# Informationssicherheit

# 6. Authentifizierung

Prof. Dr. Christoph Skornia

christoph.skornia@oth-regensburg.de

# Authentifizierung

- **Ziel:**
  - eindeutige Identifikation und Nachweis der Identität
  - Abwehr von Identitätsdiebstahl, Spoofing-Angriffen
- **Problem:**
  - Nicht nur Mensch-zu-Gerät Interaktion, sondern auch Gerät-zu-Gerät bzw. {Gerät, Dienst} zu {Dienst, Gerät}
  - Bem.: zunehmende Vernetzung u. Miniaturisierung: M2M-Kommunikation steigt rapide an (z.B. IoT) !
- **Identifiziert werden müssen:**
  - Personen
  - Geräte (Web-Server, Laptop, Handy, ...) und
  - Dienste (Dateisystem, Amazon, Bankportal, ....)

# Authentifizierung: Klassen

- Authentifizierung durch
  - **Wissen:** z.B. Passworte, PINs, kryptogr. Schlüssel
  - **Besitz:** z.B. Smartcard, USB-Token, SIM-Karte (Handy)
  - **biometrische Merkmale:** z.B. Fingerabdruck, Iris, Tippverhalten
- **Mehrfaktor-Authentifizierung:** (Kombination von Konzepten)
  - z.B. Handy, Online-Banking mit Token, EC-Karte, Smartcard
  - Beispiel: 2-Faktor-Authentifikation beim Handy:
    1. Authentifikation über PIN (Wissen) gegenüber SIM-Karte
    2. Besitz der SIM-Karte (enthält geheimen Schlüssel KSIM) SIM-Karte authentifiziert sich gegenüber dem Netz mit KSIM
- Einseitige oder Wechselseitige Authentifizierung möglich
- Sprache: Der Benutzer authentisiert sich am Server, der Server authentifiziert den Benutzer

# Authentifizierung durch biometrische Merkmale

## Biometrisches Merkmal:

Verhaltenstypische oder physiologische Eigenschaft eines Menschen, die diesen eindeutig charakterisieren

## Anforderungen an biometrische Merkmale:

- Universalität: Jede Person besitzt das Merkmal
- Eindeutigkeit: Merkmal ist für jede Person verschieden
- Beständigkeit: Merkmal ist unveränderlich
- quantitative Erfassbarkeit mittels Sensoren
- Performance: Genauigkeit und Geschwindigkeit
- Akzeptanz des Merkmals beim Benutzer
- Fälschungssicherheit

# Authentifizierung durch biometrische Merkmale

## Unterschiede zur wissensbasierten Authentisierung:

- Merkmal ist personengebunden: Konsequenz?
- Charakteristische Merkmale müssen extrahiert und mit Referenzwert verglichen werden: Probleme?

## Klassen biometrischer Merkmale:

- physiologische Merkmale (statisch):
  - keine oder nur sehr begrenzte Möglichkeiten zur Auswahl oder Änderung von Referenzdaten
  - z.B. Fingerabdruck, Gesichtsbild, Handgeometrie, Retina
- Verhaltensmerkmale (dynamisch):
  - Merkmal ist nur bei bestimmter Aktion vorhanden;
  - Möglichkeiten zur Auswahl/Änderung von Referenzdaten
  - z.B. Unterschriften-Dynamik, Sprache, Tippverhalten (Keystroke)

# Authentifizierung durch biometrische Merkmale

## Vorgehen bei biometrischer Authentifikation:

1. Messdatenerfassung durch biometrischen Sensor und Digitalisierung
   (Feature Extraction)
2. Enrollment: Registrierung eines Benutzers:
   Aufnahme, Auswahl und Speicherung der Referenzdaten
   z.B. 5 bis 7 verschiedene Fingerabduck-Werte

## Bei Authentifizierung:

1. Erfassung der aktuellen Verifikationsdaten (mittels Sensoren)
2. Verifikationsdaten digitalisieren (u.a. ggf. normieren)
3. mit gespeichertem Referenzwert vergleichen, Toleranzschwellen sind notwendig

# Authentifizierung durch biometrische Merkmale

## Sicherheitsprobleme bei biometrischen Techniken:

- Angriffe
  - Direkte Täuschung des biometrischen Sensors durch Attrappen u.a. Gummi-Finger
  - Einspielen von Daten unter Umgehung des biometrischen Sensors
    - Wiedereinspielen abgehörter Daten (Replay-Angriffe)
    - Einspielen eigens verschaffter, digitalisierter Daten
- Enge Kopplung zwischen Merkmal und Person schafft zusätzliche Probleme
  - Bedrohung der informationellen Selbstbestimmung
  - Gefahren durch gewaltsame Angriffe gegen Personen
  - Problem der öffentlichen Daten und rechtliche Aspekte
- Fazit und Einsatzbereiche
  - Aktuell nicht geeignet als ausschließliches Authentifizierungskriterium
  - Idealer Einsatz als ein Faktor einer Mehrfaktor-Authentifizierung
  - Weiterentwicklung der Verfahren wird in der Zukunft weitere Szenarien ermöglichen

# Authentifizierung durch Wissen: Passwörter

- Allgemeiner Ablauf der passwortbasierten Zugangskontrolle
  1. Es wird gleichzeitig oder nacheinander ein Benutzername und ein Passwort an einer Eingabemaske gefordert
  2. Die eingegebenen Daten werden zur Überprüfung mit gespeicherten Daten abgeglichen
  3. Der Zugang wird gewährt oder verweigert
- Statische Passworte oder Einmal-Passworte (z.B. S/Key RFC 1760) möglich
- Aktuell häufige Einsatzbereiche:

  Anmeldung an Betriebssystemen oder Webdiensten
- Typisches Protokoll: Password-Authentication-Protocol (PAP) RFC 1334:
  - Überträgt Passworte unverschlüsselt
  - Wurde sehr lange zur Einwahl via Modems verwendet

# Authentifizierung durch Wissen: Passwörter

- **Empfehlungen:**
  - einfach zu merken aber schwer zu erraten d.h. Länge mindestens 12 Zeichen ohne im Wörterbuch vorhandene Teile
  - Das überprüfende System sollte das Passwort nicht im Klartext gespeichert haben
  - Das überprüfende System sollte nur eine begrenzte Anzahl von Eingabeversuchen ohne Verzögerung erlauben
  - Jedes Passwort sollte nur für einen Dienst verwendet werden (Im Fall von Buffer-Overflow im Gehirn: Passwort-Manager oder dynmaische Passwort-Generatoren, keine Zettel)
- **Anmerkungen:**
  - Statische Passwörter können gestohlen werden d.h. per se unsicher
  - In sicheren Systemen sollte das Passwort nur eine Komponente sein

# Protokolle: Challenge Response Verfahren

- **Prinzip:**
  - Subjekt und überprüfende Instanz haben eine Benutzer-ID und ein gemeinsames Geheimnis $K_{ID}$ vereinbart
  - die Instanz stellt dem Subjekt eine Aufgabe (Challenge), welche dieses nur mit Hilfe von $K_{ID}$ lösen kann
  - die Instanz überprüft die Identität des Subjekt anhand des vom Subjekt erhaltenen Lösung
- **Vorteile:**
  - $K_{ID}$ muss nicht zwischen Subjekt und Instanz übertragen werden
  - Authentifizierung über Netzwerke kann durch den Einsatz von Zufallszahlen (leicht) Replay-sicher gemacht werden
  - Eignet sich für alle Klassen, welche auf einem vereinbarten Geheimnis beruhen

# Protokolle: Challenge Response Verfahren

## Beispiel: CHAP (RFC 1994)

Sei $ID$ das Identifikationsattribut des Subjekts (z.B. Loginname), $K_{ID}$ der geheime Schlüssel (Passwort) des Subjekts und $H$ eine kryptographische Hashfunktion:

| Subjekt | Übertragung | Instanz |
|---|---|---|
| | $\xrightarrow{\quad ID \quad}$ | |
| | $\xleftarrow{\quad RAND \quad}$ | generiert die Zufallszahl $RAND$ |
| berechnet $R = H(K_{ID}, RAND)$ | $\xrightarrow{\quad R \quad}$ | vergleicht $R$ mit eigener Berechnung |

## Anmerkungen:

- Raum der möglichen Challenges muss sehr groß sein
- Man-in-the-Middle-Angriffe möglich (wenn der Client PAP unterstützt)
- Einige weitere Angriffe möglich, d.h. gilt heute nicht mehr als besonders sicher (auch für erweiterte Varianten MS-CHAPv1 und MS-CHAP-v2)

# Protokolle: Kryptographische gesicherte Authentifizierung

Besser als Challenge Response Verfahren sind Protokolle, welche „gute" Verschlüsselung zur Authentifizierung benutzen.

**Needham-Schroeder Protokoll** (symmetrische Variante)

- Komponenten:
  - Authentifizierungsserver $AS$, Kommunikationspartner $A$ und $B$
  - $K_A$, $K_B$: geheime Schlüssel zwischen $AS$ und $A$, bzw. $AS$ und $B$
  - Nonce $I_A$ bzw. $I_B$
  - symmetrischer Sitzungsschlüssel $S_K$

Authenfizierungsserver

A

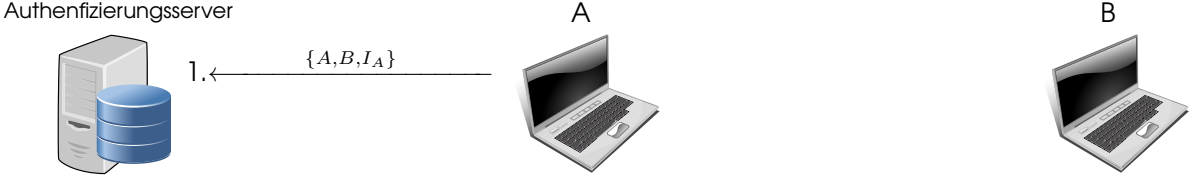
B

# Protokolle: Kryptographische gesicherte Authentifizierung

Besser als Challenge Response Verfahren sind Protokolle, welche „gute" Verschlüsselung zur Authentifizierung benutzen.

**Needham-Schroeder Protokoll** (symmetrische Variante)

- Komponenten:
  - Authentifizierungsserver $AS$, Kommunikationspartner $A$ und $B$
  - $K_A$, $K_B$: geheime Schlüssel zwischen $AS$ und $A$, bzw. $AS$ und $B$
  - Nonce $I_A$ bzw. $I_B$
  - symmetrischer Sitzungsschlüssel $S_K$

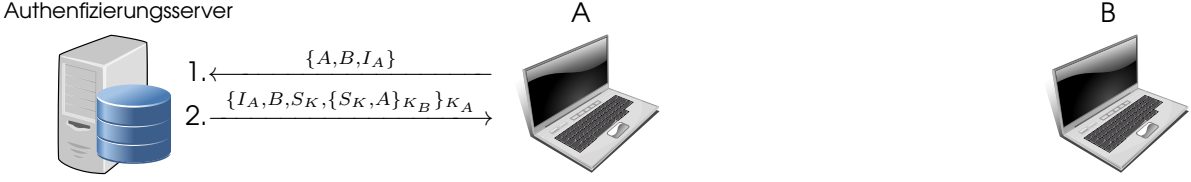


# Protokolle: Kryptographische gesicherte Authentifizierung

Besser als Challenge Response Verfahren sind Protokolle, welche „gute" Verschlüsselung zur Authentifizierung benutzen.

**Needham-Schroeder Protokoll** (symmetrische Variante)

- Komponenten:
  - Authentifizierungsserver $AS$, Kommunikationspartner $A$ und $B$
  - $K_A$, $K_B$: geheime Schlüssel zwischen $AS$ und $A$, bzw. $AS$ und $B$
  - Nonce $I_A$ bzw. $I_B$
  - symmetrischer Sitzungsschlüssel $S_K$

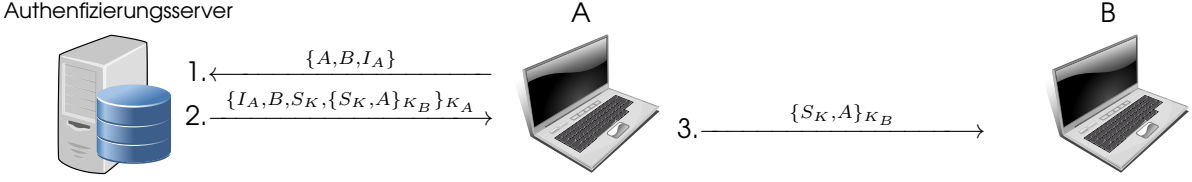


# Protokolle: Kryptographische gesicherte Authentifizierung

Besser als Challenge Response Verfahren sind Protokolle, welche „gute" Verschlüsselung zur Authentifizierung benutzen.

**Needham-Schroeder Protokoll** (symmetrische Variante)

- Komponenten:
  - Authentifizierungsserver $AS$, Kommunikationspartner $A$ und $B$
  - $K_A$, $K_B$: geheime Schlüssel zwischen $AS$ und $A$, bzw. $AS$ und $B$
  - Nonce $I_A$ bzw. $I_B$
  - symmetrischer Sitzungsschlüssel $S_K$

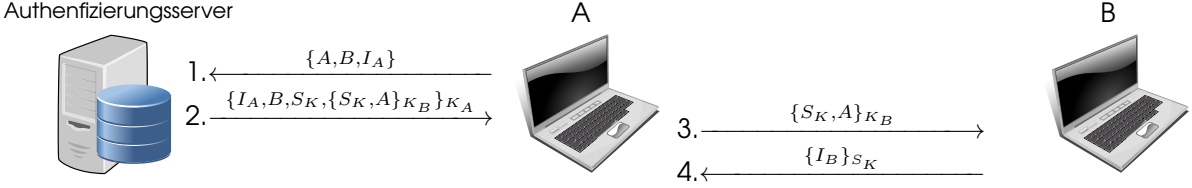


# Protokolle: Kryptographische gesicherte Authentifizierung

Besser als Challenge Response Verfahren sind Protokolle, welche „gute" Verschlüsselung zur Authentifizierung benutzen.

**Needham-Schroeder Protokoll** (symmetrische Variante)

- Komponenten:
  - Authentifizierungsserver $AS$, Kommunikationspartner $A$ und $B$
  - $K_A$, $K_B$: geheime Schlüssel zwischen $AS$ und $A$, bzw. $AS$ und $B$
  - Nonce $I_A$ bzw. $I_B$
  - symmetrischer Sitzungsschlüssel $S_K$

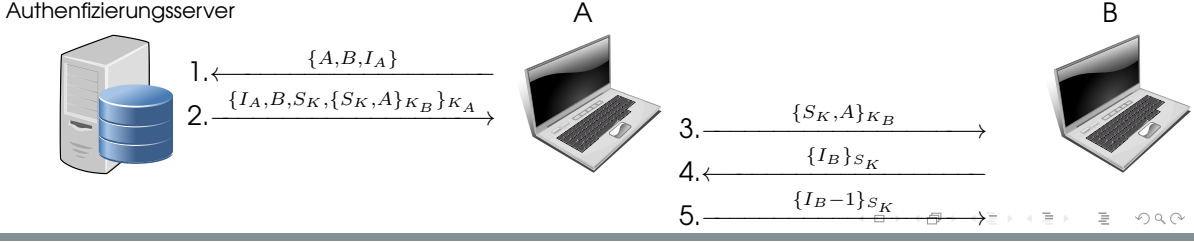


# Protokolle: Kryptographische gesicherte Authentifizierung

Besser als Challenge Response Verfahren sind Protokolle, welche „gute" Verschlüsselung zur Authentifizierung benutzen.

**Needham-Schroeder Protokoll** (symmetrische Variante)

- Komponenten:
  - Authentifizierungsserver $AS$, Kommunikationspartner $A$ und $B$
  - $K_A$, $K_B$: geheime Schlüssel zwischen $AS$ und $A$, bzw. $AS$ und $B$
  - Nonce $I_A$ bzw. $I_B$
  - symmetrischer Sitzungsschlüssel $S_K$



# Protokolle: Kryptographische gesicherte Authentifizierung

**Vorteile:**

- Sicherheit des Verfahrens kann beim Einsatz guter Verschlüsselungsverfahren auf die Sicherheit der beteilgten Systeme reduziert werden
- Zentraler Authentifizierungsserver ermöglicht einfachen Betrieb
- Verfahren zu Single-Sign-On erweiterbar

**Nachteile** (aller bisherigen Verfahren:)

- Die authentifizierende Instanz muss das Passwort zu mindestens einem Zeitpunkt währen des Prozesses besitzen

# Protokolle: Kryptographische gesicherte Authentifizierung

**Vorteile:**

- Sicherheit des Verfahrens kann beim Einsatz guter Verschlüsselungsverfahren auf die Sicherheit der beteilgten Systeme reduziert werden
- Zentraler Authentifizierungsserver ermöglicht einfachen Betrieb
- Verfahren zu Single-Sign-On erweiterbar

**Nachteile** (aller bisherigen Verfahren:)

- Die authentifizierende Instanz muss das Passwort zu mindestens einem Zeitpunkt währen des Prozesses besitzen

**Fragestellung: Geht das überhaupt anders???**

# Zero-Knowledge-Verfahren

**Ziel:** Nachweis der Kenntnis eines Geheimnisses gegenüber einem Dritten (hier Victor),

- ohne dass Victor das Geheimnis kennt und
- ohne dass Victor im Verlauf der Authentisierung Kenntnis über das Geheimnis erlangt
- Angreifer darf beliebig viele Nachrichten belauschen

# Zero-Knowledge-Verfahren

**Ziel:** Nachweis der Kenntnis eines Geheimnisses gegenüber einem Dritten (hier Victor),

- ohne dass Victor das Geheimnis kennt und
- ohne dass Victor im Verlauf der Authentisierung Kenntnis über das Geheimnis erlangt
- Angreifer darf beliebig viele Nachrichten belauschen

**Lösung:** **Feige-Fiat-Shamir-Verfahren** (1988): eines der ersten ZK-Verfahren

- Sicherheit beruht auf der Schwierigkeit, Quadratwurzeln in $Z_n^*$ zu berechnen:
- Geg.: $n = p \cdot q, x = r^2 \bmod n$, Ges.: $r$
- Einfach, falls Primfaktoren $p, q$ bekannt, sonst schwierig

# Feige-Fiat-Shamir-Verfahren

**Vorbereitung:**

- Wähle zwei Primzahlen $p$ und $q$
- Veröffentliche $N = pq$
- Wähle Geheimzahlen $s_1 ... s_k$ mit $ggT(s_i, N) = 1$
- berechne $v_i = s_i^2 \bmod N$ und gib diese an Victor weiter

**Authentifizierung:**

1. Peggy wählt zufällig eine Zahl $r$ und ein Vorzeichen $s \in \{-1, 1\}$, berechnet $x = s \cdot r^2 \bmod N$ und schickt $x$ an Victor
2. Victor wählt zufällig $a_1, ..., a_k$ mit $a_i \in \{0, 1\}$ schickt diese an Peggy
3. Peggy berechnet $y = rs_1^{a_1} \cdot \cdots \cdot s_k^{a_k} \bmod N$ und schickt $y$ an Victor
4. Victor überprüft $y^2 \bmod N = \pm x v_1^{a_1} \cdot \cdot v_k^{a_k} \bmod N$

# Authentifizierung: Zusammenfassung

- Feststellung der Identität von Benutzern, Rechnern oder Diensten ist eine zentrale Herausforderung der Informationssicherheit, welche sämtliche Schutzziele betrifft
- Einfaktorauthentifizierung mit statischen Passworten sind zwar aktuell der Standard, müssen aber als unsicher gelten
- Biometrie als zusätzlicher Faktor ist sinnvoll und reif für den Einsatz, als ausschließliches Kriterium aber nicht ausreichend

# Authentifizierung: Zusammenfassung

- Feststellung der Identität von Benutzern, Rechnern oder Diensten ist eine zentrale Herausforderung der Informationssicherheit, welche sämtliche Schutzziele betrifft
- Einfaktorauthentifizierung mit statischen Passworten sind zwar aktuell der Standard, müssen aber als unsicher gelten
- Biometrie als zusätzlicher Faktor ist sinnvoll und reif für den Einsatz, als ausschließliches Kriterium aber nicht ausreichend
- sinnvolller Umgang mit Authentifizierung muss ein Konzept Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Dienste an Systemnutzern einhergehen (**Autorisierung**)

# Danke für Ihr Interesse

Fortsetzung folgt