

# **Authentifizierung und Identitätsmanagement**

Benchaalal Amine

Betreuerin: Jutta Mülle

Seminartitel: Sicherheit und technischer Datenschutz  
in Informationssystemen  
Seminar im Sommersemester 2006

31. Oktober 2006

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>3</b>
1.1	Motivation . . . . .	3
1.2	Gliederung . . . . .	3
<b>2</b>	<b>Authentifizierung</b>	<b>3</b>
2.1	Definition . . . . .	3
2.2	Man weiss etwas . . . . .	4
2.2.1	Passwort . . . . .	4
2.2.2	Historisches . . . . .	4
2.2.3	Faktoren in der Sicherheit eines Kennwortsystems . . . . .	4
2.2.4	Beispiele von Kennwörtern . . . . .	6
2.2.5	Password-Cracking-Programme . . . . .	8
2.2.6	Schwache und starke Kennwörter . . . . .	9
2.2.7	PIN . . . . .	10
2.3	Man ist bzw kann etwas :Biometrische Merkmale . . . . .	10
2.3.1	Definition . . . . .	10
2.3.2	Fingerabdruck . . . . .	10
2.3.3	Gesichtserkennung . . . . .	10
2.3.4	Venenerkennung . . . . .	11
2.3.5	Handschrift . . . . .	11
2.3.6	Tippverhalten . . . . .	11
2.4	Man hat etwas :Besitz . . . . .	11
2.4.1	Bespiele . . . . .	11
2.4.2	PublicKey-Verfahren . . . . .	11
2.5	2-Faktoren Authentifizierung . . . . .	12
2.6	3-Faktoren Authentifizierung . . . . .	12
<b>3</b>	<b>Identitätsmanagement</b>	<b>12</b>
3.1	Warum Identitätsmanagement? . . . . .	12
3.2	Definition . . . . .	13
3.3	Pseudonyme . . . . .	13
3.3.1	Personenpseudonyme . . . . .	13
3.3.2	Geschäftsbeziehungsseudonyme . . . . .	13
3.3.3	Tansaktionspseudonyme . . . . .	13
3.4	Identität im Internet . . . . .	14
3.4.1	Das Domain Name System (DNS) . . . . .	14
3.4.2	Cookies . . . . .	14
<b>4</b>	<b>Fazit</b>	<b>16</b>
	<b>Literaturverzeichnis</b>	<b>18</b>

# 1 Einleitung



## 1.1 Motivation

Es passiert Heutzutage, dass bei einer Kom für den er sich ausgibt. Die Rolle der Identitätsmanagement und der Authentifizierung ist hauptsächlich der Nachweis der Benutzer-Identität und damit auch der Benutzungsberechtigung gegenüber dem System[3], und so werden auch noch Systemfunktionen vor Missbrauch zu schützen. Dazu dienen hauptsächlich Passwörter, persönliche ID-Nummern, kryptografische Techniken sowie Magnet- oder Chip-Ausweiskarten. Eine strenge Authentifizierung kann mit der Vergabe von Einmal-Passwörtern.

## 1.2 Gliederung

Zunächst wird im Kapitel 2 die Authentifizierung definiert, dann wird gezeigt welche Arten von Authentifizierung es gibt. Das Kapitel 3 stellt die Identitätsmanagement vor. Das Kapitel 4 ist eine Zusammenfassung.

# 2 Authentifizierung

## 2.1 Definition

Die Authentifizierung (engl. authentication) bezeichnet den Vorgang der Überprüfung der Identität eines Gegenübers (z.B. einer Person oder eines Computerprogramms). Die Authentisierung bezeichnet den Vorgang des Nachweises der eigenen Identität. Im Englischen wird zwischen den beiden Begriffen nicht unterschieden, das Wort authentication steht für beides. Dementsprechend werden auch im Deutschen die Begriffe

oft synonym verwendet. Die Authentisierung, das heißt das Nachweisen der eigenen Identität, kann auf drei verschiedenen Wegen erfolgen:

## **2.2 Man weiss etwas**

### **2.2.1 Passwort**

Ein Passwort oder Kennwort ist ein allgemeines Mittel zur Authentifizierung eines Benutzers innerhalb eines Systems, der sich durch eine eindeutige Information (das Kennwort) dem System gegenüber ausweist. Die Authentizität des Benutzers bleibt daher nur gewahrt, wenn er das Passwort geheim hält.

### **2.2.2 Historisches**

Ein Kennwort (auch Losung, Losungswort oder Parole) war im Militär ursprünglich ein als Erkennungszeichen dienendes Wort, um bei Dunkelheit oder bei unbekanntem Kombattanten Freund und Feind zu unterscheiden. Noch heute wird von nachtpatrouillierenden Soldaten auf Manöver die Frage nach der Parole gestellt. Im Mittelalter wurde manche Burgbelagerung durch den Verrat des Losungswortes entschieden.

### **2.2.3 Faktoren in der Sicherheit eines Kennwortsystems**

Die Sicherheit eines Kennwort geschützten Systems hängt von einigen Faktoren ab, die am Halten des Kennwortes vollständig geheim gebunden werden.

- **Langlebigkeit eines Kennwortes**  
Das Zwingen der Benutzer, Kennwörter zu ändern häufig stellt sicher, daß ein gültiges Kennwort in den falschen Händen unbrauchbar schnell abläuft und wird. Viele Betriebssysteme liefern solche Eigenschaften, obwohl sie nicht allgemein hinbenutzt werden.
- **Wahrscheinlichkeit, daß ein Kennwort geschätzt werden kann**  
Studien der Produktion Computersysteme haben für die durchweg gezeigten Dekaden, die ungefähr 40% aller Benutzer- gewählten Kennwörter bereitwillig geschätzt werden.

Ein Kennwort konnte guessable sein, wenn ein Benutzer ein einfach-entdecktes Stück persönliche Informationen als Kennwort wählt. Diese sind offensichtliche Wahlen Benutzer und angreifende Partei. Persönliche Daten über fast jeder sind jetzt von den verschiedenen Quellen vorhanden und also müssen angenommen werden, durch eine angreifende Partei bekannt.

Ein Kennwort ist verletzbar, wenn es in einer Liste gefunden werden kann. Wörterbücher sind für viele Sprachen vorhanden und bestehen dort Listen der allgemein-gewählten Kennwörter. In den Prüfungen auf Phasensystemen, sind Wörterbuchangriffe so routinemäßig erfolgreich, die die Software, die diese Art des Angriffs einführt, für viele Systeme vorhanden ist.

Ein zu kurzes Kennwort, möglicherweise gewählt für Mühelosigkeit des Schreibens, ist immer einfach zu schätzen, und leicht knowable, wie verletzbar von seiner unzulänglichen Länge. Ein extremes Beispiel betrachten: ein einzelnes Buchstabe Kennwort erfordert nur 128 Vermutungen höchstens, Zugang zu garantieren.

- Wahrscheinlichkeit, daß ein Kennwort entdeckt werden kann  
Kennwörter können durch die surfende, Burglary, Erpressung, Erpressung oder Drohungen Schulter entdeckt werden. Ungefähre Kennwortlänge kann sogar ohne die Schulter entdeckt werden, die indem man einfach Tastaturklicken zählt oder Fingeranträge surft, merkt. Aktive theft/snoop/extortion Vorkaufmasse wie automatisches Ende von Kennwörtern können sogar in den Fällen arbeiten, in denen ein Kennwort ohne seinen Inhaber verglichen wird, der es berücksichtigt. Diese Vorkehrung stört viele Benutzer und also wird weit kleiner häufig verwendet, als ein Interesse für Sicherheit vorschlagen würde. Und Müllcontainertauchen ist für Situationen überraschend fruchtbar, in denen empfindliche gedruckte Daten mit unzulänglicher Vorkehrung weggeworfen werden. Kennwörter durch psychologische Handhabung der Benutzer zu erhalten ist ein Beispiel der Sozialtechnik. "hallo. Systemsteuerung hier. Wir führen eine Sicherheit Prüfung durch. Können wir Ihr Kennwort haben, also können wir fortfahren? Arbeiten astonishingly häufig.
- Wahrscheinlichkeit, daß an ein Kennwort erinnert werden kann  
Die sichersten Kennwörter sind lange, gelegentliche Ansammlungen Buchstaben , die, leider von einer Sicherheit Perspektive sind, ziemlich hart, damit die meisten Leute sich erinnern. Benutzer mit solchen Kennwörtern werden mächtig gereizt, um Pfosten-es Mitteilung an ihrer Anzeige zu haften, und ein Kennwort, das notiert worden ist, ist, nicht mehr wie sicher, abhängig von, welchen Drohungen angetroffen werden. Die meisten Beobachter sehen notierte Kennwörter als notwendigerweise unsicher an.
- Verfahren für das Ändern von von Kennwörtern  
Normalerweise muß ein System eine Weise zur Verfügung stellen, ein Kennwort, irgendein zu ändern, weil ein Benutzer glaubt, daß das gegenwärtige Kennwort ist oder als Vorbeugungsmaßnahme verglichen worden konnte. Wenn ein neues Kennwort zum System in einer unencrypted Form geführt wird, kann Sicherheit verloren werden bevor das neue Kennwort in die Kennwortdatenbank sogar angebracht werden kann. Wenn einem verglichenen Angestellten das neue Kennwort gegeben wird, ist es wahrscheinlich verloren . Nichtsdestoweniger werden neue Kennwörter häufig zum Benutzerüberschuß das Telefon resultierend aus einer Nachfrage nach Bequemlichkeit gegeben.
- Von gespeicherten Kennwörtern bilden  
Wenn das System jedes Kennwort in einer cryptographically geschützten Form speichert, zum tatsächlichen Kennwort dann zugänglich machen ist schwierig für ein snooper , die herum innerhalb des Systems stoßen, während Gültigkeitserklärung weiterhin möglich bleibt. Jedoch selbst wenn erhöhte das Verwenden der ausreichenden Schlüsselverfahren, um zur Verfügung zu stellen Sicherheit, kein Kennwortsystem kann total immun sein anzugreifen. Bestehen die Werkzeuge, die einige Klartextkennwörter feststellen können, eine Kopie der Akte gegeben, die verschlüsselten enthält. Von indem es das verschlüsselte Resultat jedes Wort , von irgendeiner Wortansammlung vergleicht, kann ein Programm viele Computersysteme automatisch in Angriff nehmen. Dieses ist eine Variante eines Gewaltangriffs, in dem alle möglichen Kennwörter versucht werden . Diese Wörterbuchangriff Werkzeuge zeigen durch Bestehen die relativen Stärken der unterschiedlichen Kennwortwahlen gegen solche Angriffe.

- Methode des Neu legens des Kennwortes zum authenticator  
Kennwörter können zum Snooping verletzbar sein, wann, übertragend die beglaubigende Maschine oder Person. In einem Extremfall ist ein Kennwort, das durch Publikation in einer großen Zirkulation Zeitung übertragen wird, völlig unsicher. Wenn das Kennwort als elektrische Signale auf körperlicher Verdrahtung zwischen den Anwenderzugriffpunkt und das zentrale System, welches die Kennwortdatenbank steuert getragen wird, ist es ausgesetzt das Snooping durch irgendeine einer Vielzahl Leitung der klopfenden Methoden und wird auch, obwohl kleiner offensichtlich so unsicher sein. Dieses kann erträglich in einigen Fällen sein. Wenn es dem Internet übertragen wird, jedermann fähig, die Pakete aufzupassen, das LOGON- Informationen Dose snoop mit sehr kleiner Möglichkeit der Abfragung zu enthalten. Dieses ist weniger wahrscheinlich, erträglich zu sein.

## 2.2.4 Beispiele von Kennwörtern

- Transaktionsnummer  
Eine Transaktionsnummer(TAN) ist ein Einmalpasswort. Es gibt verschiedene Ansätze um TANs zu erzeugen, zu prüfen und zum Nutzer zu übertragen. Einige davon werden im folgenden beschrieben,

TAN-Liste :

Als Teilnehmer beim Electronic Banking erhält man, meist per Post, eine Liste von Transaktionsnummern. Bei jedem Buchungsvorgang - der Transaktion - muss eine TAN eingegeben werden. Sie ist eine Ergänzung zur PIN. Falls die Bank nach Eingabe der korrekten PIN einen Buchungsauftrag mit korrekter TAN erhält, geht sie davon aus, dass der Auftrag vom Kunden abgesendet wurde. Die TAN wird von der Bank als Quasi-Unterschrift interpretiert. Sie verfällt nach einmaligem Gebrauch. Wenn die TAN-Liste zur Neige geht, erhält der Kunde von der Bank eine neue.

Indizierte TAN-Liste:

Noch einen Schritt weiter geht das Verfahren der indizierten TAN, kurz iTAN: Der Kunde kann hier seinen Auftrag nicht mehr mit einer beliebigen TAN aus seiner Liste legitimieren, sondern die Bank fordert den Kunden auf, die TAN an einer bestimmten Position (Index) seiner dazu nun durchnummerierten Liste einzugeben. Die Positionsangabe wird von der Bank mit den Kernparametern der vorher eingegebenen Auftragsdaten verknüpft, beispielsweise mit der Kontonummer und Bankleitzahl des Empfängers einer Überweisung. Selbst wenn nun dieser mit der angeforderten TAN unterschriebene Auftrag von einem Angreifer abgefangen wird, so kann er keinen Nutzen daraus ziehen: Für andere Überweisungsziele oder gar andere Aufträge wird die einmal angeforderte TAN nicht mehr angefragt werden.

TAN mit Bestätigungsnummer:

Das Verfahren kann um eine Bestätigungsnummer (BEN) erweitert werden, durch die sich nach der Auftragsannahme im Gegenzug die kontaktierte Bank nochmals als rechtmäßiger Kommunikationspartner ausweist.

- Das Einmalpasswort  
Ein Einmalpasswort wird zur Authentifizierung genutzt. Im Gegensatz zu "nor-

malen"Passwörtern ist jedes Passwort jedoch nur für einen einzigen Vorgang (z. B. Anmeldung an einem Rechner) gültig und kann kein zweites Mal benutzt werden. Bei jedem Vorgang muss also ein neues, einmaliges Passwort benutzt werden, welches möglichst nie wieder vorkommt. Diese Vorgehensweise verbessert die Sicherheit des Anmeldevorganges, da ein Angreifer ein abgehörtes Passwort nicht für eine weitere Authentifizierung selbst benutzen kann. Gegen das Angriffsszenario "Man in the Middle", bei dem ein solches Passwort vor dem Eintreffen beim Gegenüber abgefangen wird, helfen Einmalpasswörter jedoch nicht. Als Problem erweist sich dabei die Frage, wie beide Seiten wissen, welches Passwort denn für einen Anmeldevorgang gerade gültig ist. Prinzipiell kommen mehrere Möglichkeiten in Betracht:

Passwortlisten:

Bei diesem System werden vorgefertigte Listen von Passwörtern auf beiden Seiten hinterlegt. Diese Liste wird entweder der Reihe nach abgearbeitet (d. h.: die Einträge sind durchnummeriert) oder einfach ein noch nicht benutzter Wert wahlfrei ausgewählt. Dieser Wert wird als Passwort übermittelt und auf beiden Seiten aus der Liste gestrichen. Die TAN-Listen beim Online-Banking sind ein Beispiel für eine Passwortliste.

Einmalpasswort nach Lamport:

Das Einmalpasswort nach Lamport, auch als Lamport Hash bezeichnet, ist ein System zur Erstellung von Einmalpasswörtern mittels eines Algorithmus. Der Algorithmus basiert im wesentlichen auf der mehrfachen Anwendung einer Einwegfunktion.

- Password Aging

Password Aging ist eine weitere Methode, die von Systemadministratoren verwendet wird, um unsichere Passwörter in einem Unternehmen zu verhindern. Password Aging bedeutet, dass Benutzer nach einer bestimmten Zeit (gewöhnlich 90 Tage) aufgefordert wird, ein neues Passwort festzulegen. Die Theorie dahinter ist, dass wenn ein Benutzer in periodischen Abständen dazu aufgefordert wird, sein Passwort zu ändern, ein geknacktes Passwort einem Cracker nur für eine gewisse Zeit nützlich ist. Der Nachteil von Password Aging ist jedoch, dass Benutzer eher dazu neigen, sich die Passwörter aufzuschreiben. Es gibt zwei Programme für das Festlegen von Password Aging unter Red Hat Enterprise Linux: den Befehl `chage` oder die grafische Applikation User Manager (`system-config-users`). Die Option `-M` des Befehls `chage` legt die maximale Anzahl von Tagen fest, für die das Passwort gültig ist. Wenn Sie zum Beispiel festlegen wollen, dass ein Benutzer-Passwort nach 90 Tagen ungültig wird, geben Sie den folgenden Befehl ein: `chage -M 90 username` Ersetzen Sie im oben genannten Befehl `username` mit dem Namen des Benutzers. Wenn Sie nicht möchten, dass das Passwort ungültig wird, verwenden Sie den Wert `99999` nach der Option `-M` (dies ist etwas mehr als 273 Jahre). Wenn Sie die grafische Applikation User Manager für Password-Aging-Policies verwenden möchten, klicken Sie auf Hauptmenü (im Panel) Systemeinstellungen, Benutzer und Gruppen oder geben Sie den Befehl `system-config-users` an einem Shell-Prompt ein (z.B. in einem XTerm- oder GNOME-Terminal). Klicken Sie auf den Tab Benutzer, wählen Sie den Benutzer aus der Liste aus und klicken Sie auf Eigenschaften im Menü (oder wählen Sie Datei, Eigenschaften aus dem Pull-

Down Menü). Klicken Sie dann auf Passwort-Info und geben Sie hier die Anzahl der Tage ein, bevor das Passwort ablaufen soll, wie in der folgenden Abbildung gezeigt.

The image shows a dialog box with four tabs: 'User Data', 'Account Info', 'Password Info', and 'Groups'. The 'Password Info' tab is selected. The text inside the dialog reads: 'User last changed password on: Thu 30 Sep 2004 12:00:00 AM EST'. Below this is a checked checkbox labeled 'Enable password expiration'. There are four input fields: 'Days before change allowed' with the value '0', 'Days before change required' with the value '90', 'Days warning before change' with the value '0', and 'Days before account inactive' with the value '0'. At the bottom right of the dialog are two buttons: 'Cancel' (with a red 'X' icon) and 'OK' (with a green checkmark icon).

- Challenge Response

Der Begriff Aufgabenlösungsauthentifizierung oder englisch Challenge-Response Authentication bezeichnet ein sicheres Authentifizierungsverfahren eines Teilnehmers auf Basis von Wissen. Hierbei stellt ein Teilnehmer eine Aufgabe (engl. challenge), die der andere lösen muss (engl. response).). Ein sehr einfaches Beispiel ist die Frage nach einem Passwort. Dabei ist die Herausforderung die Frage nach dem Passwort, und die korrekte Antwort ist das richtige Passwort. Bei dieser Methode kann das Passwort jedoch von Angreifern auf der Leitung mitgehört werden. Deswegen verwendet man Verfahren, bei denen das Wissen nicht preisgegeben werden muss, um herauszufinden, ob der andere Teilnehmer dies auch weiß. Der Teilnehmer muss nicht das Passwort übertragen, sondern er muss lediglich sicher beweisen, dass er das Passwort kennt.

### 2.2.5 Password-Cracking-Programme

Bei sogenannten Dictionary-Attacken werden riesige Wortlisten durchprobiert[1]. Dies führt häufig schnell zum vorgegebenen Ausgangswert, weil sehr viele Leute den Begriff "Passwort" wörtlich nehmen und eben bekannte Wörter oder Namen wählen. Dictionary-Cracker sind sehr einfach zu programmieren und laufen extrem schnell. Sie finden jedes Passwort, welches in der Wortliste enthalten ist.

Bei sogenannten Brute-Force-Attacken (auch "exhaustive search" genannt) werden alle möglichen Kombinationen von Zeichen (aus einem gewählten Zeichensatz) durchprobiert. Brute-Force-Cracker sind theoretisch in der Lage, jedes beliebige Passwort zu

finden. Je nach verwendetem Zeichensatz und Länge des gewählten Passwortes kann die Suche extrem lange dauern.

Es gibt auch Cracker, welche eine kombinierte Dictionary- und Brute-Force-Attacke durchführen (daher auch Hybrid-Cracker genannt). Hybrid-Cracker durchsuchen Wortliste und fügen den Wörtern zusätzlich alle Kombinationen aus einem gewählten Zeichensatz an (voran- und nachgestellt). Es ist auch denkbar, dass Hybrid-Cracker dem häufig verwendeten Ansatz, bestimmte Buchstaben durch Zeichen zu ersetzen (z.B. Buchstabe "O" durch Ziffer "0" oder Buchstabe "S" durch "\$Zeichen), Rechnung tragen. Hybrid-Cracker finden das gesuchte Passwort häufig schneller als reine Brute-Force-Cracker, weil viele Leute Passwörter nach einem bekannten Schema aufbauen. So verwenden beispielsweise viele Leute Passwörter, welche aus einem bekannten Wort und einer nachgestellten Jahreszahl (z.B. "geheim99") bestehen. [5]

### 2.2.6 Schwache und starke Kennwörter

Ein schwaches Kennwort würde eins sein, das kurz waren, oder das schnell geschätzt werden könnte, indem man eine Teilmenge aller möglichen Kennwörter wie Wörter im Wörterbuch, in den Eigennamen, in den Wörtern, die auf dem Benutzernamen basieren oder in den allgemeinen Veränderungen auf diesen Themen suchte. Ein starkes Kennwort würde genug lang anders produceable sein, gelegentlich, oder nur durch den Benutzer, der es wählte, damit ' das Schätzen ' für es eine zu lange Zeit erfordert. Die Zeitspanne meinte, um ' zu lang ' zu sein schwankt mit der angreifenden Partei, mit den Betriebsmitteln der angreifenden Partei und mit wie der Wert des Kennwortes zur angreifenden Partei. So konnte das Kennwort eines Kursteilnehmers nicht wertSEIN mehr als einige Sekunden der Maschinenzeit, während ein steuernder Zugang des Kennwortes Geld-Umfüllsystem einer großen Bank zum elektronischen viele Wochen der Maschinenzeit wertSEIN konnte. ' schwach ' und ' stark ' nur eine ziemlich flockige Bedeutung in diesem Kontext haben und werden fehl. angewendet sehr häufig in den Weisen, die beträchtliche Präzision andeuten. Aber merken, dass ein ' starkes Kennwort ' in dieser Richtung von einem Benutzer noch gestohlen werden, betrogen werden oder erpressen werden kann, oder zufällig hörte, indem Sie einige Kommunikationen Mittel klopfen, oder koptierte von Pfosten-Es Mitteilung. Stark hat eine streng begrenzte Bedeutung in diesem Kontext. Es ist gesagt worden, daß das ideale Kennwort unmöglich sein sollte sich zu erinnern und folglich unwahrscheinlich, guessable zu sein. Solche Kennwörter sind sicher d.h. stärker härter, damit eine angreifende Partei entdeckt; unter aber sie werden häufig notiert, und so einfacher, zu entdecken, indem man Fächer oder Tastaturen oder hinter Abbildungen oder für Pfosten-es Mitteilungen schaut. Solche Kennwörter erwähnen regelmäßig Verletzungen einer anderen Spitze von Common und kluge, Rat – ein Kennwort nie überall notieren, egal was". Das Erfordern ' der starken ' Kennwörter folglich verursacht häufig die unbeabsichtigte Konsequenz, daß viele solche Kennwörter in der Praxis unsicher werden, indem sie die Wahrscheinlichkeit, daß sie verloren sind, snooped erhöhen, kopiert, oder anders verglichen. Persönliche Gedächtnislehre wird manchmal empfohlen, leitet d.h. Sachen, die zu Ihnen denkwürdig sind, aber nicht zu anderen z.B. das Kennwort ' Iw21wIfvP ', ein schwieriges, sich an Zeichenkette zu erinnern, von ' mir waren 21, als ich zuerst Paris ' besichtigte ab, vielleicht leicht erinnert. Jedoch wenn Ihre erste Erfahrung von Paris zu Ihnen wichtig ist, kann es möglich sein, dieses Kennwort vom Wissen von Ihnen zu schätzen. In diesem Fall würde dieses nicht eine vernünftige Kennwortwahl sein.

### 2.2.7 PIN

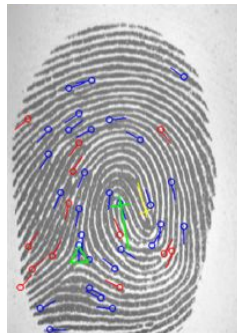
Die PIN (Persönliche Identifikationsnummer) ist eine andere Form des Kennwortes mit einer ausschließlich numerischen Zeichenfolge, die nicht immer vom Benutzer frei wählbar ist und z.B. beim Geldabheben vom Bankautomaten Verwendung findet. Sie ist meistens 4 Stellen lang.

## 2.3 Man ist bzw kann etwas :Biometrische Merkmale

### 2.3.1 Definition

Biometrische Merkmale werden häufig unterschieden in aktiv/passiv, verhaltens-/physiologiebasiert oder dynamisch/statisch. Zu den langfristig stabilen verhaltensbasierten Merkmalen zählen die Stimme, die Hand- oder Unterschrift, das Tippverhalten und die Gangdynamik. Langfristig stabile physiologische Merkmale sind beispielsweise der Fingerabdruck, die Iris oder die Handgeometrie. Diese Unterscheidung ist zwar weitgehend akzeptiert, es existieren aber Grenzbereiche. So sind die meisten verhaltensbasierten biometrischen Merkmale beeinflusst durch die Physiologie, etwa die Stimme durch den Sprachapparat des Menschen.

### 2.3.2 Fingerabdruck



Der Fingerabdruck (oder das Daktylogramm) ist ein Abdruck der Papillarleisten am Endglied eines Fingers. Da bisher keine zwei Menschen mit dem gleichen Fingerabdruck bekannt sind, geht man von der Einzigartigkeit des Fingerabdrucks aus. Da die Minutienausbildung das Ergebnis eines zufälligen Prozesses ist, haben selbst eineiige Zwillinge unterschiedliche Fingerabdrücke. Zumeist besitzt jeder Mensch einen Fingerabdruck; es gibt jedoch Anomalien durch die kein Fingerabdruck entsteht; fernerhin kann sich ein Fingerabdruck durch Narben-Bildung dauerhaft aber nur lokal verändern. Man unterscheidet verschiedene Merkmale des Fingerabdrucks: o grobe Merkmale: Schleifen, Bögen, Windungen o feinere Merkmale: Minutien o Porenstruktur

### 2.3.3 Gesichtserkennung

Gesichtserkennung analysiert die Ausprägung sichtbarer Merkmale innerhalb des frontalen Kopfes, gegeben durch geometrische Anordnung und Textureigenschaften der Oberfläche. Es ist zu unterscheiden zwischen der Lokalisation eines Gesichts im Bild (engl. face detection) und der Zuordnung des Gesichts zu einer bestimmten Person

(engl. face recognition). Im ersten Fall wird geprüft, ob und wo ein Gesicht zu sehen ist und im zweiten Fall wird bestimmt, wer zu sehen ist.

### **2.3.4 Venenerkennung**

Bei der Venenerkennung wird eine Infrarotaufnahme von der Handgefäßstruktur gemacht. Der Verlauf der Venen und Adern ist bei einem Menschen genauso einzigartig wie der Fingerabdruck. Bei diesem Verfahren wird auch die Temperatur der Hand gemessen um zu erkennen dass die Hand auch wirklich an einem lebendigen Menschlichen Körper ist. Die Venenerkennung gehört zu den sichersten biometrischen Verfahren.

### **2.3.5 Handschrift**

Sie bezeichnet o die Schreibschrift o das individuelle charakteristische Schriftbild eines Menschen, der Begriff wird jedoch auch im übertragenen Sinn gebraucht: einer Sache jemandes Handschrift aufdrücken/-drängen/-prägen o ein Manuskript

### **2.3.6 Tippverhalten**

Das Tippverhalten auf Tastaturen ist ein in der Biometrie angewandtes Merkmal. Es dient zur Identifizierung einer Person aufgrund des Rhythmus, in dem sie bestimmte Wörter auf einer Tastatur eingibt. Dazu werden die Zustände der Tasten mehrere tausend Mal pro Sekunde abgefragt, während die Person mehrmals das selbe Wort eingibt.

## **2.4 Man hat etwas :Besitz**

### **2.4.1 Beispiele**

Karte, Schlüssel, PublicKey-Verfahren

### **2.4.2 PublicKey-Verfahren**

Dieser Verfahren benutzt ein Schlüsselpaar SK und PK ,bei dem alles, was mit PK verschlüsselt wurde, nur mit SK wieder entschlüsselt werden kann, und umgekehrt. Die Asymmetrie entsteht dadurch, dass nur der Private Key SK geheimgehalten wird (z. B. durch eine Passwortphrase geschützt verschlüsselt abgespeichert), und der Public Key PK veröffentlicht wird.

Die Abbildung 1 zeigt, wie SK und PK beim Chiffrieren und Signieren jeweils andersherum verwendet werden.

Das Hauptproblem ist die Übermittlung des Public Keys über unsichere elektronische Wege. Hier ist es eigentlich immer nötig, dass entweder ein persönliches Treffen mit Übergabe einer Diskette stattfindet oder ein sog. Fingerprint des Schlüssels mit gedruckten Veröffentlichungen oder durch Vorlesen am Telefon verglichen wird. Da dies bilateral für je zwei Kommunizierer ziemlich mühsam ist, wird die Überprüfung jeweils von einer Zertifizierungs-Instanz vollzogen. Sobald man deren "Wurzelzertifikat" überprüft hat, kann man alle dort zertifizierten Public Keys als überprüft glauben.

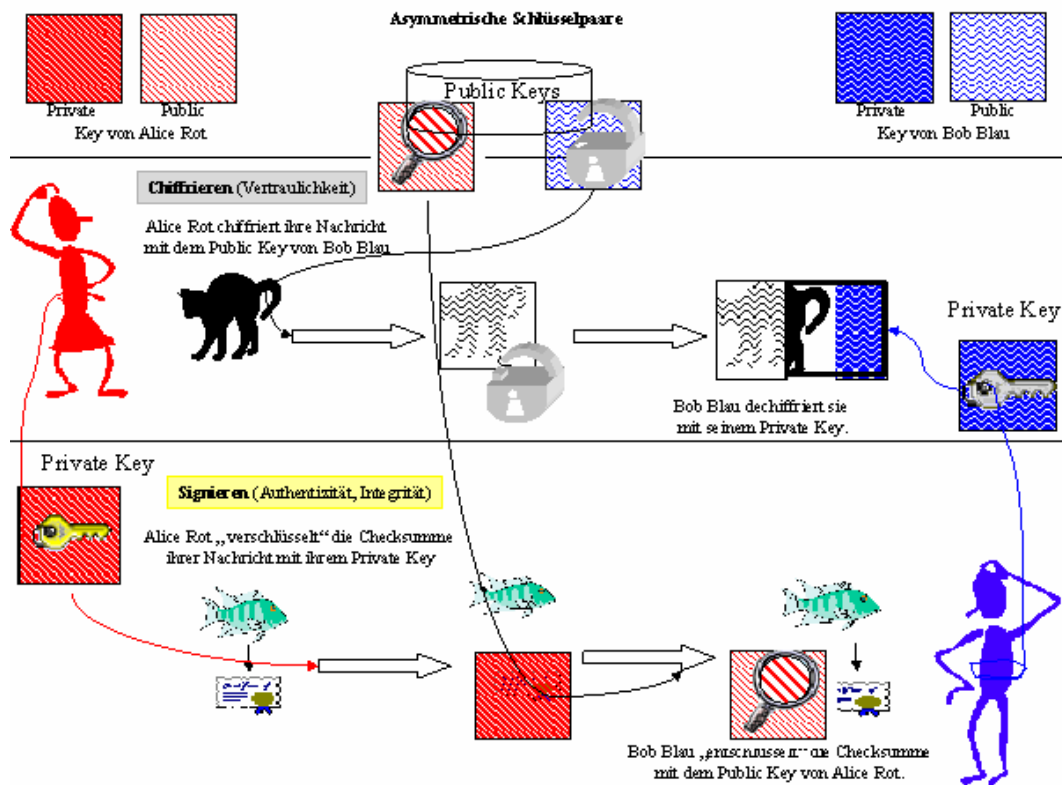


Abbildung 1: PublicKey Verfahren

## 2.5 2-Faktoren Authentifizierung

- Bankkarte +
- Kreditkarte + Unterschrift
- PIN + Fingerabdruck
- Benutzername + Passwort

## 2.6 3-Faktoren Authentifizierung

- Benutzername + Passwort + Fingerabdruck
- Benutzername + Passwort + SecurID Token

# 3 Identitätsmanagement

## 3.1 Warum Identitätsmanagement?

Einer der Gründe, warum man sich in Unternehmen mit Identitätsmanagement (im anglierten Sprachgebrauch Identity- Management) beschäftigt, ist die Anforderung, personenbezogene Daten konsistent, ständig verfügbar und verlässlich bereitzuhalten. Dienste wie ein Mail-System oder eine Personalbuchhaltung sind auf diese Daten angewiesen, ohne sie wäre kein individualisierter Betrieb möglich.

## 3.2 Definition

Die Identitätsmanagement in Computernetzen soll einen Benutzer in die Lage versetzen, persönliche Merkmale nur gezielt und bewusst weiterzugeben. Identitätsmanagement dient also dem Schutz personenbezogener Daten. Hierzu benötigen die Benutzer eine bewusst Kontrolle über die Information, mit deren Hilfe in unterschiedlichen Situationen weitergegebene personenbezogenen Daten verknüpft werden können. persönliches Merkmal ist in diesem Papier in erster Linie ein Kennzeichen für eine Personengemeint, das für sich allein meist keinen eindeutigen Personenbezug darstellt, aber in der Verketzung mit mehreren persönlichen Merkmalen zu einem identifizierenden Computerdatensatz wird und die Identität einer Person bestimmt. Beispiele für solche persönlichen Merkmale sind zum Beispiel Geburtsdatum, Wohnort, Staatsangehörigkeit, oder Beruf.

## 3.3 Pseudonyme

Häufig ist es möglich, über Identifikatoren zur Entität zu gelangen, solche Identifikatoren werden Pseudonyme genannt. Pseudonyme können nach dem Grad der erreichbaren Anonymität eingeteilt werden. Bezogen auf die Gegebenheiten heutiger Computernetze werden im folgenden die drei wichtigsten Pseudonymitätsstufen erläutert.

### 3.3.1 Personenpseudonyme

Wird von einer Person über einen längeren Zeitraum und in vielen Kommunikationsbeziehungen mit unterschiedlichen Kommunikationspartnern das gleiche Pseudonym verwendet, spricht man von einem Personenpseudonym. Ein typisches Beispiel ist die E-Mail-Adresse einer Person, so wie wir sie heute vorfinden (z.B. oliver.berthold@gmx.de und hannes@icsi.berkeley.edu). Ein Personenpseudonym stellt also ein potentielles Personenkennzeichen dar, selbst dann, wenn die Zeichenkette, die das Pseudonym repräsentiert, auf den ersten Blick keinen direkten Personenbezug aufweist.

### 3.3.2 Geschäftsbeziehungspseudonyme

Wählt sich eine Person für die Kommunikation mit einem bestimmten Kommunikationspartner jeweils ein neues, dann aber gleich bleibendes Pseudonym (z.B. eine neue E-Mail-Adresse), das keinen direkten Personenbezug aufweist (z.B. 1182643@hotmail.com), und verwendet sie das Pseudonym in keiner Kommunikationsbeziehung mit anderen Kommunikationspartnern, dann handelt es sich um ein Geschäftsbeziehungspseudonym.

### 3.3.3 Transaktionspseudonyme

Falls sich eine Person entscheidet, jeweils für jede Transaktion ein neues Pseudonym einzusetzen (z.B. heute 3735428@yahoo.com und morgen jazzfan@hotmail.com )beim Herunterladen von Musik von ein und demselben MP3-Server),dann spricht man von einem Transaktionspseudonym. Ein Transaktionspseudonym wird also nach Beendigung der Transaktion von diesem Teilnehmer nie wieder verwendet.

## 3.4 Identität im Internet

Normalerweise wird heute die "Identität" eines Teilnehmers am Internet durch seine Email-Adresse bestimmt, da diese meist ein unverwechselbares Merkmal des Teilnehmers ist. Die Email-Adresse ist normalerweise der Loginname gefolgt von der kompletten Domainadresse unter der man zu erreichen ist. Wenn man also von seinem Rechner aus eine Mail schreibt ist dies die Adresse die der Empfänger der Mail als Absenderangabe erhält. In email Nachrichten erhält man weitere Informationen aus der Path: -Zeile in der alle Hosts stehen über die diese Mail zu dem jeweiligen Empfänger gelaufen ist. Das Fälschen dieser Informationen erfordert "gehackte" Mailsoftware auf einem Rechner der am weitertransport dieser Nachricht beteiligt ist. Diese Methode ist ziemlich ungebräuchlich. Nicht so ungebräuchlich ist das Fälschen dieser Kette am Absenderort, so das Hosts in der Liste schon zum Zeitpunkt der Erstellung der Mail gefälscht sind. Diese Nachrichten zurückzuverfolgen kann sehr schwierig wenn nicht sogar unmöglich sein wenn die ursprünglichen gefälschten Felder Namen von existierenden Maschinen und existierende Transferrouen darstellen. Also es ist nicht einfach im Internet Anonym zu sein, ohne Schutzmaßnahmen erfährt die Gegenseite bei der Kommunikation auch die IP-Adresse des Benutzers.[2] Doch auch Cookies, Browserinformationen oder zuletzt besuchte Seiten können ohne Wissen des Anwenders weitergegeben werden. Mit der IP-Adresse eines Benutzers kann der Anbieter von Internetdiensten die tatsächliche Identität des Benutzers nicht ermitteln, er kann jedoch Hinweise wie den Provider und oft auch noch Land und Region herausfinden, wenn der Benutzer sich nicht schützt. Für die Identität muss eine Anfrage beim Provider erfolgen, dieser besitzt die nötigen Daten, wenn der Benutzer sich nicht schützt. Andere Teilnehmer könnten sich über das Verhalten dieses Benutzers bei dessen Provider beschweren, welcher dann in der Regel Maßnahmen für diesen Benutzer ergreift (z. B. Sperrung). Strafverfolgungsbehörden können natürlich die Herausgabe der Identität eines Benutzers verlangen, wenn unter dieser IP-Adresse Straftaten begangen wurden, was den Behörden bei entsprechenden Maßnahmen des Benutzers aber nichts nützt.[4]

### 3.4.1 Das Domain Name System (DNS)

Das DNS ist einer der wichtigsten Dienste im Internet, seine Hauptaufgabe ist, die Auflösung von Namen, d.h. auf Namensanfragen mit der zugehörigen IP-Adresse zu antworten. Hauptsächlich wird das DNS zur Umsetzung von Domainnamen in IP-Adressen (forward lookup) benutzt. Dies ist vergleichbar mit einem Telefonbuch, das die Namen der Teilnehmer in ihre Telefonnummer auflöst. Das DNS bietet somit eine Vereinfachung, weil Menschen sich Namen weitaus besser merken können als Zahlenkolonnen. So kann man sich den Domainnamen `www.tikchbila.fr` leichter merken, als die dazugehörige IP-Adresse `124.36.30.55`.

### 3.4.2 Cookies

- **Definition**

Cookies sind kleine Datensätze (wenige Byte), die im Rechner des Benutzers abgespeichert werden. Sie ermöglichen dem Betreiber des Webservers, für den das Cookie generiert wurde, den Benutzer zu verfolgen, solange bzw. so oft er sich auf den Webseiten dieses Webservers aufhält. [2]

- **Gefahrlose / sinnvolle Cookies**

Die Idee, die hinter den Cookies steckt, ist, die Zustandslosigkeit von HTTP aufzuheben. So ist es prinzipiell möglich, eine automatische Anmeldung an WWW-Sites zu implementieren. Benutzer können sogar Preference-Einstellungen abspeichern. FTP-Search ist ein gutes Beispiel: Der User kann über einen Knopf `SSave Configuration` seine Sucheinstellungen speichern. Ein anderes sinnvolles Einsatzgebiet ist das Einkaufen per WWW: In den Cookies wird dann der aktuelle Inhalt des Warenkorbs gemerkt.

- **Gefahren durch Cookie-Diebstahl**

Zwar werden die Dateien, in denen die Cookies gespeichert werden, von den üblichen Cookie-fähigen Browsern mit sinnvollen Permission-Flags (unlesbar für group und world) angelegt, sicher sind sie deshalb aber noch lange nicht. Immer wieder gab und gibt es Fehler in verbreiteten Browsern, die es Angreifern erlauben, unberechtigt auf Benutzerdateien, und damit auf Cookie-Inhalte, zuzugreifen. In Cookies sollten also keinesfalls wichtige Authentisierungs-Schlüssel oder gar Kreditkarten-Nummern oder PINs gespeichert werden. Eine gelegentliche Sichtkontrolle der, in der Regel menschenlesbaren, Cookie-Datei (z.B. bei Netscape Navigator: `$HOME/.netscape/cookies`) kann auf keinen Fall schaden.

- **Maßnahmen gegen Cookies**

Um sich vor Cookies und anderen sicherheitsgefährdenden Technologien zu schützen, braucht man sich aber nicht allein auf die Möglichkeiten zu beschränken, die der jeweils eingesetzte Browser von Haus aus bietet. Eine Möglichkeit wäre zum Beispiel: Die Cookie-Verwaltung unter MS Internet Explorer 6 ( Abbildung 2 ) Da besteht eine Möglichkeit, den Browser hinsichtlich der Cookie-Verwaltung entsprechend den eigenen Wünschen einzustellen.

Es empfiehlt sich auch vielmehr, sich auf einschlägigen Freeware-Seiten umzuschauen, auf denen sich oft kostenlose Programme zum Schutz der Privatsphäre finden. Eins dieser Tool ist z.B. WebWasher (Abbildung.3)

Das Freeware-Tool WebWasher zum Schutz der Privatsphäre Dieser besitzt auch einen Cookie-Filter, mit dem man Cookies einer spezifischen Behandlung unterwerfen kann. Dazu muss man einfach nur den Domain-Namen eingeben (durch Klicken auf "Neu") und setzt eine Bewertung für Cookies dieser Web-Seite. "Gute" Cookies werden durchgelassen, "schlechte" Cookies werden ausgefiltert und unbekannte Cookies (markiert mit einem Fragezeichen) werden nach einer vom Anwender definierten Zeitspanne wieder gelöscht. Dabei kontrolliert WebWasher den Datenstrom zwischen User und Web bidirektional, also in beide Richtungen, um eine saubere Filterung zu gewährleisten. Neben dem Cookie Filter verfügt WebWasher aber auch noch über weitere sicherheitsrelevante Funktionen, über die der MS Internet Explorer 6 nicht verfügt, so z.B. auch über einen Filter, um WebBugs unschädlich machen zu können.

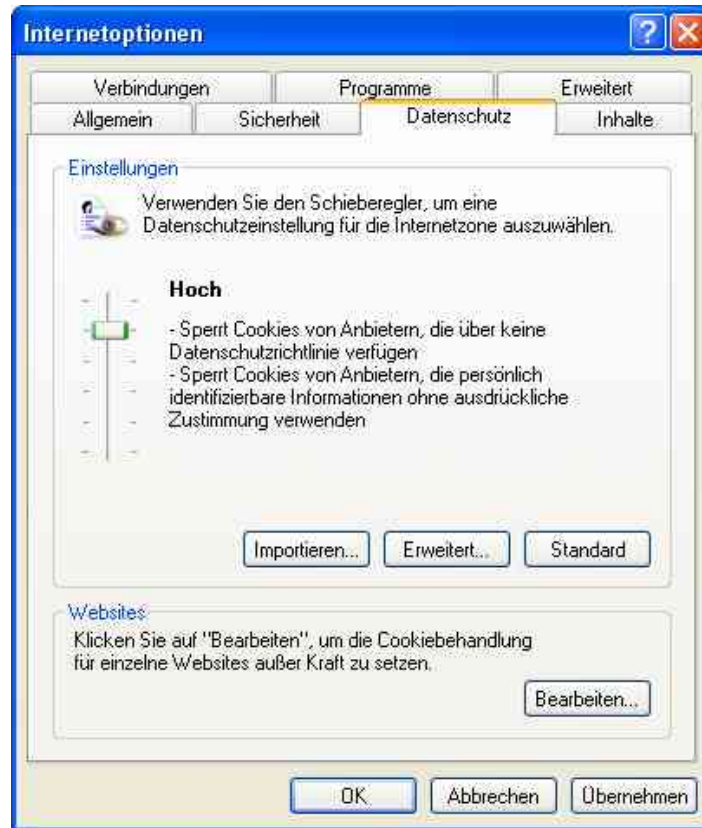


Abbildung 2: Verwaltung

## 4 Fazit

Das Vertrauen der Nutzer in die Sicherheit von Identitätsmanagement ist nach wie vor gering. Viele Anwender halten sich und ihre Daten für nicht ausreichend geschützt. Der Authentifizierungsvorgänge funktionieren nicht immer fehlerfrei, es passiert auch, Während einer Internet-Sitzung zum Beispiel, beim Besuch einer Seite übermittelt ein Surfer sehr viele Informationen die vom Zielrechner ausgewertet werden. Deshalb sollte, wann immer es möglich ist, anonym kommuniziert werden.



Abbildung 3: WebWasher

## Literatur

- [1] M. Bishop, *Computer Security*. Addison-Wesley, 2003.
- [2] K. Henry, *Anonymität ganz einfach und legal - Die Tarnkappe für das Internet - nicht nur für Langstreckenflieger*. DANA, 03/2005 S. 13ff.
- [3] G. Krüger, *Lehr- und Übungsbuch Telematik*, 3rd ed. Hanser, 2004.
- [4] T. Roessler, "WHOIS: Datenschutz im DNS?" *Datenschutz und Datensicherheit*, vol. 26, no. 11, 2002.
- [5] J. von Helden, *Verbesserung der Authentifizierung in IT-Systemen durch spezielle Dienste des Betriebssystems*. Shaker Verlag, 1998.