

# **Authentifizierung und Identitätsmanagement**

---

**Amine Benchaalal**

**Betreuerin : Jutta Mülle**

**Sicherheit und technischer Datenschutz in  
Informationssystemen  
Seminar im Sommersemester 2006**

# Inhalt

---

## o Authentifizierung

- Motivation
- Definition
- Wie Authentifizierung erfolgt:
  - Wissen
  - Biometrische Merkmale
  - Etwas Haben
- Beispiele ,Vor- und Nachteile

# Motivation

---

## Warum Authentifizierung?

- Missbrauch vertraulicher Daten
- Personenschaden durch Manipulation kritischer Daten

Unser Ziel ist das durch die  
Authentifizierung zu verhindern, d.h:

- ✓ Vertraulichkeit der Daten
- ✓ Integrität der Daten
- ✓ Authentizität der Beteiligten

# Definition

---

- Die **Authentifizierung** bezeichnet den Vorgang der Überprüfung der Identität eines Gegenübers
- Die **Authentisierung** bezeichnet den Vorgang des Nachweises der eigenen Identität, und kann auf drei verschiedenen Wegen erfolgen :

# Wissen: man weiß etwas (Beispiel: PIN, Passwort)

---



Ein **Passwort** (Kennwort): Ist ein allgemeines Mittel zur Authentifizierung eines Benutzers innerhalb eines Systems, der sich durch eine eindeutige Information dem System gegenüber ausweist.

Die Authentizität des Benutzers bleibt daher nur gewahrt, wenn er das Passwort geheim hält.

# Aufbau eines (relativ) sicheren Passworts

---

- Langlebigkeit eines Kennwortes
- Wahrscheinlichkeit, dass ein Kennwort geschätzt werden kann
- Verfahren für das Ändern von Kennwörtern
- Wahrscheinlichkeit, dass ein Kennwort entdeckt oder erinnert werden kann

# Passwort-Check

---

Ob Ihr Passwort stark oder schwach ist,  
können Sie unter diese Seite erfahren:

[https://passwortcheck.datenschutz.c  
h/check.php/](https://passwortcheck.datenschutz.c<br/>h/check.php/)

# Beispiele von Kennwörter

---

- PIN/TAN Passwort
- Einmal Passwort
- Challenge-Response
- Password aging

# Das Festlegen von Password Aging unter Red Hat durch die grafische Applikation User Manager

---

The screenshot shows the 'Password Info' tab of the User Manager application. At the top, there are four tabs: 'User Data', 'Account Info', 'Password Info', and 'Groups'. Below the tabs, the text reads 'User last changed password on: Thu 30 Sep 2004 12:00:00 AM EST'. A checkbox labeled 'Enable password expiration' is checked. Below this, there are four input fields for password aging settings:

- Days before change allowed: 0
- Days before change required: 90
- Days warning before change: 0
- Days before account inactive: 0

At the bottom right, there are two buttons: 'Cancel' (with a red 'X' icon) and 'OK' (with a green checkmark icon).

# Vor- und Nachteile

---

- kann vergessen werden
- kann einfach dupliziert und damit verteilt werden
- kann abgehört werden

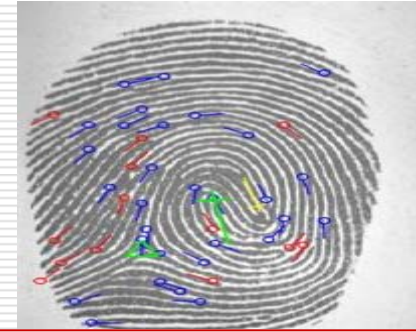
# Password-Cracking-Programme

---

- Dictionary-Attacken  
Riesige Wortlisten durchprobieren
- Brute force-Attacken  
Alle möglichen Kombinationen von Zeichen durchprobieren

# Biometrische Merkmal: man ist bzw kann etwas

---



- Biometrische Merkmale:
  - aktiv/passiv
  - verhaltens-/physiologiebasiert
  - dynamisch/statisch

# Biometrische Merkmal

---

- Zu den langfristig stabilen verhaltensbasierten Merkmalen zählen :
  - die Stimme
  - die Hand- oder Unterschrift
  - das Tippverhalten auf der Tastatur

# Biometrische Merkmal

---

- Langfristig stabile physiologische Merkmale sind beispielsweise:
  - der Fingerabdruck
  - die Iris
  - die Handgeometrie

# Weitere Beispiele

---

- Gesichtserkennung
- Venenerkennung
- Sprachverhalten

# Vor -und Nachteile

---

- fehlerhafte Erkennung möglich (False Acceptance)
- fehlerhafte Zurückweisung möglich (False Rejection)
- ist im Laufe der Zeit mehr oder weniger veränderlich und schlechter erkennbar
- je nach Merkmal Lebenderkennung erforderlich

# Besitz: man hat etwas

---

- Beispiele:

Schlüssel, Karte

# Vor-und Nachteile

---

- kann verloren gehen
- kann nur schwer dupliziert werden
- kann übergeben bzw. weitergereicht werden
- kann gestohlen werden

---

# Identitätsmanagement

# Inhalt

---

- Identitätsmanagement
  - Motivation
  - Definition
  - Pseudonymität
  - Identität im Netz
  - Anonymität im Internet
  - Host Identität
  - Domain Name System
  - Cookies

# Motivation

---

- Warum Identitätsmanagement?
  - Beispiel : Ein Mitarbeiter hat ein Mail-Konto, das nur ihm selbst zugeordnet ist. Hierfür benötigt er eine individuelle Mailadresse, einen so genannten Account mit dem dazugehörigen Passwort. Diese Daten sind nur für ihn und nicht für die Allgemeinheit bestimmt.

# Motivation

---

➤ Gegenbeispiel:

Eine Firmenpräsentation ist für alle Mitarbeiter einheitlich und bedarf keiner Individualisierung.

# Definition

---

- Also **Identitätsmanagement** in Computernetzen soll einen Benutzer in die Lage versetzen, persönliche Merkmale nur gezielt und bewusst weiterzugeben.

**Persönliches Merkmal** ist ein Kennzeichen für eine Person gemeint.

# Pseudonymität

---

- **Pseudonyme** können nach dem Grad der erreichbaren Anonymität eingeteilt werden. Bezogen auf die Gegebenheiten heutiger Computernetze werden im folgenden die drei wichtigsten Pseudonymitätsstufen erläutert.

# Pseudonymität

---

- **Personenpseudonym**
- **Geschäftsbeziehungspseudonym**
- **Transaktionspseudonym**

# Identität im Netz

---

- *Weshalb ist die Identität (Un)wichtig im Internet?*

*Das Konzept der Identität ist eng verbunden mit Kommunikation ,*  
und die Kommunikation (z.B. via **Email**)  
wäre unmöglich ohne gewisse  
Konventionen für die Identifikation  
untereinander.

# Anonymität im Internet

---

- Bei **Aktivitäten im Internet** fühlen sich viele Benutzer anonym. Diese Anonymität ist jedoch trügerisch. Ohne Schutzmaßnahmen erfährt die Gegenseite bei der Kommunikation die IP-Adresse des Benutzers. Doch auch Cookies, Browserinformationen oder zuletzt besuchte Seiten können ohne Wissen des Anwenders weitergegeben werden.

# Host Identität

---

- Die **Host-Identität** ist eng verknüpft mit der Vernetzung.
- Falls der Host mit dem Netz verbunden ist, kann er einen oder mehreren Namen (IP-Adressen) haben, es hängt davon ab, wie die Schnittstellen vom Netz strukturiert sind.
- Falls er nicht verbunden ist, dann kann er irgendeinen Name haben, weil das nur lokal benutzt wird.

# Domain Name System

---

- Das **Domain Name System (DNS)** ist einer der wichtigsten Dienste im Internet.

Hauptaufgabe ist die Auflösung von Namen, d.h. auf Namensanfragen mit der zugehörigen IP-Adresse zu antworten.

# Cookies

---

- **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.

# Maßnahmen gegen Cookies

---

Die öffentliche Diskussion zum Thema Cookies blieb natürlich auch nicht den politischen Instanzen verborgen, und so stand schon seit einiger Zeit eine EU-weite Datenschutzdirektive zur Debatte ,aber leider vergeblich.

Es bleibt damit letztendlich dem User überlassen, ob und wie er sich gegen Cookies schützt.

# Maßnahmen gegen Cookies

---

- Problem: man kann beim einfachen Ablehnen jeglicher Cookies manche Seiten gar nicht mehr nutzen .

Aber es besteht eine Möglichkeit, den Browser hinsichtlich der Cookie-Verwaltung entsprechend den eigenen Wünschen einzustellen.

Beispiel: *Die Cookie-Verwaltung unter MS Internet Explorer 6*



# Maßnahmen gegen Cookies

---

Eine andere Möglichkeit wäre der Einsatz von **Zusatz-Tools** .

Beispiel: *Das Freeware-Tool WebWasher zum Schutz der Privatsphäre*



- 
- **Anonymität und Identität im Internet sind relativ.**
  - **Es kann passieren, dass das Identitätsmanagement nicht funktioniert, weil Manipulationen bei heutiger Hard- und Software oft einfach sind.**

**Beispiel: durch Trojanische Pferde**

---

**Danke  
Für  
Ihre Aufmerksamkeit!**