hacking biometric systems
Outline

- biometric systems
- attacking the data
  - the communication
  - the templates
- attacks using the sensor
  - fingerprint recognition
  - face recognition
  - iris recognition
**biometric systems**

- access control
  - rooms
  - computers
  - mobiles
  - cars
- payment
  - stores
  - governmental
  - ATMs
- border control
biometric systems - types of attacks

- attacking the data
  - communication data (1)
  - reference data (2)

- attacking the software (3)
  - matcher
  - threshold

- attacks using the sensor (4)
attacking the communication
sniffing the communication

- **Hardware**
  - USB-Agent / USB Tracker
  - GNU-Radio (van Eck)

- **Software**
  - usbsnoop
  - sniffusb
  - usbmon
**attacking the communication**

- directly replaying sniffed packages

  **sniffing**

  **replaying**

  **replay attack**

- attacking the software by manipulated stream data

by Lisa Thalheim
extracting images

- analysing stream data

- extracting images for dummies

- inserting own payload
  - data of allowed users
  - brute force
  - analysing template data
attacking the templates
templates

- localisation
  - in the filesystem (filemon)
  - in the registry (regmon)

- analysing
  - template to user correlation
  - used algorithms
  - checksums
  - raw images (making dummies)
**attacking the templates**

- extracting data for making dummies
- adding or deleting a template
- two people matching one template
attacks using the sensor
fingerprint recognition
fingerprint recognition

- convolution of the skin
- sensor types
  - capacitive
  - optical
  - thermal
  - pressure
- minutia based recognition
reactivating latent prints

- reactivating latent prints on touch sensors
  - capacitive: aspirate, graphite
  - optical: coloured powder
- graphite or coloured powder on adhesive tape
visualisation of latent prints on glossy surfaces

- coloured or magnetic powder
- cyanoacrylate
- vacuum metal deposition
visualisation of latent prints on paper

- amino acid indicator
  - Ninhydrin
  - Iodide

- thermal decomposition of grease
**making a dummy finger**

- gelatine
- silicone, wood glue
  - enhancing with graphite or gold
- aluminium foil on PCBs
fingerprint recognition :: life check

- **pulse**
  - IR illuminated bloodstream
  - deformation of the ridges

- **property of the skin**
  - electrical and thermal conductivity
  - colour

- **absorption of the blood**

- **sweat**
face recognition
face recognition

- 2 dimensional
- 3 dimensional
- infrared

- feature points
- eigenface
- template matching
face recognition :: defeatment

- **2D**
  - adapting the face (make up)
  - pictures or video
  - latex mask

- **3D**
  - latex mask
  - modeling the whole head

http://www.heise.de/ct/english/02/11/114/
face recognition :: life check

- moving of the head

- moving of the face
  - blinking
  - speaking

- reflection of the skin
iris recognition
**iris recognition**

- taking picture
  - near infrared spectrum for better contrast
- extracting the iris
- calculating iris code
iris recognition :: defeatment

- picture or video
- contact lense
  - printed or painted iris
  - iris hologram

http://www.heise.de/ct/english/02/11/114/
iris recognition :: life check

- moving the eye
- reflections of the eyes
- contracting pupil if illuminated
- flatness of the iris
conclusion

- most of the biometric systems are easy to fool
- fooling needs only a small amount of time and money

- Don't use biometric systems for security relevant applications!
Thank you.

starbug@biometrische-systeme.org
preventing the recognition

- superglue
- hard work :)  
- etching
- scorching
- remove with emery paper
- transplantation