Sprach-Biometrie im Hochschulumfeld

Andreas Wolf und Andreas Battenberg

VOICE.TRUST AG
Landshuter Allee 12-14
D-80637 München
{awolaba}@voicetrust.de

Zusammenfassung: Sprach-Biometrie ist inzwischen im Praxiseinsatz bewährt, robust und sicher. In diesem Papier werden einige Grundlagen kurz umrissen. Den Hauptteil füllt eine Diskussion potenzieller Einsatzmöglichkeiten im Hochschulbereich unter Betriebs-, Einsparungs- und Sicherheitsaspekten. Es werden Fragestellungen aufgezählt, die für Hersteller von Biometrie-Lösungen wichtig sind und gleichzeitig interessante Forschungsthemen ergeben.

1 Einleitung

Um die Einsatzmöglichkeiten biometrischer Systeme beurteilen zu können, ist es notwendig, diese als Authentifizierungssysteme zu identifizieren, mit denen die Identität von Personen festgestellt oder überprüft werden kann. In Abschnitt 2 werden darum Authentifizierungssysteme, Biometrie und im Besonderen Sprach-Biometrie einführend erläutert. Anschließend wird in Abschnitt 3 auf Themen zu IT-Sicherheit und Datenschutz eingegangen. Abschnitt 4 listet eine Vielzahl von möglichen Anwendungsfällen für sprachbiometrische Lösungen im Hochschulbereich auf. Daran schließt sich in Abschnitt 5 eine Diskussion über die in Einführungsprojekten für biometrische Systeme über das normale Projektmanagement hinaus zu berücksichtigenden „best practices“ an. In den Abschnitten 6 und 7 werden Themen adressiert, die die Beschäftigung mit Sprach-Biometrie aus Hochschulsicht auch für Forschungskooperationen interessant machen und es wird eine zusammenfassende Bewertung der Einsatzmöglichkeiten gegeben.

2 Sprach-Biometrie

2.1 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*). Authentifizierungsverfahren können in drei Klassen unterteilt werden. Sie fragen geheimes *Wissen* des Benutzers ab, wie etwa PIN- oder passwortbasierte Verfahren, überprüfen den *Besitz* von speziellen, schwer zu fälschenden Dingen, wie etwa Magnet- oder

Chipkarten, oder verwenden *persönliche Eigenschaften* des Benutzers für seine Identifizierung oder Verifikation. Letztere sind die biometrischen Verfahren. Biometrische Verfahren haben den Vorteil, dass sie nicht ohne weiteres gestohlen oder ausgespäht werden können. Häufig sind biometrische Systeme auch komfortabler zu bedienen. Viele biometrische Merkmale sind der Natur der Dinge nach bereits *öffentlich zugänglich*. Diese Eigenschaften biometrischer Merkmale führen zu einer Reduktion der mit Verlust oder Kompromittierung verbundenen Gefährdungspotenziale, bringen aber andererseits neue Risiken mit sich.

2.2 Biometrie

Biometrische Verfahren können in passive und aktive Verfahren unterteilt werden. Passive Verfahren sind solche, bei denen *offensichtliche* Merkmale des Benutzers ohne seine aktive Mitwirkung 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 Fingerabdruck-Scan. Unterschrifts-, Sprach- oder Ganganalyse sind dynamische Verfahren.

2.3 Sprecher-Erkennung und Sprach-Erkennung

Automatische 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.

Dass eine Sprecher-Erkennung 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. Jeder Teil des Vokaltraktes bringt charakteristische Resonanzfrequenzen in diesen Klang ein. Da diese Resonanzen dazu tendieren, das Frequenzspektrum der menschlichen Sprache zu formen, werden sie *Formanten* genannt, ein Begriff, der aus der Harmonielehre stammt. Das Überlagerung dieser vielen verschiedenen Frequenzen ist individuell verschieden. Mittels geeigneter mathematischer Verfahren können Individuen anhand ihres Klangspektrums unterschieden werden. Im einfachsten Fall, der *textabhängigen* Sprecherverifikation, werden dem Entscheidungsprozess immer gleiche Worte oder Sätze zugrunde gelegt. Ein Benutzer spricht bei der Registrierung diese festen Wörter mehrfach auf, der Computer berechnet daraus die Referenzdaten

und hinterlegt diese Informationen in einer Datenbank. Um sich zu authentifizieren, wird eine Person dann aufgefordert, eben diese festgelegten Ausdrücke zu sprechen. Die zweite Variante, die *textunabhängige* Sprecherverifikation, erlaubt es, das gesamte Vokabular zu nutzen. Hierzu muss der Sprecher aber das System mit vergleichsweise umfangreichem 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 bezieht sich nicht auf ein Wort, sondern auf die Sprache einer Person.

3 Sicherheitsaspekte und Datenschutz

Spricht man im Kontext von Authentifizierungslösungen über Sicherheit, so sind dabei neben der erreichbaren Funktionsstärke auch Datenschutz- und Akzeptanzthemen zu untersuchen. Kostengesichtspunkte müssen ebenfalls berücksichtigt werden. Ziel sollte es sein, für den Schutz von Ressourcen Lösungen zu finden, die bei sparsamem Mitteleinsatz ausreichend Absicherung gewähren und vor allem von den Benutzern akzeptiert werden.

3.1 IT-Sicherheit

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 Systems, die Fehlerquote der FR (FRR) den Komfortlevel des Systems. Die Bedeutung der FAR liegt auf der Hand. Ist die FRR eines Systems zu hoch, ist also sein Komfort-Level zu niedrig, dann ist die Motivation der Benutzer hoch, dieses System zu umgehen oder absichtlich nicht ordnungsgemäß zu nutzen. Für den Betreiber eines biometrischen Systems kommt es wie für den Betreiber einer jeden sicherheitsrelevanten Installation darauf an, ein für ihn optimales Gleichgewicht zwischen Komfort und Funktionsstärke zu finden.

Gleiche Bedeutung bezüglich der Sicherheit haben Systemintegrationsaspekte: Schutz der Templates durch Verschlüsselung, Schutz und Verschlüsselung der Rohdaten, Schutz vor Bedrohungen durch Administrationspersonal und vor Gefahren, welche für alle Authentifizierungssysteme gelten. Darunter fällt etwa der Schutz der Datenbank, damit Attribute nicht umbenannt oder Berechtigungen nicht verändert werden können. Ebenfalls betrachtet werden muss der Schutz der Verbindungen zu dem System, auf dem entsprechend der getroffenen Authentifizierungsentscheidung Aktionen ausgelöst werden sollen, wie beispielsweise bei der Zurücksetzung von Passworten.

Die Sicherheit von biometrischen Systemen kann mittels der Common Criteria [CC00] evaluiert werden. Die CC erlauben es, unter Benutzung objektiver und international anerkannter Kriterien die Sicherheitseigenschaften von IT-Lösungen bewerten und vergleichen zu können. Für den bereits erwähnten VOICE.TRUST Server wurde in Zusammenarbeit mit dem TÜViT Essen eine Vorstudie [GT02] für eine Zertifizierung angefertigt. Derzeit befindet sich der VOICE.TRUST Server im Zertifizierungsprozess nach EAL2 SOF

medium. 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).

3.2 Datenschutzaspekte

Biometrische Systeme können nur Personen verifizieren, die vorher registriert wurden, also Referenzdaten (Templates) hinterlegt haben. Damit ist es erforderlich, dass Referenzdatensätze gehalten werden. Diese Datensätze können zentral oder dezentral gehalten werden, wobei Datenschützer die dezentrale Speicherung bevorzugen, da sie ein geringeres immanentes Missbrauchsrisiko hat. Bei Sprach-Biometrie per Telefon ist eine dezentrale Speicherung der Templates allerdings nicht möglich, da dadurch die Einfachheit der Anwendung verloren gehen würde: Sprach-Biometrie kommt ohne jegliche zusätzliche technische Vorrichtungen aus, es muss einzig und allein ein ganz normales Telefon verfügbar sein.

Sprach-Biometrie hat gegenüber fast allen anderen Biometrien den Vorteil, dass der Benutzer gefragt werden kann, wer er ist. Diese Feststellung einer *claimed identity* ohne Medienbruch ermöglicht es, das Problem der Identifikation (der *Feststellung* der Identität eines Benutzers) zu umgehen und nur eine Verifikation (die *Überprüfung* der Identität) durchführen zu müssen. Neben dem Vorteil der Komplexitätsreduktion (es ist nur noch ein 1:1-Match anstelle eines 1:n-Vergleiches erforderlich) können Verfahren verwendet werden, die die Möglichkeit einer Verwendung für Identifikationszwecke weitgehend ausschließen, was unter Datenschutzaspekten vorteilhaft erscheint. Es ist möglich, text-abhängige Verfahren zu verwenden, mittels derer nur anhand vorher festzulegender Phrasen die Identität eines Benutzers überprüft werden kann. Diese Phrasen sollten für nahezu jeden Benutzer verschieden sein. Es sollten solche Phrasen verwendet werden, die im Alltag üblicherweise nicht verwendet werden, da auf diese Weise die Erfolgswahrscheinlichkeit von Replay-Attacken verringert werden kann.

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. Eine aktive Mitwirkung des Nutzers macht das Verfahren zudem transparenter, baut Ängste ab und befördert die Akzeptanz [DS03].

3.3 Mögliche Schäden

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. Alternativ können PIN-basierte Verfahren zum Einsatz kommen. Das Täuschen des Systems durch Tonbandaufnahmen oder andere Replay-Attacken wird durch einen Lebendtest, das sogenannte Challenge&Response-Verfahren, verhindert. In

der Sprachauthentifizierung ist dies ohne einen Medienbruch möglich, indem der Nutzer aufgefordert wird, willkürlich ausgewählte Phrasen zu wiederholen. 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.

Grundsätzlich ist natürlich jede Sicherheitstechnik überwindbar. Auf diversen Karten wird die PIN notiert, Passworte werden vorzugsweise mit Klebezetteln am Monitor notiert oder im Schreibtischfach deponiert. Die reale Funktionsstärke derartiger Mechanismen ist damit wohl deutlich reduziert. Für viele Anwendungen wird selbst eine Kalibrierung des Sprach-Biometrie-Systems, die eine FAR von 1-2% hat, eine deutlich höhere reale Sicherheit hervorbringen, als sie heute vorhanden ist. Wie in jedem Fall ist es unerlässlich, in einer Risikoanalyse mögliche Schäden und ihre Wahrscheinlichkeit zu analysieren, um sie durch die Anwendung adäquater Mittel auf ein vertretbares Maß zu reduzieren.

3.4 Vorteile der Arbeit mit kooperativen Benutzern

Ein Einsatz von sprachbiometrischen Systemen zum Zweck der Automatisierung von Dienstleistungen wird von Personen benutzt, die kooperativ mitwirken. Schließlich wollen sie, dass ein bestimmter Vorgang durchgeführt wird. Kooperative Benutzer werden eher bereit sein, bestimmte „Widrigkeiten“ des Systems zu „erdulden“. Schließlich würde eine konventionelle, nicht automatische Erledigung ihres Anliegens länger dauern und umständlicher oder an das Vorliegen bestimmter Bedingungen geknüpft sein.

Für alle Dienstleistungen, die inhaltlich sinnvoll über das Telefon angefordert werden und automatisiert durchgeführt werden könnten, bietet sich der Einsatz sprachbasierter Authentifizierung an. Überall dort, wo solche Dienste sinnvoll in Arbeitsabläufe eingefügt werden können, man aber bisher aufgrund der fehlenden Möglichkeit der Überprüfung der Identität des Gesprächspartners davon Abstand nehmen musste, lassen sich jetzt automatisieren. Da diese Automatisierung für den Benutzer bequem ist, wird er sie auch benutzen.

Manchen biometrischen Methoden haftet im gesellschaftlichen Ansehen ein gewisser Makel an. Das Abgeben von Fingerabdrücken hat ein Image aus dem Bereich der Kriminalistik, und an oder in seine Augen lässt man wohl doch nur den Augenarzt. Sprache hat diesen Makel nicht. Überall dort, wo man sowieso per Sprache Aktionen auslösen möchte, wird man bereit sein, ein paar Sekunden mehr zu sprechen, um in den Genuss authentifizierungspflichtiger Leistungen zu kommen. Auch in vielen anderen Situationen, die auf den ersten Blick keinen Bezug zum Telefon haben, wie etwa bei der Türöffnung via Voice, wird ein Benutzer gern zum Telefon (als Türöffner) greifen, wenn ihm das offensichtliche Vorteile bringt. Aus der Erkenntnis der Vorteile des Einsatzes einer biometrischen Lösung heraus werden die Benutzer auch eher bereit sein, ihren Teil zum Funktionieren des Systems beizutragen und zum Beispiel ein hochwertiges Enrollment beizubringen.

4 Einsatzszenarien im Hochschulbereich

4.1 Einschreibung/Rückmeldung

Der ideale Zeitpunkt zur Erfassung eines Stimm-Templates ist die Immatrikulation. Die Zahl der Erstsemester beträgt ca. 10% der Gesamtzahl an Studenten (z.B. Heinrich Heine Universität Düsseldorf Wintersemester 2003/2004: 2456/25133). Ist der Studierende einmal angemeldet, können verschiedenste Prozesse über eine Stimm-Authentifizierung abgesichert werden.

Der Vorgang der Erstanmeldung (Enrollment) kann in einem Vier-Augen-Prozess (sicherste Variante) im Studentensekretariat selbst durchgeführt werden oder beispielsweise durch Zusenden einer Einmal-PIN zusammen mit dem Studentenausweis. Die Einmal-PIN weist den Anrufer bei der Erstanmeldung als Berechtigten aus. Weitere Variationen sind nach administrativen Notwendigkeiten oder entlang bereits etablierter Prozesse realisierbar.

Mit der Rückmeldung erklärt der Studierende, dass er das Studium im folgenden Semester fortsetzen will. In vielen Fällen ist persönliches Erscheinen notwendig und entsprechend lange Schlangen im Studentensekretariat vorprogrammiert. Die Zahlung des Studentenwerksbeitrags oder etwaiger Semestergebühren erfolgt im Voraus. Der Zahlungseingang kann in einigen Hochschulen automatisiert dem Studenten zugeordnet werden, in anderen wird die Zuordnung manuell erledigt.

Eine telefonische Rückmeldung über ein Sprachportal bedeutete eine enorme Entlastung für das Studentensekretariat. Eine Stimm-Authentifizierung müsste in diesem Zusammenhang die Identität des Rückmeldenden verifizieren. Über Spracherkennung könnten auch komplexere Vorgänge wie Fächerwechsel bewältigt werden. Gleichzeitig könnte auch eine automatische Abbuchung des Semesterbeitrags vom Konto ausgelöst werden, wenn der Studierende die entsprechende Erlaubnis erteilt hat.

4.2 Prüfungsanmeldung

An einigen Hochschulen ist es bereits möglich, sich über das Internet zu Prüfungen oder Klausuren anzumelden oder sich von Prüfungen abzumelden (z.B. bei Krankheit). Hierbei hat es aber auch schon Rechtsstreitigkeiten über nicht erfolgreiche An- oder Abmeldungen gegeben, da die Identität der meldenden Person nicht in allen Fällen bewiesen werden kann.

Eine Anmeldung per Telefon mit eingeschlossener Authentifizierung stellt sicher, dass nur ein berechtigter Studierender eine An- oder Abmeldung durchführen kann und dass auf Seiten der Universität eine unbestreitbare Willenserklärung vorliegt. In gleicher Weise kann auch ein bestehendes Web-basiertes System mit einer Stimm-Authentifizierung nachgerüstet werden.

4.3 Passwort Reset

Als Zugangskontrolle für Rechner und andere Systeme wird weltweit die Kombination User-ID und Passwort eingesetzt. Zwar liefert praktisch jedes Betriebssystem diese Zu-

gangskontrolle mit, jedoch werden Passwörter häufig weitergegeben oder auch vergessen. Daher verursacht diese Art der Zugangskontrolle einige Sicherheitsprobleme und erhebliche Folgekosten. Auf 1000 Benutzer eines Systems vergessen ca. 5-15 pro Tag ihr Passwort. Aus Passwort-Problemen resultieren so ca. 30-40% aller Anfragen am internen HelpDesk.

Ist ein einfaches Verfahren zur Erlangung eines neuen Passworts implementiert, so kann jeder, der dieses Verfahren kennt, ohne große Probleme zu einem neuen Passwort kommen und damit unerkannt Schaden anrichten, unbefugt Systeme nutzen oder sogar Daten ausspionieren. Einfache Web-basierte Passwort Reset Systeme arbeiten mit Frage/Antwort-Prozessen. Dem liegt die Annahme zugrunde, die Antwort wäre nur dem berechtigten Benutzer bekannt. Aber die Antwort auf Fragen wie den Namen des Dackels kennen in aller Regel mehrere Personen.

Aus diesen Gründen haben die meisten Hochschulen mit zentraler Nutzerverwaltung für Passwort Reset ein System implementiert, das zwar ein gewisses Maß an Sicherheit bietet, aber umständlich ist. Typisch ist hier ein Vier-Augen-Prinzip, bei dem wissenschaftliche Hilfskräfte eine Identitätsprüfung vornehmen (persönliches Erscheinen plus Studentenausweis). Außerhalb der üblichen Sprechzeiten oder für Remote Access Lösungen ist ein solches Verfahren jedoch nicht einsetzbar.

Die Stimm-Authentifizierung per Telefon verbindet hier Sicherheit und Effizienz mit einem hohen Maß an Benutzerfreundlichkeit. Mit der Authentifizierung über Stimm-Verifikation steht ein sicheres Verfahren zur Verfügung. Die automatische Abwicklung der Anfragen spart Ressourcen in Administration und HelpDesk und macht den Service rund um die Uhr verfügbar. Die Dialog-basierte Benutzerführung macht die Benutzung sehr einfach.

4.4 Zugangskontrolle

In der Regel stellt die Hochschule IT-Infrastruktur und viele andere Services zur Verfügung. Vielfach gibt es Probleme, die Nutzung solcher Ressourcen durch Unberechtigte zu verhindern. Unberechtigte können dabei auch Studierende anderer Fakultäten sein oder Benutzergruppen mit begrenzten Privilegien.

So stellt die Bayerische Akademie für Werbung und Marketing (BAW) ihren ca. 500 Studenten kostenfrei öffentlich zugängliche Computer zur Verfügung. Die Erfahrung hat gezeigt, dass hier Passwort-Sicherheit nicht ausreicht, da Passwörter weitergegeben werden und Manipulationen nicht einem bestimmten Benutzer zugerechnet werden können.

Eine Stimm-Authentifizierung für das Log-on schafft hier eine Zugangsberechtigung, die nicht an andere Personen weitergegeben werden kann. Gleichzeitig bietet sie einen gewissen Schutz vor Manipulationen, da den Studenten bekannt ist, dass im Log-file gespeichert ist, wer wann auf die Computer zugegriffen hat.

In ähnlicher Weise lässt sich der Zugriff auf besonders kostspielige Geräte oder auf besonders rechenintensive Anwendungen begrenzen.

4.5 Autorisierung für Telefon- und Web-Services

Bei vielen gegen Ende des Semesters geschriebenen Klausuren ist es für den Studierenden wichtig, die Ergebnisse unter Umständen auch vom Heimatort aus in Erfahrung bringen zu können. Der öffentliche Aushang von Prüfungsergebnissen (und die Weitergabe der Information durch Kommilitonen) stößt an datenschutzrechtliche Grenzen. Die telefonische Mitteilung ist streng genommen ebenfalls unzulässig, jedenfalls ohne ausreichende Legitimation des Anrufers.

Hier eröffnet die Stimm-Authentifizierung einen einfachen Weg, die Abfrage der Informationen zu automatisieren. Werden die Daten auf einem Web- oder Vocie-Portal bereitgestellt, kann durch die Stimm-Authentifizierung sichergestellt werden, dass der Anrufer nur auf seine eigenen Daten zugreifen kann.

In ähnlicher Weise könnten auch Unterlagen beispielsweise zur Prüfungsvorbereitung zum Abruf über Internet bereitgestellt werden. Auch hier stellt die eindeutige Bindung der biometrischen Authentifizierung an die Person sicher, dass nur eine berechtigte Person Zugriff auf diese Unterlagen bekommt. Insbesondere für Fernstudiengänge kann auf diese Weise ein guter Schutz des geistige Eigentums erreicht werden.

In den meisten Hochschulbibliotheken ist ein Ausweissystem etabliert. Oft wird der Bibliotheksausweis auch dazu benutzt, die Daten für Vorbestellungen und Verlängerungen zu speichern und ans System zu übertragen. Mit Hilfe einer Stimm-Authentifizierung lässt sich hier auch ein Fernzugriff realisieren, der nur für berechtigte Benutzer zur Verfügung steht und auch ohne Webzugang funktioniert.

Ein weiterer Service wäre die Bereitstellung eines gesicherten Speicherbereichs, beispielsweise für Arbeitsgruppen, die hier gemeinsam zu bearbeitende Dokumente sicher nur für eine definierte Benutzergruppe zugänglich machen wollen. Insbesondere im medizinischen Bereich müssen hier aus Gründen des Patientendatenschutzes deutlich höhere Anforderungen erfüllt werden als sonst allgemein üblich.

4.6 Management von Serviceangeboten

An vielen Hochschulen gibt es kostenpflichtige Services. Diese reichen von Kopierservices bis hin zum subventionierten Mensa-Essen. Vor allem bei für Studierende vergünstigt angebotenen Leistungen stellt sich das Problem der Nutzungsbeschränkung.

Wo Mensamarken verkauft werden, da gibt es auch einen regen Graumarkt, über den nicht berechtigte Personen in den Besitz von Mensamarken kommen. Es gibt bereits Pilotprojekte, bei denen eine Authentifizierung per Fingerabdruck den Zugang zur Mensaschlange regelt. In anderen Fällen wird eine Smartcard ausgegeben, die dann von Zeit zu Zeit wieder aufgeladen werden muss.

Über den Wiederaufladungsvorgang lässt sich eine einfache Berechtigungskontrolle etablieren, indem die Aufladung per Telefon und Stimm-Authentifizierung freigegeben werden muss. Gleichzeitig lässt sich hier auch die Freigabe einer Abbuchung vom Konto mit einbauen. Den gleichen Vorgang kann man natürlich für alle Karten dieser Art einführen.

Geht eine solche Karte verloren, muss sie gesperrt werden können, um eine unbefugte Nutzung zu unterbinden. Findet der Verlierer seine Karte wieder, ist meist der Sperrvorgang nicht mehr rückgängig zu machen – für Serviceanbieter und -Nutzer ein aufwändiges Problem.

Die Stimm-Authentifizierung bietet hierzu eine einfache und sichere Lösung. Über einen einfachen Anruf lässt sich die Karte bei Verlust sperren. Temporär, wenn der Besitzer die Karte nur verlegt hat, permanent, wenn die Karte geklaut wurde. Die temporäre Sperrung kann der Besitzer durch einen weiteren Anruf wieder aufheben, wenn er die Karte wieder gefunden hat.

4.7 Zutrittskontrolle

In vielen Hochschulen gibt es für Diplomanden und Doktoranden eigene Schlüssel zum Betreten bestimmter Räumlichkeiten, die sie dann auch außerhalb der normalen Öffnungszeiten nutzen können. Geht ein solcher Schlüssel verloren, sind unter Umständen hohe Kosten für den Austausch von Schlüsseln und Schlössern zu veranschlagen. Da Schlüssel unter Umständen auch weitergegeben werden können, ist nicht immer gewährleistet, dass nur berechtigte Personen Zugang haben.

Natürlich ist der Verwaltung daran gelegen, die Zahl der im Umlauf befindlichen Schlüssel so gering wie möglich zu halten. In vielen Fakultäten werden eigens studentische Hilfskräfte oder Hausmeister für Spät-Öffnungsdienste eingesetzt. Hierdurch entstehen zusätzliche Kosten.

Durch eine Stimm-Authentifizierung kann der Zugang zum Gebäude (oder Gebäudeteilen) jederzeit auch außerhalb der Öffnungszeiten auf einfachste Weise realisiert werden. Dazu wird neben der Tür, durch einem einfachen Kasten geschützt, ein Telefonhörer montiert, der direkt mit dem Authentifizierungsserver verbunden ist. Der Server gibt bei erfolgreicher Authentifizierung den Öffnungsbefehl an die Schließanlage.

Einmal am Authentifizierungsserver angemeldet, kann jeder Berechtigte sich entsprechende Türen öffnen. Als User-ID dient seine Matrikel- oder Personalnummer. Aus dem Logfile geht damit dann auch eindeutig hervor, wer wann ein bestimmtes Gebäude betreten hat.

5 Einführungsprojekte

Wie alle biometrischen Systeme arbeitet auch die Stimmerkennung um so besser, je sorgfältiger die Registrierung (Enrollment) 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 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.

Insgesamt lässt sich feststellen, dass die Authentifizierung per Telefon gegenüber jedem anderen biometrischen oder auch auf Besitz basierenden Mechanismus den unschätzbaren Vorteil hat, dass keinerlei Hardware-Rollout stattfinden muss. Die benötigten Telefone befinden sich bereits auf den Schreibtischen bzw. in den Taschen der Benutzer. In den Fällen, in denen die nach einer erfolgreichen Authentifizierung durchzuführenden Prozesse bereits heute in der IT-Welt automatisiert durchgeführt werden, besteht der einzige nennenswerte Aufwand in der Erfassung der Templates.

5.1 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 und entsprechende Richtlinien für den Einsatz festzulegen. Versäumnisse in dieser Phase sind später nur mit erheblichem Aufwand oder gar nicht zu korrigieren.

Für sprach-biometrische Anwendungen müssen zu einer Vielzahl von Themenkreisen die Anforderungen festgelegt werden. In der folgenden Aufstellung sind Fragen zu allgemeiner IT-Safety und IT-Security, wie Statistiken, Datensicherung, Log-Auswertung, Intrusion-Detection, e-Mail-Einbindung etc. nicht berücksichtigt.

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 Hochschulkultur ein?

Skalierung: Welchen Durchsatz soll das System bieten? Wie viele Anrufer sollen gleichzeitig mit dem System sprechen können?

Vertrauenskette: Um die Vertrauenskette zu den registrierten Templates verfolgen zu können, muss jederzeit nachvollziehbar sein, wie die Registrierung der Benutzer erfolgt ist.

Benutzermanagement und Rechtevergabe: Sollen die Templates und Berechtigungen der User mittels einem oder mehreren GUI verwaltet werden können? Erfolgt das Benutzermanagement über eine bereits vorhandene Datenhaltung, etwa eines Verzeichnisdienstes? Welcher Benutzer soll welche Rechte erhalten? Wo, wie und von wem sollen diese Rechte verwaltet werden?

Benutzerdatenimport: Für große Anwendungen, wie man sie an Hochschulen mit Tausenden Mitarbeitern und Zehntausenden Studenten, die noch dazu nur begrenzte Zeit verbleiben, erwarten darf, ist ein automatisierbarer Benutzerdatenimport unabdingbar. Es muss geklärt werden, wie mit fehlerhaften Daten umgegangen wird, die in der Regel zu erheblichen Anlaufschwierigkeiten eines Biometrie-Projektes führen würden.

5.2 Motivation der Teilnehmer

Die rechtzeitige Kommunikation mit den betroffenen Anwendern und Verantwortlichen in den Fakultäten, in der Verwaltung und auch im Personalrat sind ein wesentlicher Erfolgsfaktor. Insbesondere sind hier auch die rechtlichen Aspekte des Datenschutzes zu beachten.

Im Fall der Authentifizierung via Telefon ist das Enrollment 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, ist die technische Erfassung der Sprachdaten denkbar einfach. Damit ist die Datenerfassung für den Benutzer nicht mit unzumutbaren Belästigungen verbunden. Es ist aber trotzdem notwendig, jeden Benutzer immer wieder darüber aufzuklären, dass die Qualität der durch ihn abgelieferten Enrollmentdaten auch für den von ihm in der Anwendung selbst empfundenen Komfort entscheidend ist. Auch Selbstverständlichkeiten wie das richtige Halten des Telefonhörers bedürfen erfahrungsgemäß einer Auffrischung.

Die Erfahrung zeigt, dass gerade die Berichte zufriedener Benutzer es sind, die Biometrieprojekte schließlich zum Selbstläufer machen. Je schneller es genügend Erfolgsberichte gibt, um so schneller drängen die Benutzer von selbst in das System. Zusätzliche Vorteile, die den Erstnutzern gewährt werden, beschleunigen diesen Initialprozess.

5.3 Enrollmentverfahren

Grundsätzlich bieten sich zwei Verfahren an, mit denen die Templates der Benutzer erfasst werden können: die persönliche Vertrauenskette und ein wissensbasiertes Verfahren. Es ist auch möglich, beide Verfahren kombiniert einzusetzen oder im Verlaufe eines Projektes die Verfahren zu wechseln.

Verfahren mit persönlicher Vertrauenskette heißen *Superuser-Enrollment*. Hierbei wird das Enrollment eines neuen Benutzers in Gegenwart eines berechtigten bereits angemeldeten Benutzers durchgeführt. Auf diese Weise kann man etwa über Beauftragte an den Lehrstühlen und Instituten, aber auch durch die Personalstelle bzw. die Studierendenverwaltung die Erfassung vornehmen. Die Berechtigung der Beauftragten kann sehr flexibel und auch befristet vorgenommen werden.

Ein wissensbasiertes Verfahren ist zunächst das *PIN-Enrollment*, bei dem dem zu erfassenden Benutzer vorab eine PIN übermittelt wird, die er zum Nachweis der Berechtigung beim Enrollment eingeben muss. Bei späteren Verifikationsereignissen wird diese PIN nicht mehr benötigt. Varianten des Verfahrens benutzen vorhandene „Geheimnisse“, die nur dem zu erfassenden Benutzer bekannt sind. Das könnte etwa das Passwort eines vorhandenen Accounts an der Hochschule sein. Eine weitere Variante ist die Initiierung der Erfassung durch eine Web-Applikation, der gegenüber sich der Benutzer auf herkömmliche Weise authentifizieren muss und die Telefonnummer eingibt, unter der er zum Enrollment angerufen werden möchte.

Von entscheidender Bedeutung für die zu erreichende Qualität eines in Betrieb befindlichen biometrischen Systems ist die Qualität der Enrollmentdaten. Es liegt auf der Hand,

das eine spätere Erkennung um so besser sein kann, je hochwertiger die dem System vorliegenden Vergleichsdaten sind. Bei der Sprach-Biometrie ist darauf zu achten, dass der Benutzer den Telefonhörer richtig hält, den Lautsprecher am Ohr, das Mikrofon vor dem Mund. Das hört sich trivial an, ist es aber erfahrungsgemäß nicht. Es hat sich gezeigt, dass eine vorherige Sensibilisierung und Aufklärung der Benutzer über die Wirkungsweise des biometrischen Systems und über ein zweckmäßiges Verhalten die Qualität der Enrollments signifikant verbessern. Die Umgebung des Benutzers beim Enrollment sollte möglichst ähnlich zu der Umgebung sein, in der die späteren Verifikationsanrufe durchgeführt werden sollen. Es bietet sich an, insbesondere dasselbe Telefon zu verwenden, auch wenn das nicht Bedingung ist. Mittel zur Qualitätssicherung sind neben der Sensibilisierung der Benutzer die Aufsicht bei der Datenerfassung wie beim Superuser-Enrollment, die Forderung nach der Durchführung eines Verifikationsanrufes in unmittelbarer Folge des Enrollments, oder auch die Gewährung von Vergünstigungen für Benutzer des biometrischen Systems wie Boni oder Rabatte.

6 Forschungsthemen

Die Beschäftigung mit biometrischen Verfahren, in unserem Fall mit Sprachbiometrie, kann auch aus wissenschaftlichen Gesichtspunkten für Hochschulen von Interesse sein. Viele Themen bedürfen weiterer Forschungsanstrengungen, um die Qualität des verwendeten biometrischen Verfahrens auch zukünftig zu entwickeln und für noch breitere Einsatzfelder einsetzbar zu machen. Im Folgenden seien einige dieser Themen stichpunktartig skizziert. Die Erfahrung hat bereits gezeigt, dass derartige Fragestellungen erfolgreich in einer Kooperation zwischen Hochschulen und kleineren IT-Firmen bearbeitet werden können [VW04].

- **Statistische Verfahren**. Biometrische Verfahren sind stochastische Verfahren. Man kann damit die Funktionsstärke nicht wie bei einer Smartcard 2 “ausrechnen“. Große Datenbanken mit Templates oder Rohdaten sind kaum verfügbar. Feldversuche mit Millionen Benutzern kann man kaum durchführen. Wie kommt man nun zu verlässlichen Aussagen über Leistungseigenschaften von biometrischen Systemen? Welche statistischen Schätzverfahren sind anwendbar? Wie groß muss eine Stichprobe sein, wenn man Aussagen etwa zu einer FAR (false acceptance rate) von 10^{-4} machen möchte? Ein Ausgangspunkt zur Annäherung an diese Frage ist z.B. die BEM [BEM].
- **Spracherkennung**. Automated Speech Recognition (ASR) ist eine Kerntechnologie für Sprachportale. Die von derartigen Spracherkennern zu detektierenden Sprachäußerungen werden in der Regel mit Grammatiken beschrieben. Welche gibt es, welche sind international durchgesetzt, wie sieht der Markt von ASR-Anbietern aus? Es ist bekannt, dass auch freie Software verfügbar ist. Ist sie leistungsfähig und stabil genug, um für kommerzielle Zwecke eingesetzt werden zu können? Ein Projekt in diesem Bereich könnte bis hin zur Entwicklung eines Prototypen oder darüber hinaus gehen.
- **IVR-Marktübersicht**. Der Markt für IVR-Systeme (Interactive Voice Response) ist in großer Bewegung. Sprachportale lösen die vorhandenen DTMF-Portale ab. Damit verbunden ist ein Standardisierungsprozess für Sprachportale. Die relevanten Standards sind VoiceXML und SALT. Wie kompatibel sind am Markt erhältliche Systeme

tatsächlich mit diesen Standards? Für welche Bereiche fehlt noch eine Standardisierung? Auch hier sind prototypische Implementierungen, etwa mit freien IVR-Plattformen, ein sinnvoller Projektteil.

- **Feldversuche.** Biometrische Systeme müssen durch Feldversuche evaluiert werden. Diese Versuche müssen bestimmten Ansprüchen genügen (siehe Thema 1). Erste Erfahrungen dazu liegen bereits vor. Ein zukunftssicheres, universelles und auch für verteilte Versuche mit mehreren beteiligten Partnern brauchbares System bedarf aber erst noch der Spezifikation, Implementierung und Abschätzung der erforderlichen Ressourcen. In einem Projekt sollte ein solcher Feldversuch praktisch durchgeführt werden.

- **X-Channel-Effekt.** Biometrische Templates werden durch die Scanner, die zu ihrer Erfassung benutzt werden, verändert. Auch die Übertragungskanäle können Einfluss haben. Welchen Einfluss haben Telefone und Telfonkanäle auf die Verwendbarkeit von Sprachmaterial für Verifikationszwecke? Wie kann man den Einfluss quantitativ erfassen? Welche Verfahren sind bekannt, diesen Effekt zu mindern oder aufzuheben? Wie gut funktionieren diese Verfahren?

- **Template-Aging**. Biometrische Templates ändern sich im Laufe der Zeit. Oder besser: Ihre Träger altern. Welchen Einfluss hat diese sogenannte Template-Alterung auf die Langzeit-Eigenschaften biometrischer Verfahren? Welche Erfahrungen gibt es dazu in der Literatur? Wie kann man diesen Einfluss messen? Erste Ergebnisse zu diesem Thema liegen bereits vor [Wo04].

- **Konnektoren**. Sprachbiometrische System können u.a. für das Zurücksetzen von vergessenen Passworten verwendet werden. Dafür werden Softwarekomponenten verwendet, die in der Gesellschaft der Autoren Konnektoren genannt werden. Für viele Zielplattformen gibt es Standard-Schnittstellen, die es ermöglichen, unter Verwendung vorhandener Sicherheitsmechanismen administrative Aufgaben zu erledigen. Ein zu entwickelnder Konnektor, der gerade im Hochschulbereich Anwendung finden dürfte, ist ein Konnektor für diverse UNIXe. Dieser Konnektor sollte re-entrant sein und den Passwort-Reset unter anderem für Solaris, HP-UX, AIX und Linux ermöglichen, nativ und/oder unter Benutzung von NIS(+)-Mitteln.

- **Voice over Internet Protocol.** (VoIP) verbreitet sich immer weiter. Welche Protokolle werden international dafür verwendet? Wie funktionieren die mit Verlust behafteten Komprimierungsverfahren? Wovon sind die Verluste abhängig? In diese Untersuchungen sollen auch die Reduktionsverfahren von GSM und DECT mit einbezogen werden. Welchen Einfluss haben verlustbehaftete Verfahren auf die Erkennungsleistung von Sprecher-Erkennern und Sprach-Erkennern?

- **Automatische Tests**. Sprachbasierte Dialogsysteme können auf die unterschiedlichste Art und Weise getestet werden. Die einschlägigen am Markt verfügbaren Testwerkzeuge müssen auf Funktionsweise und Eignung getestet werden. Auch freie Sprach-Plattformen können Ausgangspunkt eines in einem Projekt entwickelten Werkzeuges zum Funktionstest sein. Insbesondere die Automatisierung von Lasttests ist ein wichtiges Vorhaben.

7 Bewertung und Zukunftsperspektiven

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 hineinwachsen. Aus diesem Grunde ist es erforderlich, dass an den Hochschulen entsprechende Kompetenzen in der Ausbildung vermittelt werden. Der Umgang mit realen Applikationen dürfte dabei hilfreich sein.

Biometrie ist kein Ersatz zur PKI (public key infrastructure) oder anderen „sicheren“ Verfahren, sie ist eine Ergänzung dazu. Ihre Stärken sollten ausgenutzt werden, vor allem dort, wo Dienstleistungen besser erbracht und darüber hinaus auch noch Kosten eingespart werden können. 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.

Biometrische Anwendungen werden aufgrund ihrer einfachen Bedienbarkeit in alle Bereiche hineinwachsen; wir werden sie bei Application Service Providern (ASP), Unternehmen, Dienstleistern, aber auch bei Hochschulen und Behörden vorfinden. Sie werden Einzug halten in Haushalte, Fahrzeuge, Maschinen und technische Geräte jeder Größe.

In naher Zukunft wird die Sprache die wichtigste und selbstverständlichste Art der Mensch-Computer-Interaktion werden. In diesem Zusammenhang wird der Sprach-Authentifizierung eine wichtige Schlüsselrolle zukommen. Sprachbiometrie wird aufgrund ihrer Vielseitigkeit und Benutzerfreundlichkeit einen sehr weit verbreiteten Einsatz finden.

Die schon heute absehbare technologische Entwicklung wird dazu führen, dass der Sprachdialog die Tastatur als Eingabemedium fast vollständig ersetzt. Börsenkurse abfragen von unterwegs? Aktien verkaufen oder Geld überweisen? Ein Anruf beim Sprachportal der Bank, Authentifizierung während des Dialogs und die Sache ist erledigt. Auch vor den Hochschulen wird diese Entwicklung nicht halt machen. Gerade im Gegenteil: Hier besteht die Möglichkeit, wertvolle Forschungs- und Entwicklungsarbeit zu leisten und den Einsatz der Technologie entscheidend mit zu gestalten.

Vor allem die ideale Kombination von Sicherheit, Kosteneffizienz und Benutzerfreundlichkeit macht die Sprecher-Authentifizierung zum idealen Werkzeug und wird ihren Teil dazu beitragen, dass Computertechnologie sich nahtlos in unseren Alltag integriert und sich unseren Wünschen anpasst statt umgekehrt.

8 VOICE.TRUST

VOICE.TRUST ist ein weltweit führender Lieferant von sicheren Stimm-Authentifizierungslösungen und mit über 100.000 verkauften Lizenzen europäischer Marktführer. VOICE.TRUSTs Lösungen haben in führenden Unternehmen Europas eine drastische Senkung der Authentifizierungskosten um bis zu 80% bewirkt. Höchste Datensicherheit und einfachste Benutzung führen zu sehr guter Akzeptanz. VOICE.TRUST liefert die sichere Lösung für PIN- und Passwort Reset Self-Service, Remote Access, Single Sign-On,

PKI-Support, Anrufer-Identifizierung oder Zwei-Faktor Authentifizierung in den Märkten Netzwerk-Sicherheit, Voice-Portale, Callcenter und HelpDesk. VOICE.TRUST wurde 2000 in Deutschland gegründet und verfügt inzwischen über ein weltweites Partnernetzwerk.

9 Literaturverzeichnis

Literatur

[BEM] Working Group Biometric Evaluation Methodology: Common Criteria Biometric Evaluation Methodology, Release 1.0, August 2002.

[VW04] Vatterrott, H.; Wolf, A.: Gestaltung graphischer Administrationsoberflächen für sprachbiometrische Authentifizierungssysteme, submitted for GI-2004.

[Wo04] Wolf, A.: Template Aging in Speech Biometrics, Workshop "Biometrics: Challenges arising from Theory to Practice" of ICPR2004, IEEE, 2004.

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

[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.

[GT02] Grans, K.; Tekampe, N.: Dokumentation der Testumgebung und Testergebnisse VOICE.TRUST Server, 2002