abc information
IT Solution Company

Billing & Accounting Verifikation/Identifikation

abc Information GmbH verfolgt mit seinen Arbeiten in den Bereichen der Sicherheitsanwendungen und Abrechnungssystemen, Plug&Play Lösungen. Diese Grundlagen werden durch eigene Forschungen- und Evaluierungen vervollständigt und fließen somit erfolgreich in praktische Anwendungsbereiche mit ein. Unser Projekt "Virtuell Communcation Terminal" zeigt Zukunftsperspektiven von der Smart Card bis zur holographischen Kommunikation.

Biometrische Verfahren

Über biometrische Verfahren wird derzeit sehr viel berichtet und diskutiert. Dennoch warten sie nach wie vor auf ihren Durchbruch und Einsatz.. Das dieser in absehbarer Zeit gelingt, ist voraussehbar.

Das Volumen für den weltweiten **Electronic Commerce** wird derzeit von der Boston Consulting Group auf 6 bis 12 Mrd. USD geschätzt. Nach der Jahrhundertwende soll das Volumen drastisch steigen. Entsprechend wächst auch der Bedarf an Sicherheit.

Eine ganze Reihe von Gründen spricht für die Anwendung biometrischer Verfahren in diesem Bereich, wie Sprecher-, Iris-, Gesichts- und dynamische Unterschriftenerkennung sowie Erkennung der Handgeometrie und des Fingerabdrucks:

- Die digitale Signatur nach dem Signaturgesetz (SigG) wird in Kürze verfügbar sein. Dabei werden Chipkarten eingesetzt, bei denen sich der berechtigte Anwender durch Eingabe eines PIN Codes authentifiziert.

Die Schwächen dieses Verfahrens sind allgemein bekannt.

Die PIN ist leicht kompromittierbar, und so besteht eine relativ hohe Gefahr, daß rechtsverbindliche Unterschriften mißbräuchlich geleistet werden. Hier können biometrische Verfahren für ein wesentliches Plus an Sicherheit sorgen.

- Die Techniken der Mustererkennung, basierend auf der Anwendung von künstlichen neuronalen Netzen, haben einen langen Forschungsweg hinter sich und stehen vor dem produktiven Einsatz.
- Die Leistungsfähigkeit moderner Computersysteme und Chips ist derart ausgeprägt, daß selbst komplette und sehr rechenintensive Erkennungsprozesse bei einer akzeptablen Antwortzeit auf Standard-Hardware lauffähig werden. Hinzu kommen gewaltige Fortschritte bei der Entwicklung von Sensoren in den letzten Jahren.
- Der SB-Bereich bei Banken und auch der Sicherheitsbedarf in anderen Massenanwendungen, z.B. die Authentifikation bei Mobiltelefonen, erzeugen „Marktdruck“. Die bisher verwendeten Verfahren sind reif für ihre Ablösung.

Hier haben biometrische Systeme ihre große Chance.

Verifikation und Identifikation

Die Prüfung der Berechtigung einer Person und die Beweisbarkeit ihrer Aktivitäten sind die zentralen Kernfragen. Grundlegend sind die Benutzer- oder Anwendererkennung. Berechtigte müssen von Nichtberechtigten sicher unterschieden werden. Meist geht es dabei um die Verifikation der Identität, d.h. es wird geprüft, ob eine Person wirklich diejenige ist, die sie vorgibt zu sein.

Verifikation ist im allgemeinen weniger aufwendig als eine Identifikation. Bei dieser wird ohne die Vorgabe einer Identität durch Vergleichen herausgefunden, um wen es sich handelt. Dazu werden bekannterweise im Zuge polizeilicher Ermittlungen Fingerabdrücke und Fotos genutzt.

Die Verifikation kann prinzipiell auf drei verschiedene Arten vorgenommen werden. –

- Zum einen durch Besitz, z.B. eines Ausweises oder Schlüssels, wobei die bekannten Probleme der sicheren Aufbewahrung, von Diebstahl, des unberechtigten Weitergebens, des Verlierens oder der Fälschung bestehen.
- Eine andere Möglichkeit liegt im Wissen einer Person. Typische Beispiele hierfür sind Paßwort und PIN-Code. Hier liegen die Gefahren im Aushorchen, Ausspähen, unberechtigtem Weitergeben, aber auch im Vergessen.
- Eine dritte Möglichkeit besteht in der Verwendung biometrischer Merkmale. Sie haben nicht die aufgeführten Nachteile.

Man hat sie immer dabei, kann sie nicht vergessen oder verlieren, und sie sind (praktisch) nicht zu

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

fälschen. Lediglich durch Verletzungen oder Krankheit kann es eine Einschränkung der Verfügbarkeit geben. Biometrische Merkmale sind dadurch gekennzeichnet, daß sie in bezug auf ein und dieselbe Person eindeutig sind, aber bei verschiedenen Personen mehr oder weniger stark variieren.

Biometrische Merkmale

Es gibt biometrische Merkmale, die sich im Lebensablauf einer Person nicht ändern, wie beispielsweise der Fingerabdruck, oder aber nur sehr langsam, wie beispielsweise das Gesicht.

Es ist zweckmäßig, zwischen

- physiologischen, man spricht auch von statischen Merkmalen, und
- verhaltensorientierten (dynamischen) zu unterscheiden.

Physiologisch ist ein Merkmal oder auch das dieses Merkmal feststellende Verfahren dann, wenn eine anatomische Eigenschaft gemessen und festgestellt wird, beispielsweise die Handgeometrie.

Zu den physiologischen Merkmalen zählen: Gesicht, Handgeometrie, Fingerabdruck, Augenhintergrund, Iris und auch Venenstruktur, Körpergeruch, Gesichtstemperatur. Letztere sicher bislang ohne große praktische Relevanz, teilweise jedoch schon auf Messen gezeigt.

Zu den verhaltensorientierten Merkmalen zählen: Stimme, Unterschrift, Tastatureingaberhythmus.

Kombinierte Verfahren zur Verifikation/ Identifikation beziehen zwei oder mehrere Merkmale ein.

Bislang hat keines der automatisiert arbeitenden biometrischen Verfahren in größerem Umfang einen kommerziellen Einsatz erfahren. Einschränkungen gibt es bekannterweise beim Fingerabdruck der für kriminalistische Zwecke schon seit sehr langer Zeit genutzt wird, ebenso bei Unterschriften für Verträge und im Zahlungsverkehr. Beim Telefonieren erkennt man seinen Gesprächspartner an der Stimme. In Ausweisen liefern Paßfotos die Identität.

Wie soll man nun die am Markt verfügbaren oder kurz vor der Einführung stehenden Systeme bewerten?

Akzeptanzproblem

Einige der wichtigsten Kriterien sind unter dem Begriff Akzeptanz zu subsumieren. Im Hinblick auf einige biometrische Merkmale sind durchaus auch Ängste anzutreffen. Es wird beispielsweise befürchtet, daß ein Laserstrahl bei der Abtastung des Augenhintergrunds Schäden hervorrufen könnte. Der Komfort und die Geschwindigkeit einer Überprüfung sind weitere Kriterien.

Auch hygienische Bedenken werden immer wieder vorgetragen, allerdings auch an Stellen, die nach allgemeiner Meinung nicht unbedingt nachvollziehbar sind. Es sei nur daran erinnert, daß bei Verfahren, die den Fingerabdruck nutzen, natürlich auch ein Körperkontakt entsteht. Das unvermeidbare Anfassen von Türklinken, Telefonhörern oder beispielsweise Haltestangen in öffentlichen Verkehrsmitteln dürfte unter Hygieneaspekten aber ohne jeden Zweifel noch wesentlich dramatischer einzustufen sein.

Auch die Ängste vor einer mißbräuchlichen Anwendung sind stark verbreitet, z. B. bei einer „gespeicherten Unterschrift“, wie man meint. Zur Beurteilung biometrischer Systeme gehören weiter die Art und Dauer der Erfassung berechtigter Personen, die Investitions- und Folgekosten und nicht zuletzt die Marktverbreitung bzw. das vorhandene Erfahrungspotential des Herstellers oder Vertreibers.

Fehlerproblem

In der Praxis sind die bei der Verifikation auftretenden Fehler von größtem Interesse. Alle biometrischen Verfahren benötigen im weitesten Sinne einen Sensor, um das biometrische Merkmal zu messen. Sie erzeugen aus dieser aktuellen Messung ein aktuelles (Bit-)Muster, das mit einem gespeicherten Referenzmuster verglichen wird. Ein typisches Kennzeichen dabei ist, daß Referenz- und aktuelles Muster niemals bzw. nur mit verschwindend geringer Wahrscheinlichkeit hundertprozentig übereinstimmen, z. B. aufgrund von Meßtoleranzen oder Umgebungseinflüssen bei der Messung. Das heißt, daß bei der Entscheidung, ob eine Person akzeptiert oder zurückgewiesen wird, immer eine mehr oder weniger große Abweichung zwischen aktuell erzeugtem und Referenzmuster toleriert werden muß, deren Ausmaß über einen Schwellen- oder Toleranzwert eingestellt werden kann. Bei den verhaltensorientierten Verfahren wird u. U. durch

das Ergebnis einer aktuellen Messung das gespeicherte Referenzmuster angepaßt. Man spricht dann von einer Referenzmusteradaption.

Eine Person kann berechtigt oder nicht berechtigt sein, und das biometrische System kann die Entscheidung fällen, sie zu akzeptieren oder zurückzuweisen. Wird eine berechtigte Person akzeptiert oder eine nicht berechtigte zurückgewiesen, sind keine Fehler aufgetreten. Andernfalls sind zwei qualitativ unterschiedliche Fehler denkbar, nämlich die unberechtigte Zurückweisung einer berechtigten Person (False Rejection - FR) und die Akzeptanz einer nicht berechtigten Person (False Acceptance-FA). Mit welcher Wahrscheinlichkeit (Rate - R) diese Fehler auftreten, d. h. welchen Wert FAR und FRR haben, hängt zum einen vom Verfahren ab, zum zweiten vom System und zum dritten von der Toleranzschwelle, mit der es eingestellt wird. Prinzipiell kann bzw. muß eine niedrigere Wahrscheinlichkeit des einen Fehlertyps mit einer erhöhten Wahrscheinlichkeit des anderen erkauft werden.

Ein ideales System würde beide Fehlerraten auf 0% bringen können. Das ist jedoch, wie oben ausgeführt, nicht realisierbar. Vielmehr bedingen sich diese Fehler, wie bereits gesagt, gegenseitig. Es besteht die folgende Abhängigkeit durch Einstellung der Akzeptanz- bzw. Toleranzschwelle: Wird die Wahrscheinlichkeit für den Fehlertyp 1 verringert, steigt gleichzeitig die Wahrscheinlichkeit für den Fehlertyp 2 und umgekehrt.

Im Extremfall bedeutet die Reduktion der Fehlerrate des einen Fehlers auf 0% den Anstieg beim anderen auf 100% und umgekehrt: Entweder wird ein Berechtigter niemals abgewiesen, d. h. aber dann auch, jeder Unberechtigte wird akzeptiert oder umgekehrt. Deshalb sieht man sich in der Praxis grundsätzlich vor die Entscheidung gestellt, welcher Fehler ist schlimmer? Soll das Motto sein „Berechtigte bloß nicht abweisen“ oder „Unberechtigte bloß nicht zulassen“ oder soll ein Kompromiß dazwischen liegen? Darüber ist bei der jeweiligen Anwendung zu entscheiden.

Verfahrensvergleich

Beim Vergleich verschiedener Verfahren sollten beide Fehlermöglichkeiten herangezogen werden. Das ist aber wegen der Abhängigkeit von der einstellbaren Toleranzschwelle nicht ohne weiteres möglich. Deshalb wird häufig auf die Gleichfehlerrate (EER - Equal Error Rate) zurückgegriffen, die dann vorliegt, wenn FAR und FRR gleich groß sind. Nach heutigem Stand der Technik ist eine Reduktion der EER auf deutlich unter 1 % möglich.

Herstellerangaben zur Gleichfehlerrate sind meist auch auf Nachfrage nicht zu bekommen. Ähnlich sieht es mit Angaben darüber aus, welche Datenbasis einer Aussage über Fehlerwahrscheinlichkeiten zugrunde liegt und mit welchem Vorgehen sie ermittelt wurden. Natürlich wäre ein Vergleich über unabhängig durchgeführte Tests der verschiedenen Verfahren bzw. am Markt verfügbarer Systeme hinsichtlich verschiedener Bewertungskriterien wünschenswert. Beispielsweise ist ein Vergleich hinsichtlich

- EER
- Leistungsfähigkeit - Geschwindigkeit - Benutzerakzeptanz - Kosten

interessant, wobei diese einzelnen Kriterien auch noch näher zu definieren wären. Solche Tests gibt es aber nicht, allerdings ist ein Kriterienkatalog von einer Arbeitsgemeinschaft bei TeleTrusT (Erfurt) in Angriff genommen worden und liegt in einer ersten Version vor.

Derzeit sind keine Tests bekannt, die die Anfälligkeit bzw. Resistenz gegenüber aktiven Angriffen auf Software, Hardware usw. erkennen lassen. Allerdings bemühen sich die meisten Hersteller, solchen Angriffsversuchen Rechnung zu tragen. Ein gutes Beispiel hierfür ist, daß ein abgetrennter Finger zur Überwindung des Systems verwendet werden könnte. Gegenmaßnahmen sind beispielsweise eine Spektrogrammauswertung des Lebendfingers bezüglich des Hämoglobins oder aber eine Messung des Sauerstoffgehalts in der Fingerspitze.

Nicht untersucht und meist nicht einmal in der Diskussion ist die Gefahr eines Angriffs zur Überwindung eines biometrischen Systems, die davon ausgeht, daß das gespeicherte Referenzmuster ausgeforscht oder manipuliert werden kann. So wäre es möglich, beispielsweise durch Einspeisung eines gefälschten, künstlich erzeugten, aktuellen Musters über eine typischerweise vorhandene Schnittstelle zwischen biometrischem und Zugangsschutzsystem, wiederholt oder dauerhaft, eine Berechtigung vorzutäuschen. Während ein Paßwort oder PIN-Code meist in gewissen Abständen gewechselt wird, bleibt das biometrische Merkmal entweder konstant oder ändert sich nur innerhalb von

Zeiträumen, die diese Änderung unter Sicherheitsaspekten irrelevant machen. Dieser Vorteil würde hier also zum Nachteil gereichen.

Verbindung zu Chipkarten

Chipkarten haben eine weite Verbreitung erlangt. Zu ihren Anwendungsgebieten zählt u. a. die Nutzung als Zahlungsmittelfunktion. Dabei ist an die elektronische Geldbörse zu denken, beispielsweise aber auch an die Autobahn Mailand-Brescia, wo ein computergesteuertes System an den Mautstellen drahtlos mit einem Kartenlesegerät im KFZ kommuniziert. Übermittelt werden die relevanten Daten für die später vorzunehmende Inrechnungstellung der Mautgebühr. Eine massenhafte Anwendung als Dokument findet die Chipkarte als Krankenversichertenkarte. Sicherheitsfunktionen erfüllen die im Bereich der mobilen Telekommunikation, der digitalen Signatur und der Datenverschlüsselung eingesetzten Chipkarten.

Chipkarte: breite Anwendungsmöglichkeiten

Am Ende der derzeitigen Entwicklung der Chipkarte steht die multifunktionale Prozessorchipkarte, in die ein Krypto-Coprozessor integriert ist. Es stehen praktisch kleine Computer mit eigenem Betriebssystem zur Verfügung, die durchaus in der Lage sind, verschiedenen Anwendungen bzw. Anwendungssystemen nebeneinander gerecht zu werden. Durch eine sogenannte Partitionierung lassen sich auf einem Chip unterschiedliche und voneinander unabhängige Bereiche mit unterschiedlichen Funktionen und Zugriffsberechtigungen abbilden. Eine Kommunikation zwischen diesen Funktionsbereichen ist möglich. Dadurch erschließen sich für eine einzelne Chipkarte sehr breite Anwendungsmöglichkeiten.

Die derzeitige Entwicklung auf dem Chipkartenmarkt ist durch zwei Effekte geprägt. Zum einen ist ein Substitutionseffekt zu verzeichnen, d. h., die Chipkarte verdrängt aufgrund ihrer Vorteile andere, beispielsweise die Magnetkarte, weil hohe Sicherheitsanforderungen zu erfüllen sind. Weiter ist ein Expansionseffekt zu nennen, das soll heißen, es werden neue Anwendungsbereiche erschlossen. Ein jüngeres Anwendungsbeispiel ist das Check-In als Flugticketersatz der Lufthansa.

Symbiose: Chipkarte und biometrische Verfahren

Geht man also davon aus, daß bei denjenigen, die Inhaber einer Chipkarte sind, in Zukunft erhöhte Sicherheitsanforderungen zu befriedigen sind und daß die Preise für solche Chipkarten wegen ihrer massenhaften Verbreitung rückläufig sind, könnte es zu einer Ergänzung zwischen Chipkarten und biometrischen Systemen kommen.

Das Referenzmuster, erzeugt mit Hilfe eines biometrischen Verfahrens aus einem oder mehreren Merkmalen, wird auf einer Chipkarte gespeichert. Das ist technisch kein Problem mehr, weil zum einen die Speicherkapazität der Chips gestiegen ist, zum anderen durch geeignete Kompressionsverfahren Referenzmuster nur noch relativ wenig Raum beanspruchen. Auch sind neue Sensoren (Fingerabdruck) entwickelt worden, die sogar eine Integration des biometrischen Systems in die Chipkarte erlauben dürften, allerdings sind noch nicht alle Probleme gelöst.

Bei der Speicherung des Referenzmusters auf der Chipkarte lassen sich deren mögliche Sicherheitsfunktionen nutzen: Fälschungs- und Manipulationssicherheit, Ausleseschutz und Verschlüsselungsfunktionen bei der Kommunikation. Ein großer Vorteil ergibt sich durch die Unabhängigkeit von der ortsgebundenen Speicherung in einer Datenbank. Bei der Unterschriftenverifikation können so auch mögliche Akzeptanzprobleme vermieden werden. Auf Messen konnte beobachtet werden, daß Mitarbeiter der Standbesatzung sich weigerten, ihre Unterschrift als Referenzmuster im System speichern zu lassen. Statt dessen wurden, man höre und staune, drei Kreuze (xxx) erfaßt. Argumentiert wurde offiziell damit, daß so die Sicherheit des Systems noch drastischer demonstriert werden könne.

Ausblick

Berührungslos arbeitende biometrische Systeme oder solche, die keine andere Benutzeraktivität erfordern als eine ohnehin notwendige Bedienfunktion, z. B. „Knopfdruck“ zum Einschalten eines PC oder eines Handies, haben naturgemäß die besten Aussichten für eine Akzeptanz durch den Nutzer. Von den derzeit am Markt verfügbaren Systemen bieten somit die Gesichtserkennung, die Fingerabdruck- und die

Irisüberprüfung sowie die Unterschriftenverifikation gute Voraussetzungen.

Wie die Gesichtserkennung erfolgt die Irisüberprüfung ebenfalls über eine Kamera. Bei dieser ist jedoch für eine kurze Zeit, quasi naturgemäß, eine genauere Ausrichtung der Augen erforderlich. Die Fingerabdruckprüfung ist mit neuen Sensoren direkt - ohne zwischengeschaltete Geräte wie Scanner - möglich geworden. Bei der Unterschriftenverifikation gibt es Systeme, die nicht mehr die Verwendung eines speziellen Stiftes erfordern.

In naher Zukunft werden biometrische Systeme die bisher verwendeten konventionellen nicht ersetzen. Eine kombinierte Anwendung mit konventionellen Verfahren, in erster Linie ist dabei an den Einsatz eines Mediums, das als Ausweis fungiert (Chipkarte), zu denken, kann jedoch erhöhte Sicherheit und auch Bequemlichkeit bieten. Biometrische Systeme könnten PIN-Codes und Paßwörter ablösen und durch die Vermeidung von deren Schwächen das Sicherheitsniveau erhöhen oder wie bei der digitalen Signatur ein ganzes System auf ein durchgängig hohes Sicherheitsniveau anheben.