Leibniz Universität Hannover

Grundlagen der IT-Sicherheit
VL 5: Authentifizierung

Prof. Dr. Markus Dürmuth, Wintersemester 2023/24

Unsere heutigen Themen…

- Motivation
- Passwort-basierte Authentifizierung
- Graphische Passwortverfahren
- Biometrie
- Token-basierte Authentifizierung

NUTZERAUTHENTIFIZIERUNG

Authentifizierung

- *authentikos* (Griechisch: echt/ehrlich)
- *facere* (Latein: machen).

→ Bestätigung der Identität oder des Ursprungs von Gütern/Daten/Menschen

Nutzerauthentifizierung

Authenticate: To establish the validity of a claimed identity.

[Orange book]

Entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired).

[Menezes et al.]

Authentifizierung vs. Autorisierung vs. Identifizierung

Authentifizierung (Authentication):
Verifiziere, dass du bist, wer du angibst zu sein.

Autorisierung (Authorization):
Verifiziere, dass du berechtigt bist das zu tun, was du versuchst zu tun

```
-rwxr-xr-x
```

Zugriffskontrolle (Access control):
Beschränkung des Zugangs zu einem Ort oder einer Ressource, z. B. durch Authentifizierung und Autorisierung

Identifikation (Identification):
Bestimmung der Identität eines Individuums

Konzeptuell unterschiedliche Formen der Authentifizierung

- Wissen
  - (Selbst gewählte) Passwörter (uncued recall)
  - “Cultural passwords” (Wissensfragen) (cued recall)
  - Zugewiesene Passwörter
- Biometrie
  - Verhaltensbiometrie
  - Physiologische Eigenschaften
- Besitz
  - (Sicherheits-) Token

PASSWORTBASIERTE AUTHENTIFIZIERUNG

Passwörter in IT-Systemen

- Authentifizierung und besonders Passwörter gehen (mindestens) bis zum römischen Militär zurück (watchword)
- Militär benutzt häufig Passwort-Antwort für “gegenseitige” Authentifizierung.


IBM 7090

- Beim MIT für das CTSS (Compatible Time Sharing System), das 1961 – 1973 auf IBM 7094 Hardware lief

- Bei IBM für das Sabre reservation system (Sabre Corp. founded in 1960), (American Airlines, Expedia, American Express,…)

Passwort-Themen

Password Snooping

- Belauschen von Passwörtern in (unverschlüsseltem) Netzwerkverkehr
- Passwort vom Besitzer erlangen (z.B. über Malware)
- Shoulder Surfing Angriffe

Password guessing (online) und Password cracking (offline)

- Wörterbuch-Angriffe
- Brute-Force Angriffe

Menschliche Schwachstelle

- Menschen wählen schlechte Passwörter und verwenden Passwörter mehrfach

PASSWORTBASIERTE AUTHENTIFIZIERUNG: SICHERER UMGANG MIT PASSWÖRTERN

Passwörter

Alice

Server

Enroll:

Choose password *pwd*

(A, pwd_A) →

Store (A, pwd_A)

Authenticate:

Send password

(A, pwd') →

Retrieve (A, pwd_A)

$pwd' =? pwd_A$

Probleme? Passwort wird als Klartext übermittelt

Passwörter
(über verschlüsselte Kanäle)

Alice

Server (pk_S)

Enroll:

Choose password *pwd*

$$E((A, pwd_A), pk_S) \longrightarrow$$

Store (A, pwd_A)

Authenticate:

Send password

$$E((A, pwd'), pk_S) \longrightarrow$$

Retrieve (A, pwd_A)

$pwd' =? pwd_A$

Probleme? Passwort wird als Klartext auf dem Server gespeichert

Passwörter (+ Hashing)

Alice

Server (pk_S)

Enroll:

Choose password *pwd*

$E(\,(A, pwd_A),\, pk_S\,)$ →

Compute $h_A = H(pwd_A)$
Store (A, h_A)

Authenticate:

Send password

$E(\,(A, pwd'),\, pk_S\,)$ →

Retrieve (A, h_A)
Compute $h' = H(pwd')$
$h' =? h_A$

Probleme? Dasselbe Passwort resultiert in demselben Hash

Passwörter
(+ Hashing + Salt)

Alice

Server (pk_S)

Enroll:
Choose password *pwd*

$$E(\,(A, pwd_A),\, pk_S\,) \longrightarrow$$

Choose random $s_A \in \{0,1\}^{64}$
Compute $h_A = H(pwd_A, s_A)$
Store (A, s_A, h_A)

Authenticate:
Send password

$$E(\,(A, pwd'),\, pk_S\,) \longrightarrow$$

Retrieve (A, s_A, h_A)
Compute $h' = H(pwd', s_A)$
$h' =? h_A$

Probleme? Gezieltes Offline-Raten,
Phishing, Wiederverwendung, ...

Sicherer Umgang mit Passwörtern

- Offline-Raten ist wenig effizient, aber möglich
- Kryptographische Hashfunktionen sind (per Design) schnell zu evaluieren
- Das ist kontraproduktiv für Passwort-Hashing: Angreifende sollten verlangsamt werden
- Problem: Das würde (fast zwangsläufig) auch den legitimieren Server verlangsamen

Geschwindigkeit oclHashCat

Performance

- PC1: Windows 7, 64 bit • Catalyst 13.1 • 1x AMD hd7970 • stock core clock
- PC2: Windows 7, 64 bit • ForceWare 310.90 • 1x NVidia gtx570 • 1600Mhz clock
- PC3: Ubuntu 12.04.1, 64 bit • Catalyst 13.1 • 1x AMD hd6990 • stock core clock
- PC4: Ubuntu 12.04.2, 64 bit • ForceWare 310.32 • 1x NVidia gtx560Ti • stock core clock

Hash Type	PC1	PC2	PC3	PC4
NTLM	7501M c/s	2137M c/s	9096M c/s	1641M c/s
MD5	5470M c/s	1619M c/s	6956M c/s	1345M c/s
SHA1	2136M c/s	629M c/s	3081M c/s	433M c/s
SHA256	1012M c/s	272M c/s	1101M c/s	170M c/s
SHA512	76M c/s	86M c/s	152M c/s	62M c/s
LM	1245M c/s	346M c/s	992M c/s	236M c/s
phpass P	2167k c/s	661k c/s	3087k c/s	538k c/s
descrypt	65594k c/s	29029k c/s	78941k c/s	18636k c/s
md5crypt 1	3592k c/s	963k c/s	5033k c/s	872k c/s
bcrypt $2a$	4080 c/s	680 c/s	3877 c/s	604 c/s
sha512crypt 6	12584 c/s	9932 c/s	18536 c/s	6545 c/s
Password Safe (SHA-256)	501k c/s	k c/s	608k c/s	k c/s
IKE-PSK (MD5)	296M c/s	93M c/s	324M c/s	78M c/s
Oracle (DES)	365M c/s	110M c/s	167M c/s	70M c/s
DCC (MD4)	3647M c/s	941M c/s	5194M c/s	798M c/s

Passwort-Hashing verlangsamen

Iterative Konstruktion:

- Evaluation eines Passwort-Hashes verlangsamen durch die Iteration über eine „normale“ kryptographische Hashfunktion, z.B.

  $H(pwd) = SHA1^{1000}(pwd)$

„Secret Salt“

- Alternativ können wir einen (kurzen) Salt verwenden, diesen aber nicht speichern

Keyed Hash Function

- Verwendung eines geheimen Schlüssels, um Passwörter zu hashen

  $H(pwd, k)$

- Speichere Schlüssel *k* an einem „sicheren Ort“ : Separate DB, fest codiert in Quellcode oder in Hardware (HSM)

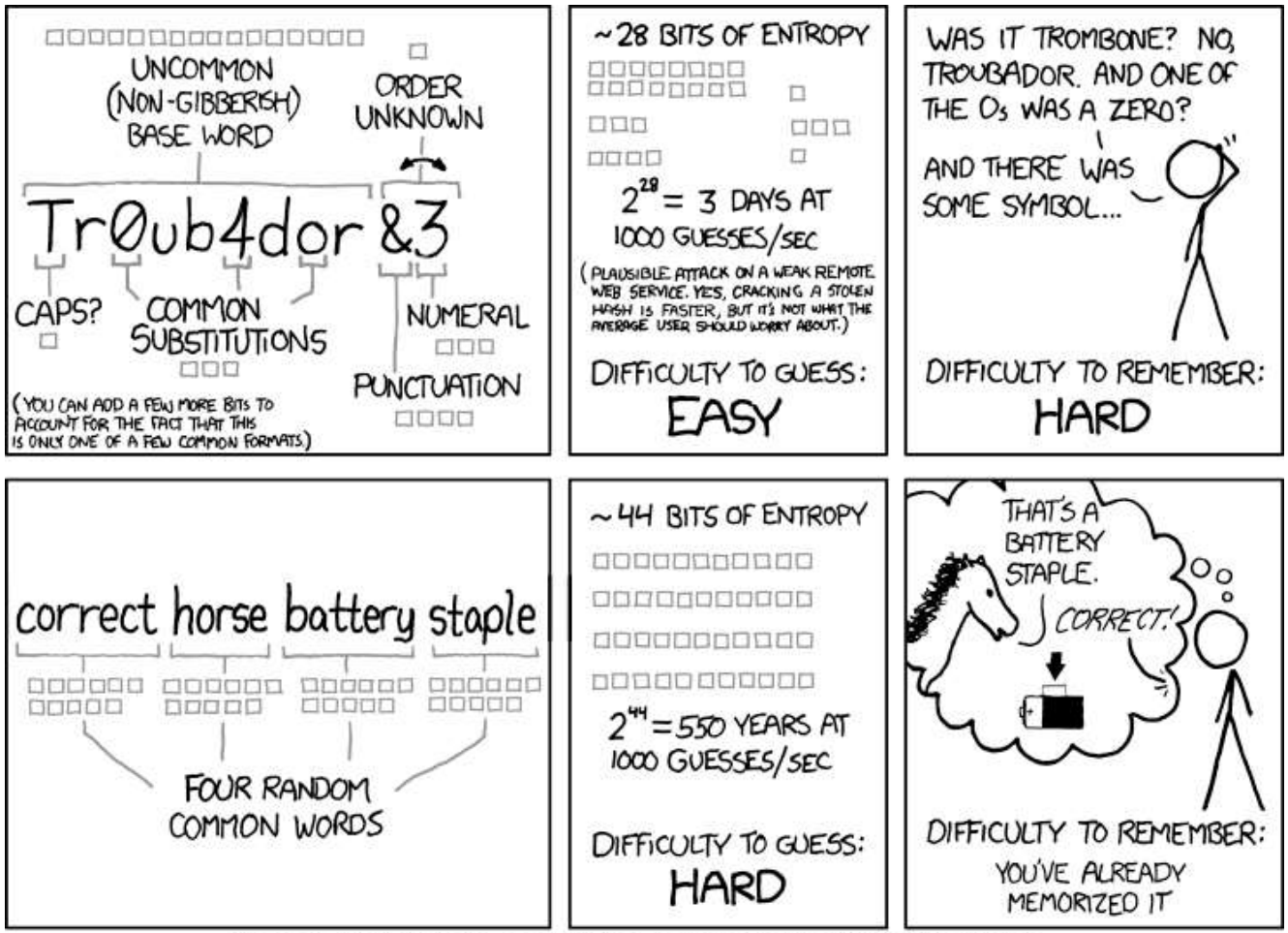
Multi-Faktor Authentifizierung

Authentifizierung kombiniert multiple Faktoren

- Beispiel: Zwei-Faktor

Sichere Passwörter

Eine ungelöste Aufgabe



GRAPHISCHE PASSWÖRTER

Was ist einfacher zu merken?

Leibniz Universität Hannover

`oqD7@3hj`

(In der Regel:) Graphische Information!
(-> Dual coding theory…)

Drei grundlegende Designs

1. Recall-basierte graphische Passwörter
   - Reproduziere gelerntes Wissen
   - Z.B. Text-Passwörter

2. Cued recall-basierte Passwörter
   - Reproduziere gelerntes Wissen mit einem Hinweis (cue)

3. Recognition-basierte Passswörter
   - Wiedererkennen von bereits gesehener (gelernter) Information, z.B. durch Unterscheiden von “neuer” Informationen

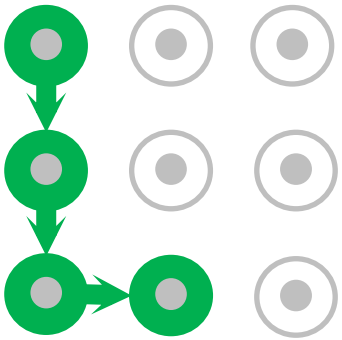
Recall-based: Pass-Go

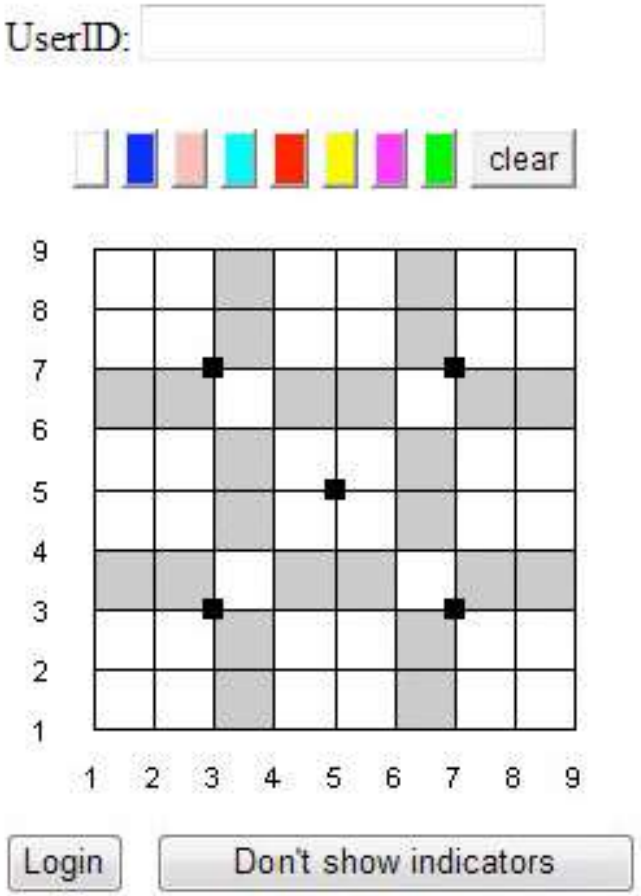
Pass-Go:

- Linien richten sich am Raster aus
- Dadurch recht feines Raster möglich
- Mehrere Linien möglich, Farben, …

Das sieht bekannt aus…

- Vorläufer des Android Verfahrens





[Tao et al. 2008, Biddle et al. 2012]

Cued-recall based Windows 8 Picture Passwords

- Punkte, Linien, Kreise

http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx

Recognition-based: PassFaces

- Identify known images/faces/…

- Iterate several time, or select several known faces
- Bias when user-chosen faces

BIOMETRISCHE AUTHENTIFIZIERUNG

Einführung

- *biometry:* Griechisch *bios* (Leben) und *metron* (Maß), d.h. “das Leben messen”
- In der Authentifizierung: etwas, das du bist

- Einige Beispiele:
  - Fingerabdruckerkennung,
  - Gesichtserkennung,
  - Iris-Erkennung,
  - Stimmerkennung,
  - Tastenanschlagdynamik,
  - Gangerkennung,
  - Handgeometrie,
  - ...

Zentrale Eigenschaften

Erwünschte Eigenschaften der Biometrie

- **Messbarkeit**: idealerweise Verwendung eines einfachen, schnellen und günstigen Prozesses
- **Einzigartigkeit**: es sollte (mit hoher Wahrscheinlichkeit) eine Person charakterisieren, beim Vorliegen von “typischen Fehlern”
- **Beständigkeit (im Laufe der Zeit):** Es sollte sich im Verlauf der Zeit nur wenig verändern
- **Universalität**: Jeder und jede (in der gewünschten Gruppe) sollte diese Eigenschaften aufweisen

Beispiele?

Erfüllen folgende Beispiele die Abforderungen?

- Körpergröße
- Körpergewicht
- Fingerabdruck
- Gesichtserkennung
- …

- **Messbarkeit**:
- **Einzigartigkeit**:
- **Beständigkeit (im Laufe der Zeit):**
- **Universalität**:

Zwei unterschiedliche Ziele

- **Identifizierung** (1-out-of-N): Gegeben Sei eine Probe. Finde das Passende aus einer großen Datenbank (Galerie)
  - Eine Person mittels Fingerabdruck wiederfinden
  - Eine Person in einer großen Menschenmenge identifizieren

- **Authentifizierung/Verifizierung**(1-out-of-1): Eine angebliche Identität verwenden und die Probe mit einem einzelnen Bild der Galerie vergleichen.

- Hier: Primär Authentifizierung

Vor- und Nachteile biometrischer Authentifizierung

Viele biometrische Verfahren teilen sich die gleichen/ähnliche Vor- und Nachteile:

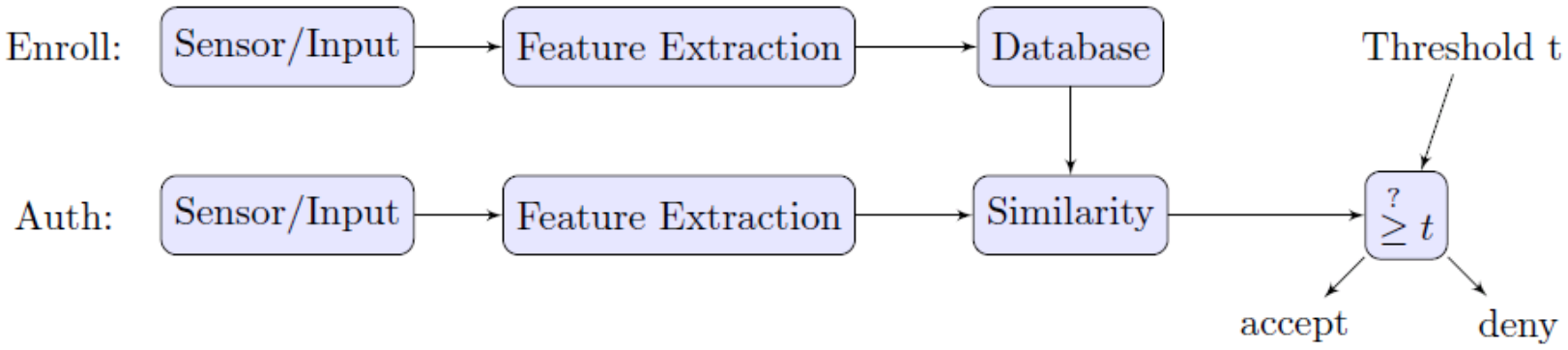
Vorteile:

- Man muss nichts auswendig lernen oder mitbringen
- Üblicherweise relative schnell
- Verlässt sich nicht darauf, dass die Nutzenden starke Geheimnisse wählen

Nachteile:

- Die meisten biometrischen Eigenschaften sind nicht geheim
- Biometrische Muster werden in verschiedenen Konten wiederverwendet.
- (Meist) Bedarf an zusätzlicher Hardware
- Kein Widerruf der Authentifizierungsdaten

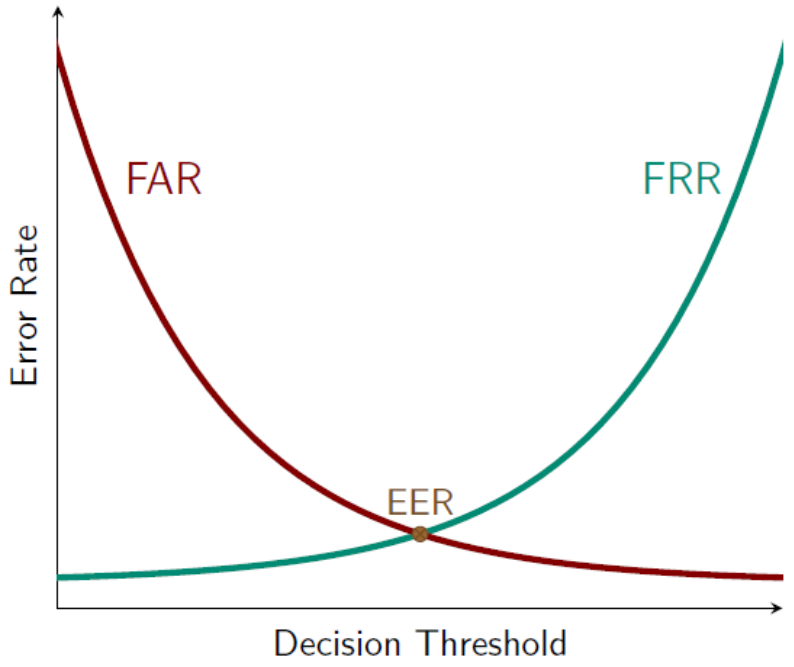
Overall structure



- Most biometric schemes have a common structure
- Of central importance is the parameter *t*

Gesamtperformance

- **False Acceptance Rate (FAR)**: Percentage of illegitimate samples that are falsely accepted
- **False Reject Rate (FRR)**: Percentage of legitimate samples that are falsely rejected
- **Equal error rate (EER)**: Error rate when FAR=FRR



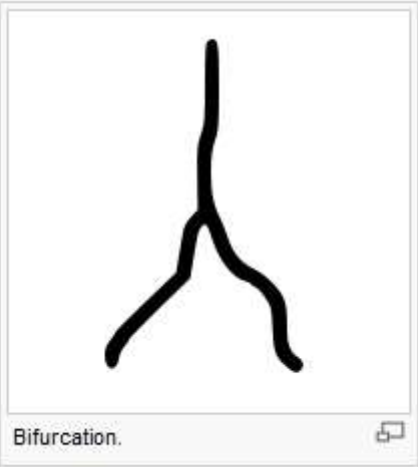
BEISPIEL: FINGERABDRUCK-ERKENNUNG

Fingerabdruck: Level 2 Details

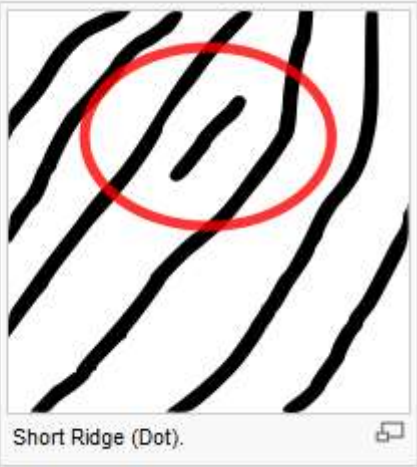
- Level 2 Eigenschaften: Details in der Rillenstruktur (ridge structure), insbesondere **Minutien**

Minutien

Ridge ending.



Bifurcation.



Short Ridge (Dot).

Fingerabdruck: Level 3 Details

- Merkmale der Stufe 3: basierend auf der genauen Form der Rillen, z. B. der Porenstruktur.
- Erfordert eine sehr hohe Auflösung des Eingabegeräts.

FTIR

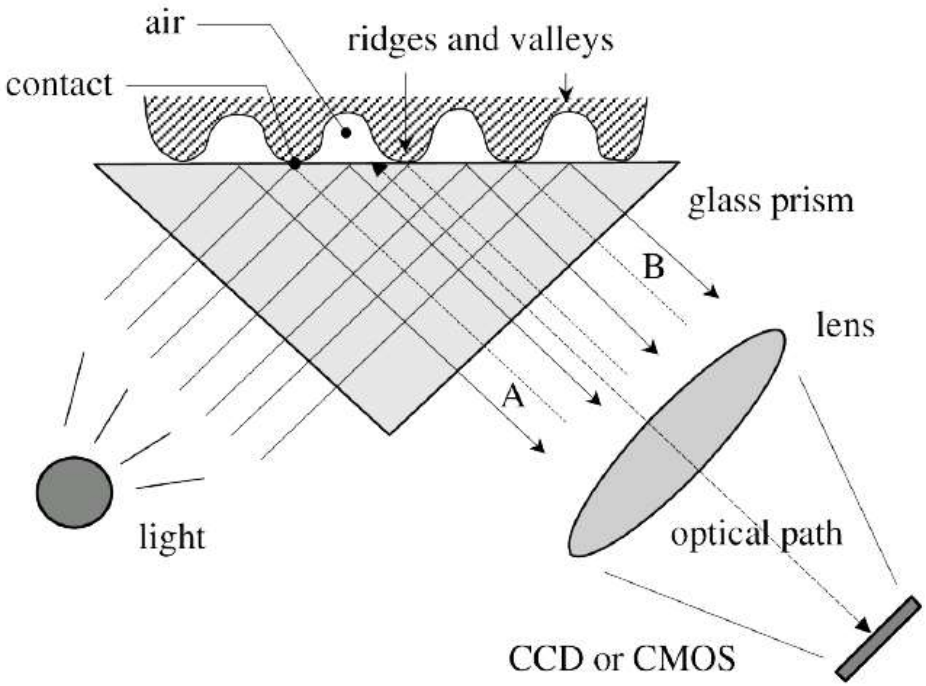
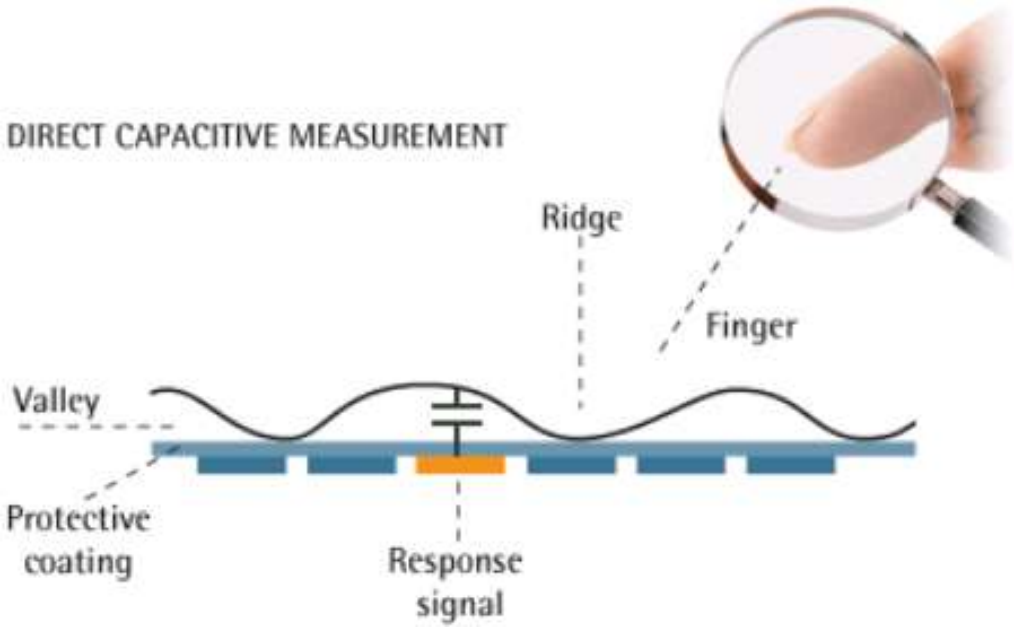


Figure 9.1: Principle of an optical fingerprint reader based on frustrated total internal reflection (FTIR). Image by Davide Maltoni, University of Bologna, 2003.

Capacitive


DIRECT CAPACITIVE MEASUREMENT
Ridge
Finger
Valley
Protective coating
Response signal

Lifeness detection

- Erkennung der Verwendung von gefälschten biometrischen Daten
- D.h. erkennen, ob die vorgelegten biometrischen Daten "lebendig" sind

Fake-Fingerabdrücke

WINDOWS HELLO

Notebooks lassen sich mit A4-Gesichtsausdruck entsperren

Ein Foto aus dem Laserdrucker reicht, um Windows-Hello-Geräte zu entsperren. Tester der Syss GmbH konnten das bei einem Dell-Notebook und dem Surface Pro 4 bestätigen. Sicher sind nur aktuelle Geräte mit aktiviertem Anti-Spoofing.

Die Gesichtserkennung von Windows Hello scheint in einigen Fällen nicht sicher zu sein. Zwei Mitarbeiter der auf IT-Sicherheit spezialisierten Syss GmbH konnten ein Surface Pro 4 mit einem auf ein A4-Blatt ausgedruckten Selbstbild entsperren. Dieser Trick scheint auch bei zumindest einem anderen Windows-Gerät zu funktionieren: dem Notebook Dell Latitude E7470 mit externer Kamera. Syss konnte das für mehrere Versionen von Windows 10 Testen, darunter das Creators Update 1703 und das Fall Creators Update 1709.

golem.de

Lifeness detection: Gesichtserkennung

- Textur
- Augenbewegung
- Blinzeln
- 3D-Informationen (Neufokussierung, echtes 3D,...)
- Bewegung der Lippen

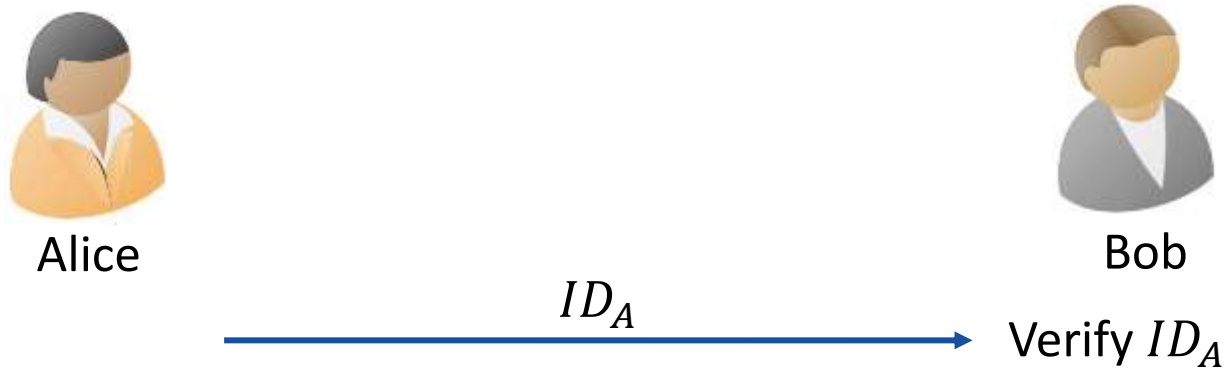
AUTHENTIFIZIERUNG MIT TOKEN

Tokens

- Authentifizierung über
  „etwas, das du hast“
- Viele verschiedene Formen

Figure 1: Hardware Tokens

Wie es nicht sein sollte



Unsicher:

- Replay
- Erraten von ID_A
- …

Challenge response protocols

Alice

Bob

challenge

Choose Challenge

Compute response(challenge)

response

Verify response

- Challenge kann von unterschiedlicher Natur sein

Tokens

- Winzige Rechengeräte
- Führen kryptographische Operationen durch um zu garantieren, dass sie die Gegenstelle sind
- Beinhalten einen kryptographischen Schlüssel
  - Geteilter symmetrischer Schlüssel oder
  - Geheimer asymmetrischer Schlüssel

Protokolle zur Authentifizierung

- Eine Reihe von Protokollen, die in ISO/IEC 9798-3 definiert sind

- Basiert auf asymmetrischer Kryptographie
- Voraussetzung: Vorab geteilte geheime Schlüssel sk_A

Unilaterale Authentifizierung in einem Durchgang

Alice

Bob

Zeitstempel T_A

$$s := sig\ \ ((T_A, B), skA)$$

Verify signature s
Check Timestamp T_A
Check Identity B

In der Nachricht (payload)

- Zeitstempel T_A stellt sicher, dass die Nachricht „frisch“ ist
- B’s Identität
- A’s Identität impliziert durch die Verwendung von sk_A.
- Zeitstempel T_A kann duch Zähler C_A erstetzt werden

Unilaterale Authentifizierung in zwei Durchgängen

Alice

Bob

n_B

Nonce $N_A \leftarrow^R \{0,1\}^{128}$

Choose nonce $N_B \leftarrow^R \{0,1\}^{128}$

$s := sig\,((N_A, N_B, B), skA)$

verify signature s
Check nonce N_B
Check identity B

In der Nachricht (payload)

- Zeitstempel durch Nonce ersetzt
- Benötigt zusätzliche Nachricht (und bidirektionalen Kommunikationskanal)
- Besonderheit: N_A verhindert Angriffe mit Alice als Signatur-Orakel

Diskussion:

- Primitive
  - Asymmetrische Kryptographie
  - Symmetrische Kryptographie
  - Hash Funktionen
- Challenge
  - Explicit Challenge (nonce)
  - Zeitstempel
  - Zähler
- Konnektivität
  - Kontakt
  - Kontaktlos
  - Disconnected

FRAGEN BIS HIERHER?

EVALUATION DER HEUTIGEN VORLESUNG

… oder über Stud.IP im Ordner der Vorlesung