Characteristics – Hand Geometry

- Based on a number of measurements taken from the human hand including
  - Shape, size of palm, lengths and widths of the fingers
- Commercial authentication systems based on hand geometry are available and highly used
- Advantage: simple, easy to use, inexpensive, not prone to environmental factors such as dry wheather
- Disadvantages
  - Hand geometry not very distinctive
    - Do not scale for systems requiring identification in large populations
  - Limitation of dexterity (e.g. from arthritis) cause problems
  - Physical size of the hand makes it inapplicable in certain applications e.g. laptop access

Characteristics – Palmprint

- Palms contain pattern of ridges and alleys much like fingerprints
- Area of palm much larger and more distinctive than fingerprints
- Palmprint scanners are bulkier than fingerprint scanners
- Using a high-resolution palmprint scanner would allow to use all features of the hand simultaneously
  - Hand geometry, palmprint, fingerprints, principle lines and wrinkles
  - Higher accuracy

Characteristics - Iris

- Annular region bounded by the pupil and the sclera
- Visual texture of the iris is formed during fetal development and stabilizes during the first two years of life
- Texture carries very distinctive information
  - Can be used for identification
  - Accuracy and speed very promising to support large-scale identification systems
- Irises of identical twins are different
- Requires considerable user participation
- Typically have low false accept rates compared to other biometric traits but rather high false reject rates

Characteristics Keystroke

- Hypothesized that each person types on a keyboard in a characteristic way
- Not expected to be unique to each individual
- Expected to be sufficiently discriminatory to permit authentication
- Behavioral biometrics, large intra-class variations expected due to
  - Changes in emotional state, position of user with respect to the keyboard, type of keyboard used etc.
- Acquiring could be done unobtrusively as person keys in information
- Permits “continuous authentication” during a session e.g. after a user logged on

Characteristics - Signature

- Way a person signs his name
- Requires contact and effort from the user
- Widely accepted in governmental, legal, commercial transactions
- Behavioral biometric that
  - Changes over a period of time
  - Is influenced by physical and emotional conditions
- High intra-class variations for some people
- Professional forgers are very good at reproducing signatures

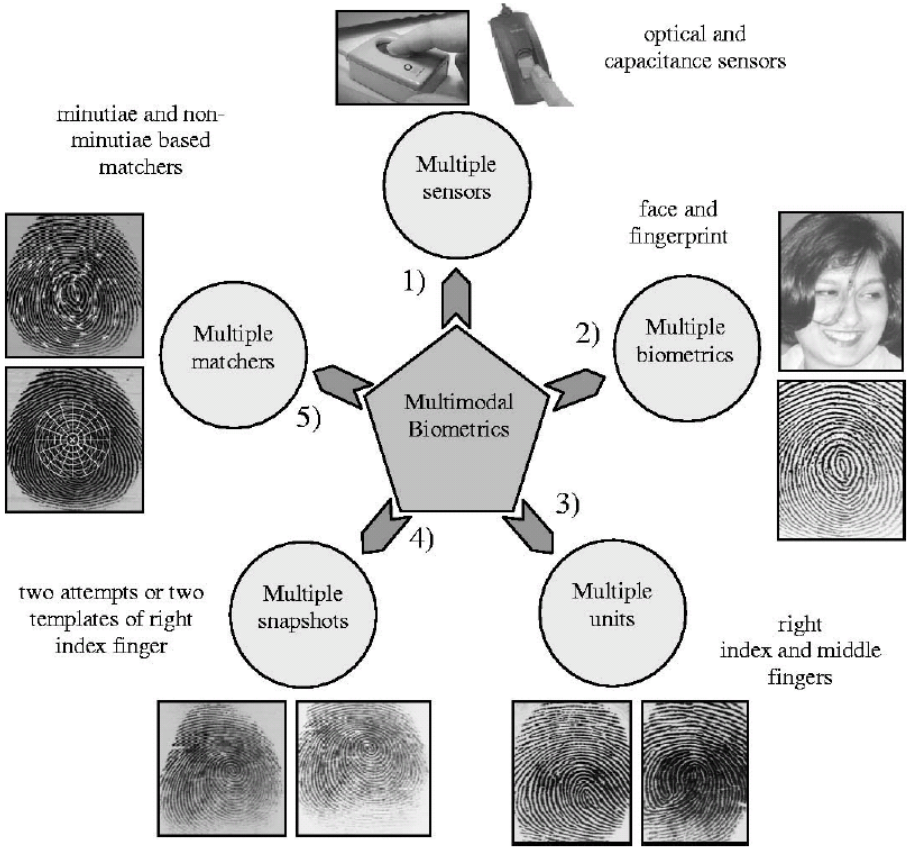
Characteristics - Voice

- Combination of physical and behavioral biometric
- Physical features based on shape and size of appendages
  - Vocal tracts, mouth, nasal cavities, lips
- Physical characteristics are invariant for each individual
- Behavioral aspects change over time due to
  - Age, medical conditions, emotional state
- Not very distinctive
  - Not usable for identification in large populations
- Sensitive to background noises
- Nevertheless sometimes the only usable biometrics
  - E.g. authentication over the phone

Characteristics - Gait

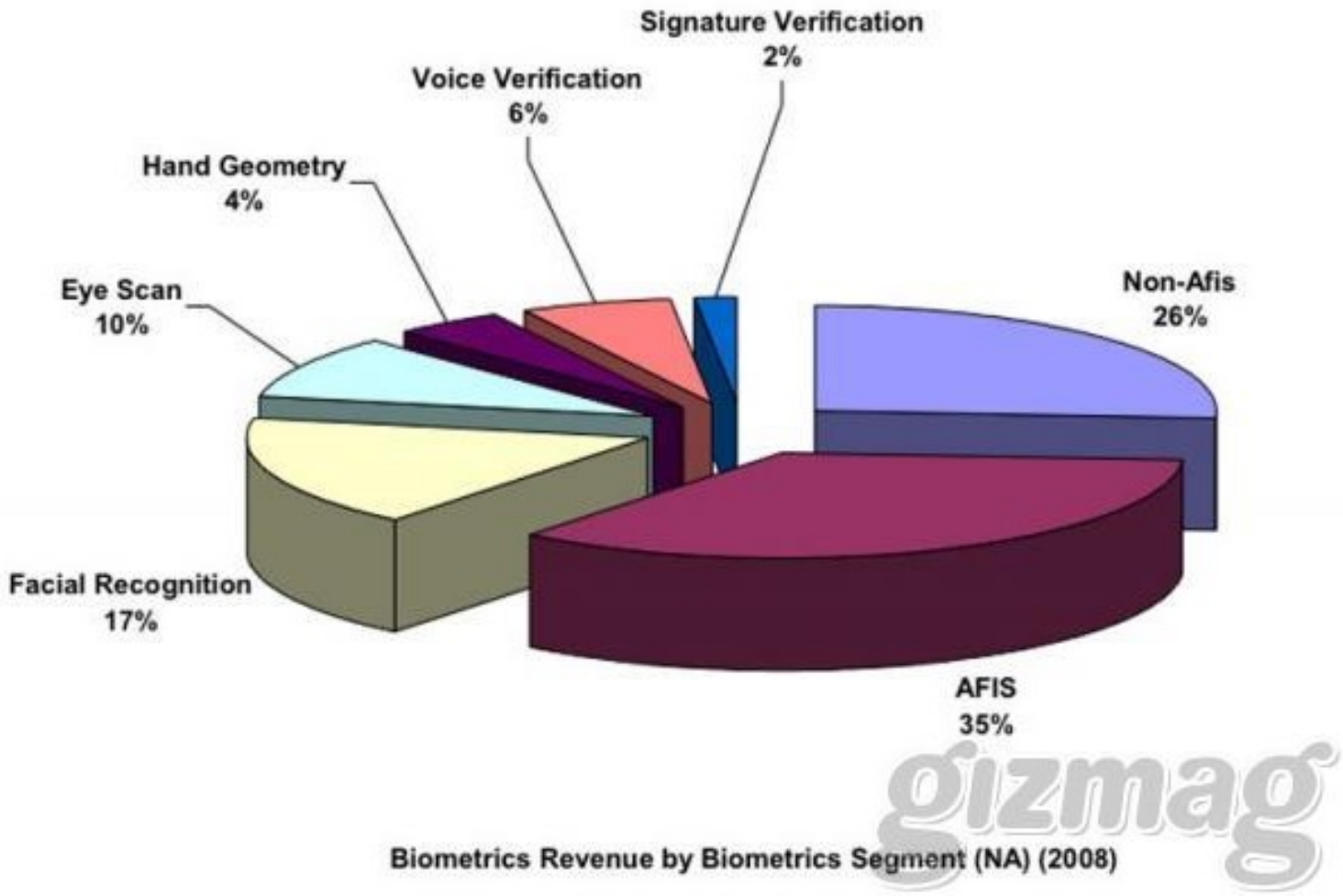
- Manner in which a person walks
- Can be used to recognize people at a distance
- Very appropriate for surveillance scenarios
  - Identity of an individual could be surreptitiously established
  - Tracking could be possible
- Algorithms attempt to extract human silhouette in order to derive spatio-temporal attributes
- Gait is affected by several factors including
  - Footwear, nature of clothing, affliction of legs, walking surface etc.

Multimodal Biometrics



- Increases matching performance, increases population coverage, deters spoofing (?)

Biometrics Market



- AFIS = Automated Fingerprint Identification Systems

Potential Vulnerabilities of Systems

- Circumvention
  - Attacker gains access to protected resources by a technical measure to subvert the system e.g. by replacing database templates, overriding matcher decisions,…
- Covert acquisition
  - Attacker uses biometric information captured from legitimate users, e.g. capture and playback of voice passwords, lifting latent fingerprints
- Collusion and coercion
  - Attacker collides or collaborates with legitimate user (willingly: collusion, unwillingly: coercion)
- Denial of Service
  - Attacker prevents legitimate use e.g. by enrolling many noisy samples -> decreases threshold, increases false acceptance rate
- Repudiation
  - Attacker / user may claim not to have accessed a protected resource by claiming that his data was stolen

Biometric Vulnerabilities Faced by Users

- Biometrics are not secret
  - Technology for taking facial images, fingerprints, scanning irises and recording voice is available to anyone – even without consent of the user
  - Biometrics cannot be used in the same way as passwords or security tokens
- Biometrics cannot be revoked
  - Biometrical features are permanently associated with an individual and cannot be revoked if they are misused
- Biometrics have secondary uses
  - If the same biometrical feature is used by different applications then the user can be tracked if the organizations share the data
- Biometric features can carry private information such as indicating genetic disease, use of medication, etc.
- Automatic identification and profiling constitutes a potential privacy threat

Attacks Against Biometric Systems (1)

- Attacks against data acquisition: spoofing
  - Attacker presents faked biometric sample to the sensor
  - Attacker's goal is either to
    - Avoid detection (identification) or
    - Masquerade as another individual
  - Avoiding detection is typically simpler
    - Change makeup, facial hair, wearing glasses, rotating the head etc.
- Attacks against sensors
  - Subvert or replace sensor hardware
- Segmentation
  - Escape surveillance by failing the system to detect the presence of the appropriate feature
    - E.g. cover one eye such that system that expects user's to have two eyes from detecting the presence of a human being

Attacks Against Biometric Systems (2)

- Replay attacks:
  - Attacker intercepts output flow of the sensor and puts previously intercepted genuine biometric information into the proper place in the processing chain
- Malware-based attacks:
  - E.g. attacker replaces original extractor or matcher with a fake one
- Attacks against feature extraction
  - If feature extraction algorithm is known to an attacker, attacker can try to construct special features that allow for impostor

Attacks Against Biometric Systems (3)

- Attacks against quality control
  - Attacker may e.g. try to pollute the template data base with lambs such that the threshold needs to go down and the false accept rate increases
- Data storage
  - Templates should be stored encrypted
  - Storage should be protected against inserting fake templates
  - Storage should be protected from unauthorized deletes
- Availability of templates in plaintext
  - Classical biometric systems require clear text access to templates
  - Differs from traditional computer security systems where passwords can be stored encrypted or hashed

Attack Motivations

- Attacker wants to disguise his identity




- Attacker wants to gain privileges of a legitimate user
- An attacker may want to benefit from sharing a biometric
  - E.g. attacker creates new identity using artificial biometric, enrolls in a system, shares the fake identity with multiple people
- Most dangerous attacks: spoofing attacks
  - Presenting faked biometrics to the sensors

Approaches to Spoof Detection

- Spoof detection - differentiating between a genuine biometric trait presented from the right live person versus some other source
- Approaches
  - Sensing vitality (liveness) signs such as pulse, sweat, temperature, etc
  - Acquiring several raw data samples
    - E.g. taking pictures of faces from several angles
  - Using challenge response techniques

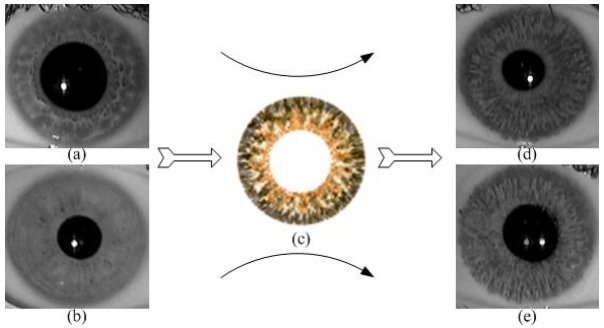
Example: Spoof Attacks - Fingerprints

- Spoofing Fingerprints
  - Artificial fingers from soft material such as gelatin
  - Ink jet finger prints on transparencies
  - Latent prints on sensors can sometimes be reactivated by directing light onto the platen
- Detecting Spoofs of Fingerprints
  - Measuring perspiration of the skin surface
  - Use skin absorbance and reflection profiles
  - Measure temperature (can even detect foil between attacker's finger and the scanner)
  - Measure pulse in the finger tip
- Detailed example for spoofing fingerprints at the end of this chapter

Example: Spoof Attacks - Irises

- Spoofing Iris images
  - High-quality photograph of the eye
  - Use contact lens on which an iris pattern is printed
  - 3D artificial irises
- Spoof detection
  - Measuring the involuntary motions of the pupil at rest
  - Measuring reaction to changing ambient light conditions
  - Challenge-response: ask person under test to blink or move eyes in a certain direction

- Without lens



- With lens

Example: Spoof Attacks - Face

- Spoof attacks against 2D systems
  - Often already fooled by simple photographs
  - Sometimes even by line drawings
- Protection against spoofing
  - Detection of small involuntary movements of the head
  - Detection of blinking
  - Can be fooled by video sequences
  - Challenge-response more promising
- Spoof attacks against 3D systems
  - Artificial 3D faces, masks
- Protection against spoofing
  - Challenge-response asking the user to blink, smile etc

Conclusion

- Spoofing attacks become more complex
- Much research work hypotheses how attacks can be performed
- Unclear whether systems are adequately protected against yet unknown fake biometrics
- Unclear how resilient anti-spoofing approaches are against attacks that differ from the anticipated ones
- Further research needed to measure the performance of anti-spoofing measurements

Faking Fingerprints

- The Chaos Computer Club published a small “how to” on faking fingerprint in October 2004
- The fingerprints produced with the method can supposedly be used to fool fingerprint scanners
- The pictures on the following slides are taken from the CCC’s web site
- We have NOT tested whether faking fingerprints this way works or not, however it sound convincing

Fingerprints: Fat and Sweat Residue

- Glasses, door knobs and glossy paper are good sources for fingerprints

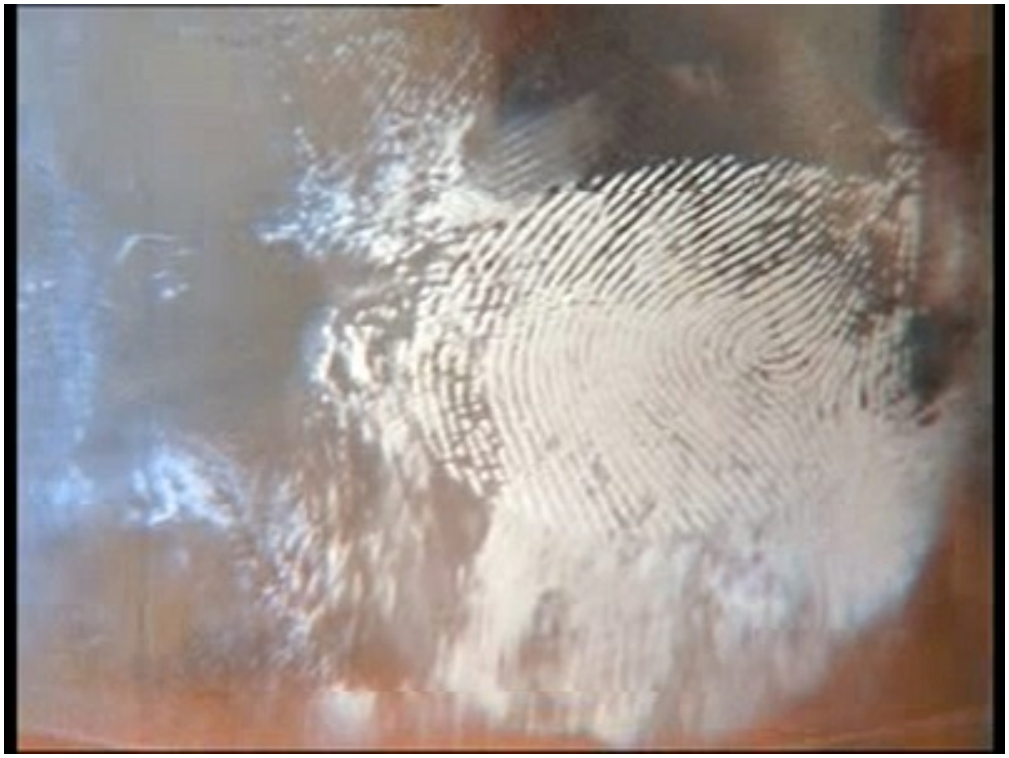
Making Fingerprints Visible

- Standard method in forensics: sprinkle with colored powder that sticks to the fat

Alternative for Making Fingerprints Visible

- Cyanoacrylat poured into a bottle cap which is turned upside down and placed over the fingerprint

Print after Cyancrylate Processing



- Cyanoacrylat gasses out and reacts with the fat residue to a solid white substance

Scanning or Photographing the Result

Graphical Refurbishment

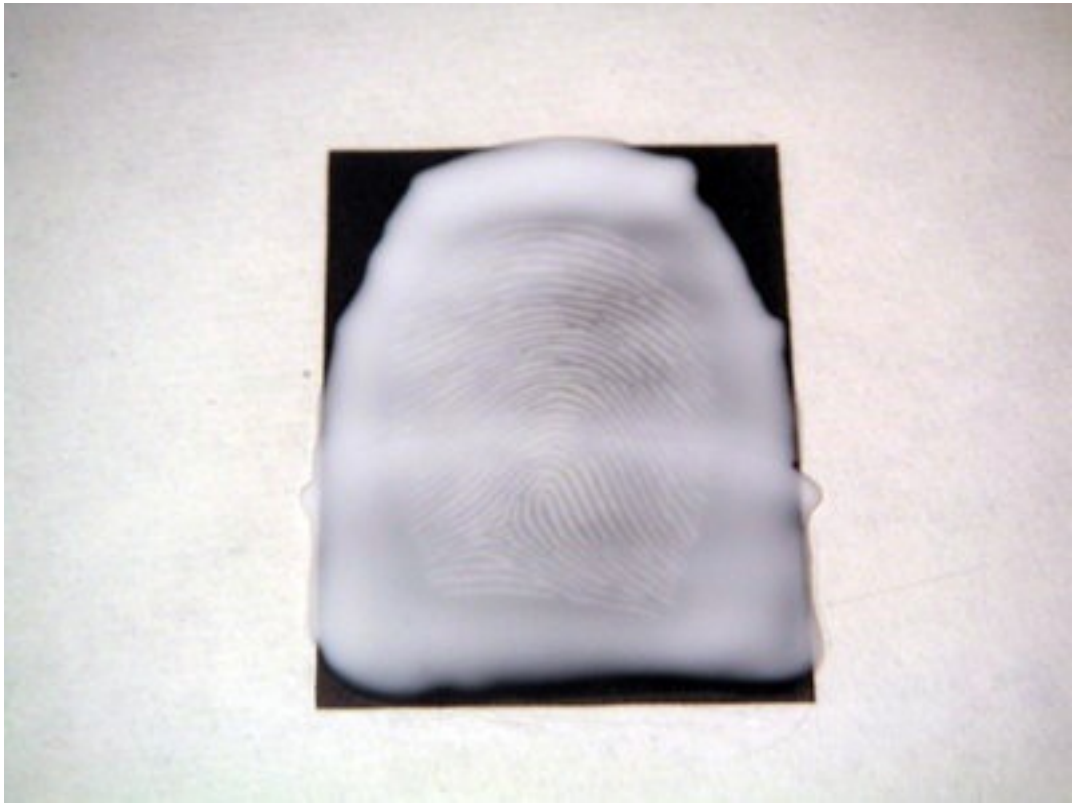
Printout on a Transparency Slide

- Toner forms a relief which is later used similar to letter press printing

Producing the Dummy

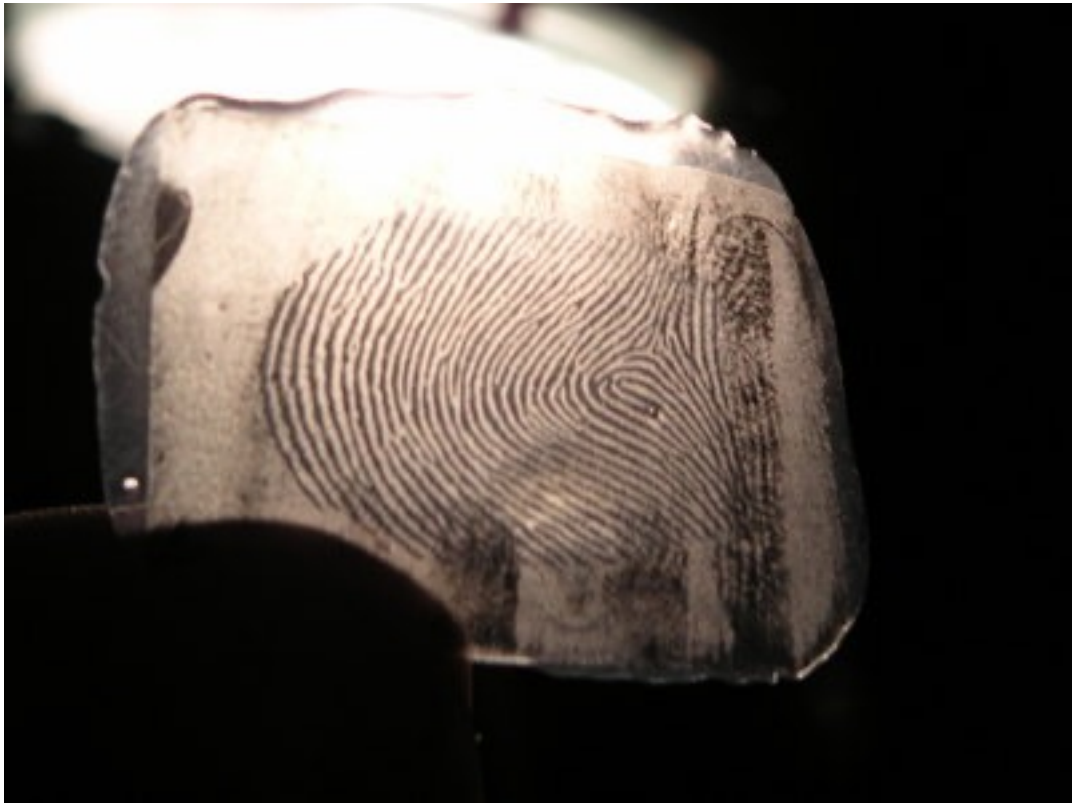
- Wood glue can be used to produce the dummy
  - Glycerin may be used to optimize humidity

Thin Glue Layer on the Printout



Hardened Glue

Cutting to Finger Size



- Dummy ready to use

The New Identity is Ready

- Theatrical glue can be used to glue the dummy onto the own finger

Fingerprint of Schaeuble

- March 2008: the Chaos Computer Club (CCC) impressively demonstrates how easy it is to obtain fingerprints
- The CCC Journal includes a transparency slide with Schaeuble's fingerprint
- The fingerprint originates from a glass the minister of interior (later finance, president of the Bundestag) used during a panel discussion
- The fingerprint is captured in the way described above