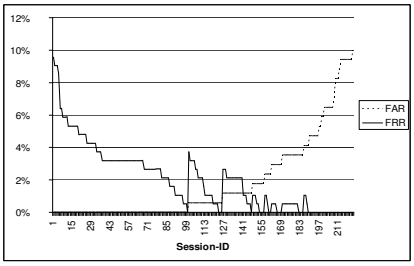
Fehlerraten auf dem Verifikationslevel 2.



Fehlerraten auf dem Verifikationslevel 3.



Nach Fehlerraten sortierte Sitzungsergebnisse.



Sitzungen mit Fehlerwerten nahe der Zone der *Equal Error Rate* (EER).

Abbildung 7: Fehlerquoten (FAR und FRR) des VOICE.TRUST Servers in einem dreistufigen Verifikationsverfahren entsprechend den Ergebnissen der TÜV-Studie [GT02].

Eine weitere wichtige Aufgabe ist die Sammlung von repräsentativem Datenmaterial, um in einem Feldtest Sicherheitseigenschaften mit hinlänglicher Aussagekraft bewerten zu können.

Eine Evaluierung wird voraussichtlich nach Evaluation Assurance Level (EAL) 2 für mittlere Funktionsstärke (SOF medium) erfolgen. EAL 2 bedeutet *strukturell getestet*.

EAL 2 erfordert die Kooperation des Entwicklers hinsichtlich der Lieferung von Entwurfsinformationen und Testergebnissen. Dabei sollte aber der dem Entwickler abgeforderte Arbeitsaufwand das in gut geführten Betrieben übliche Maß nicht überschreiten. Das heißt, sie soll keine erheblichen finanziellen oder zeitlichen Zusatzinvestitionen erfordern. EAL 2 ist daher in den Fällen anwendbar, in denen Entwickler oder Benutzer eine niedrige bis mittlere Stufe an unabhängig geprüfter Sicherheit benötigen und die vollständigen Entwicklungsaufzeichnungen nicht verfügbar sind. Eine solche Situation kann bei der Prüfung der Sicherheit von Altanwendungen entstehen oder dann, wenn der Entwickler nur eingeschränkt zur Verfügung steht. EAL 2 schafft Vertrauenswürdigkeit dadurch, dass die Sicherheitsfunktionen unter Verwendung einer funktionalen und Schnittstellenspezifikation sowie von Handbüchern und des Entwurfs des TOE (Evaluationsgegenstand) auf hoher Ebene analysiert werden, um das Sicherheitsverhalten zu verstehen. Die Analyse wird unterstützt durch unabhängiges Testen der TOE-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation, durch selektive, unabhängige Bestätigung der Entwicklertestergebnisse, durch Analyse der Stärke der Funktionen und durch einen Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen (zum Beispiel solchen, die allgemein bekannt sind). EAL 2 schafft Vertrauenswürdigkeit auch mittels eines Konfigurationsverzeichnisses für den TOE und durch einen Nachweis der Sicherheit der Auslieferungsprozeduren.

SOF-Mittel ist eine Stufe der TOE-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen angemessenen Schutz gegen naheliegendes oder absichtliches Brechen der TOE-Sicherheit durch Angreifer bieten, die über ein mittleres Angriffspotential verfügen.

7 Bewertung und Ausblick

Die Autoren gehen davon aus, dass in naher Zukunft die Biometrie die wichtigste und selbstverständlichste Art der Mensch-Computer-Interaktion werden wird. Biometrische Anwendungen werden in alle Bereiche skalierbar hineinwachsen, wir werden sie bei Application Service Providern (ASP), Großfirmen, Dienstleistern, aber auch bei Behörden vorfinden. Sie werden Einzug halten in Unternehmen jeder Größe, in Haushalte, Fahrzeuge, Maschinen und technische Geräte jeder Größe bis hin zu Handhelds.

Sprache könnte für den Schutz von mobilen Devices, Türzugängen, Telefonieapplikationen, Computern, Fahrzeugsteuerung oder Haustechnik eingesetzt werden. Fingerprints bieten sich für den Schutz von Türzugängen, Luftfahrteinrichtungen, Computern oder Waffen an. Die Unterschrift könnte Signaturen, Computer oder auch mobile Devices absichern. Iris-Scan und Retina-Scan werden wir in Zutrittskontrollen für Sicherheitsbereiche finden, Gesichtserkennung in Geldausgabegeräten und der Luftfahrt. Für Handgeometrie

geeignete Anwendungsfelder könnten Geldausgabegeräte, Luftfahrt und Zugangskontrollen sein.

Zusammenfassend läßt sich feststellen, daß Biometrie kein Ersatz zur PKI oder anderen *sicheren* Verfahren ist, sie ist eine Ergänzung dazu. Biometrie ist eine eigenständige Technologie, die in ihrer formalen Sicherheit zwischen Passworten und PKI liegt. Jedes Authentifikationsverfahren hat Stärken und Schwächen, es kommt darauf an, die Stärken unter Vermeidung der Schwächen miteinander zu kombinieren. Biometrie ist inzwischen praxisreif. Biometrie ist sicher, bedienungsfreundlich und bequem. Es gibt bereits ernsthafte in der Praxis eingesetzte biometrische Systeme und es werden in naher Zukunft schnell mehr werden. Biometrie ist die natürlichste Art und Weise, wie der Mensch mit dem Computer interagieren kann.

8 VOICE.TRUST AG

Die VOICE.TRUST AG (www.voicetrust.de) wurde 2000 gegründet und ist führender Anbieter sicherer Authentifizierungslösungen mittels biometrischer Stimmverifikation. VOICE.TRUST Lösungen führen zu einer Senkung der laufenden Kosten herkömmlicher Authentisierungslösungen von bis zu 80%. Anwendungsgebiete sind die sichere Authentisierung für PIN- und Passwort Reset, Single Sign-On, Logon, Remote Access oder Anruferauthentifizierung in den Bereichen Netzwerk-Sicherheit, Call-Center, Mobile Banking und E-Commerce.

Literatur

[BEM02] Common Criteria Biometric Evaluation Methodology Working Group Biometric Evaluation Methodology, Release 1.0, August 2002, p. 19–21, 23, table 12.

[CC00] Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, 2000. (www.bsi.bund.de)

[Co02] http://www.phon.ox.ac.uk/~jcoleman/phonation.htm

[DHP99] Deller, J. R., Hansen, J. H. L., and Proakis, J. G.: Discrete Time Processing of Speech Signals, pp. 100. IEEE Press Classic Reissue, Wiley Interscience, 1999.

[DS03] Auszug aus einem Beitrag zum Kriterienkatalog „Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren“ der TeleTrusT AG6 „Biometrische Identifikationsverfahren“,http://www.datenschutzzentrum.de/projekte/biometri/kap6krit.htm.

[Fu81] S. Furui. Comparison of speaker recognition methods using statistical features and dynamic features. IEEE Trans. Acoust., Speech, Signal Processing, 29(3):342-350, 1981.

[GT02] Grans, K., Tekampe, N.: Dokumentation der Testumgebung und Testergebnisse Voice.Trust Server, 2002

[Ha87] Hartung, J.: Statistik, Lehr- und Handbuch der angewandten Statistik;1987, Oldenbourg.

[Lu99] Luettin, J.: Speaker Verification Experiments on the XM2VTS Database, IDIA Research Report 99-02.

[Me03] Meffert,B. et al.:Biometrik, ein aktueller Forschungsgegenstand. HUMBOLDT-SPEKTRUM 1/2003.

[MW02] Mansfield, A. J. , Wayman, J. L.: Best Practice in Testing and Reporting, Performance of Biometric Devices; Biometric Working Group, Version 2.01, p. 19, 2002

[Ot03] Ott, H.-J.: Biometrische Verfahren der Zugangskontrolle, http://www.kecos.de/script/35biometrie.htm.

[Sc00] Schneier, B. Secrets and Lies: Digital Security in a Networked World. pp. 136-141. Wiley Computer Publishing.

[Va03] Vandor: Gesellschaft: Biometrie datenschutzgerecht gestalten. http://biometrie.inhos.de/article.php?sid=14.

[W303] W3C: Voice Extensible Markup Language (VoiceXML) Version 2.0 (www.w3.org)