hacking fingerprint recognition systems

(can I buy you a beer)

starbug@berlin.ccc.de

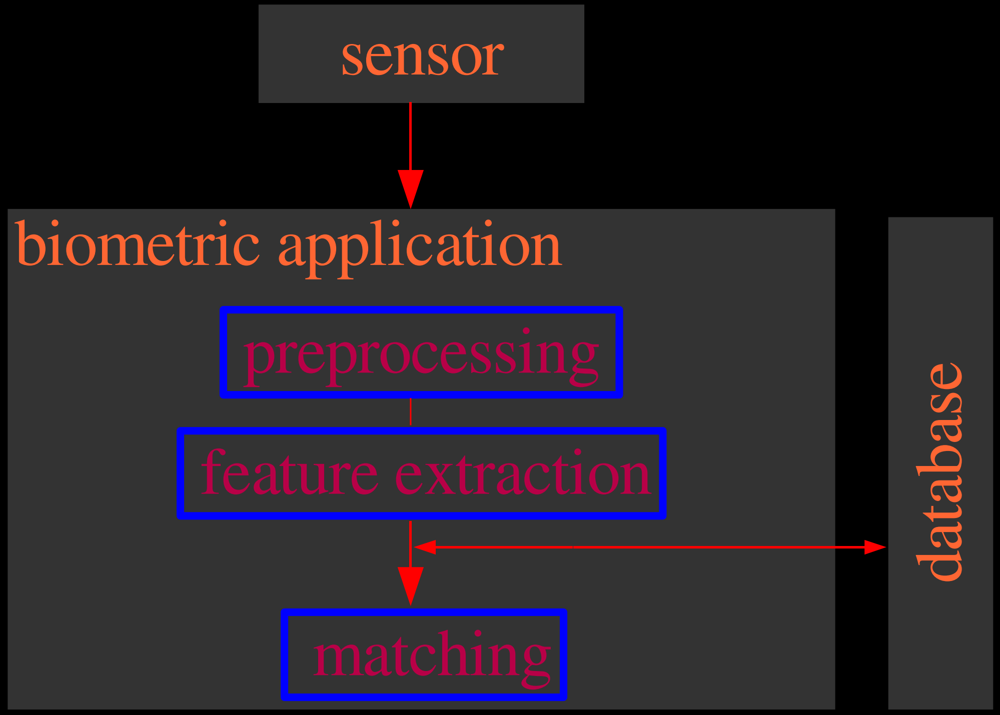
overview

- introduction

- collecting fingerprint data

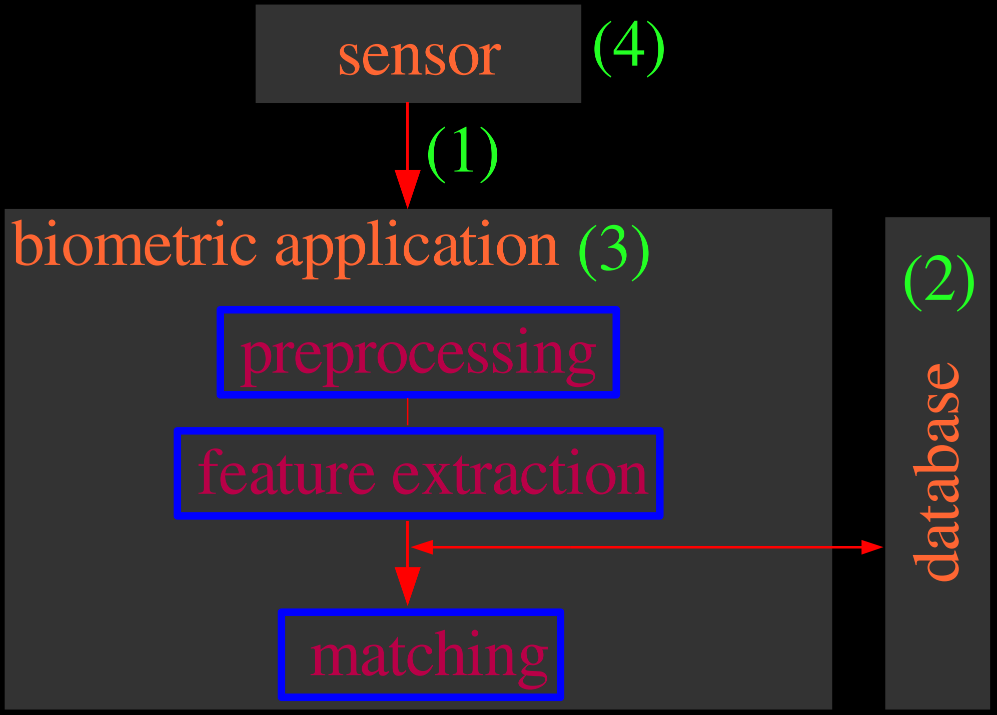
- attacking the communication
- attacking the templates
- attacks using the sensor

parts of biometric systems



parts of biometric systems

parts of biometric systems - types of attacks



sensor (4)

(1)

biometric application (3)

preprocessing

feature extraction

matching

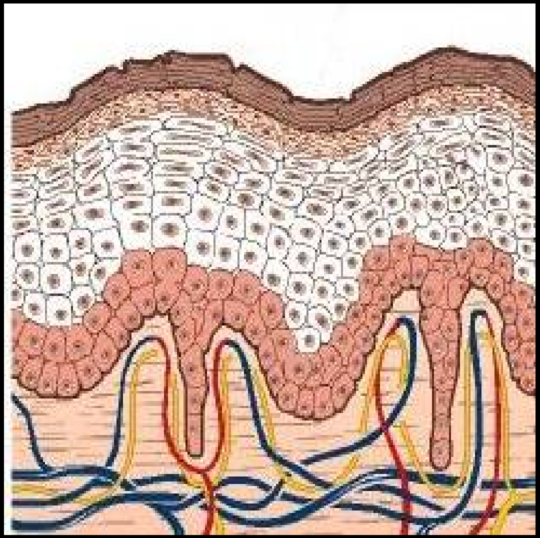
(2)

database

parts of biometric systems

- attacking the data
  - communication data (1)
  - reference data (2)
- attacking the software (3)
  - matcher
  - threshold
- attacks using the sensor (4)

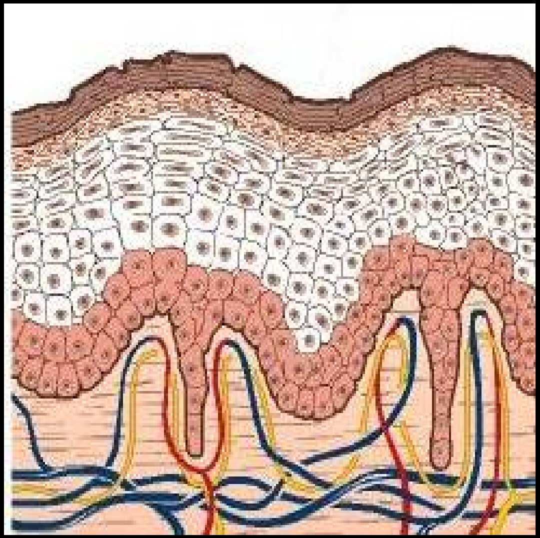
skin



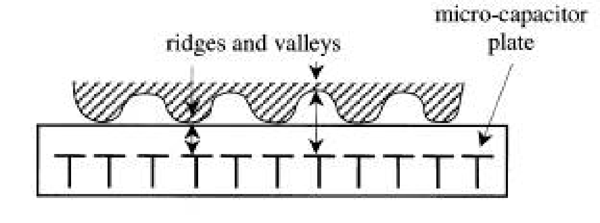
profile of the finger

skin

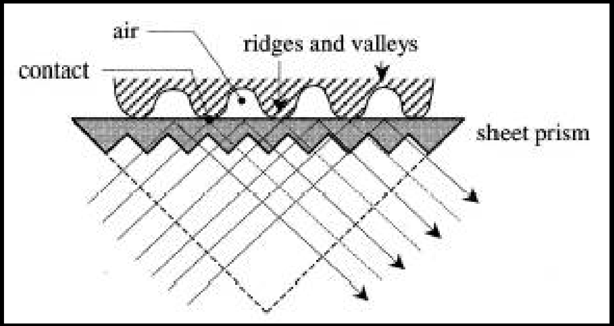
sensors



profile of the finger

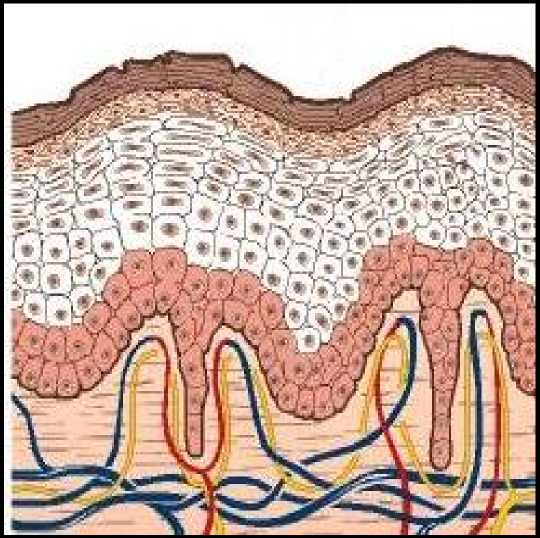


capacitive sensor



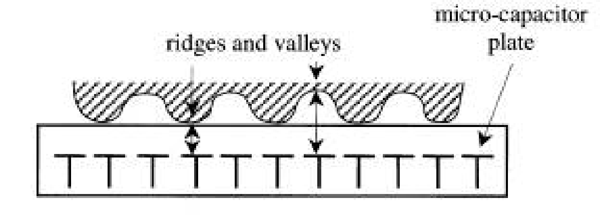
optical sensor

skin

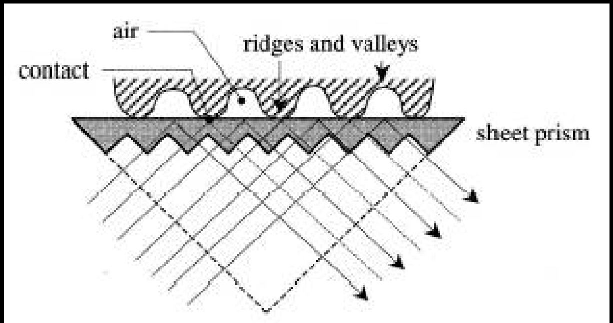


profile of the finger

sensors

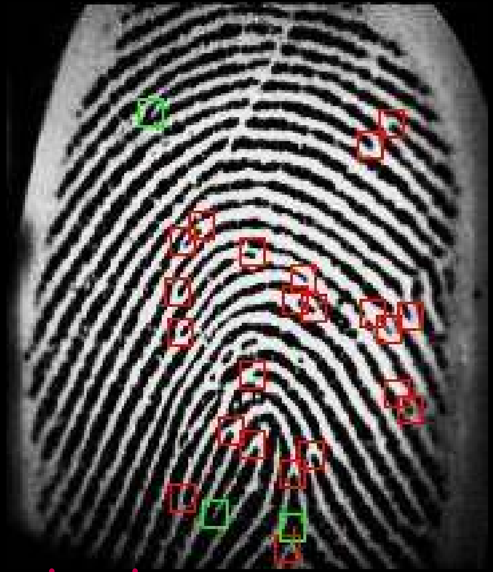


capacitive sensor

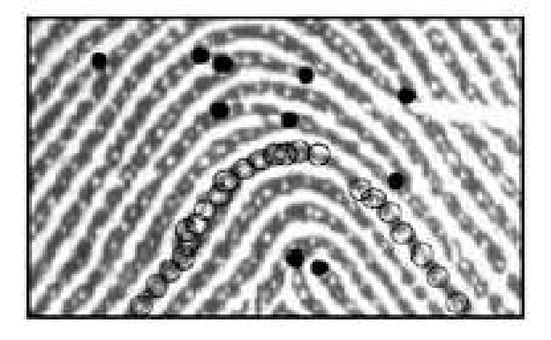


optical sensor

features



minutias



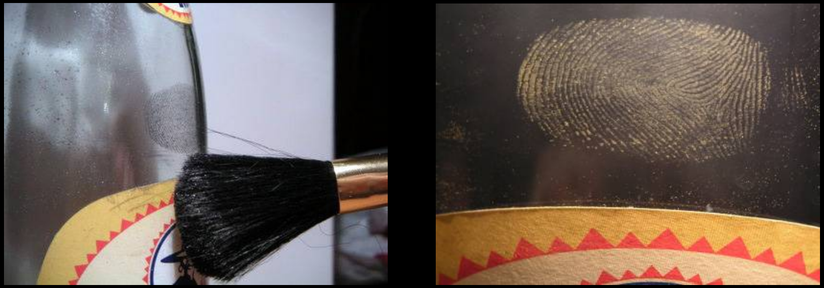
sweat pores

Marie Sandström

collecting the data

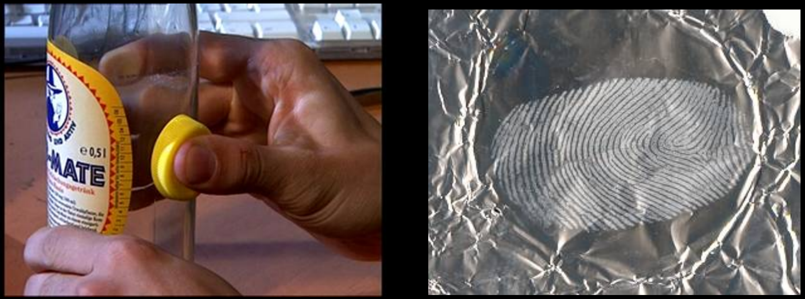
visualisation of latent prints on glossy surfaces

- coloured or magnetic powder



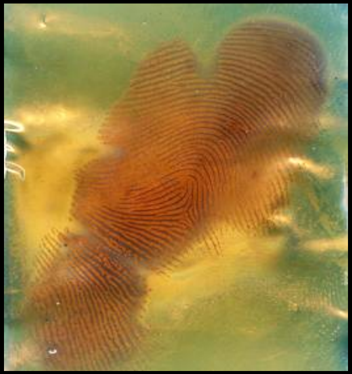
visualisation with coloured powder

- cyanoacrylate



visualisation with cyanoacrylate

- vacuum metal deposition



visualisation with sputtered gold

visualisation of latent prints on paper

- amino acid indicator
  - Ninhydrin
  - Iodide

visualisation with Ninhydrin

- thermal decomposition of grease

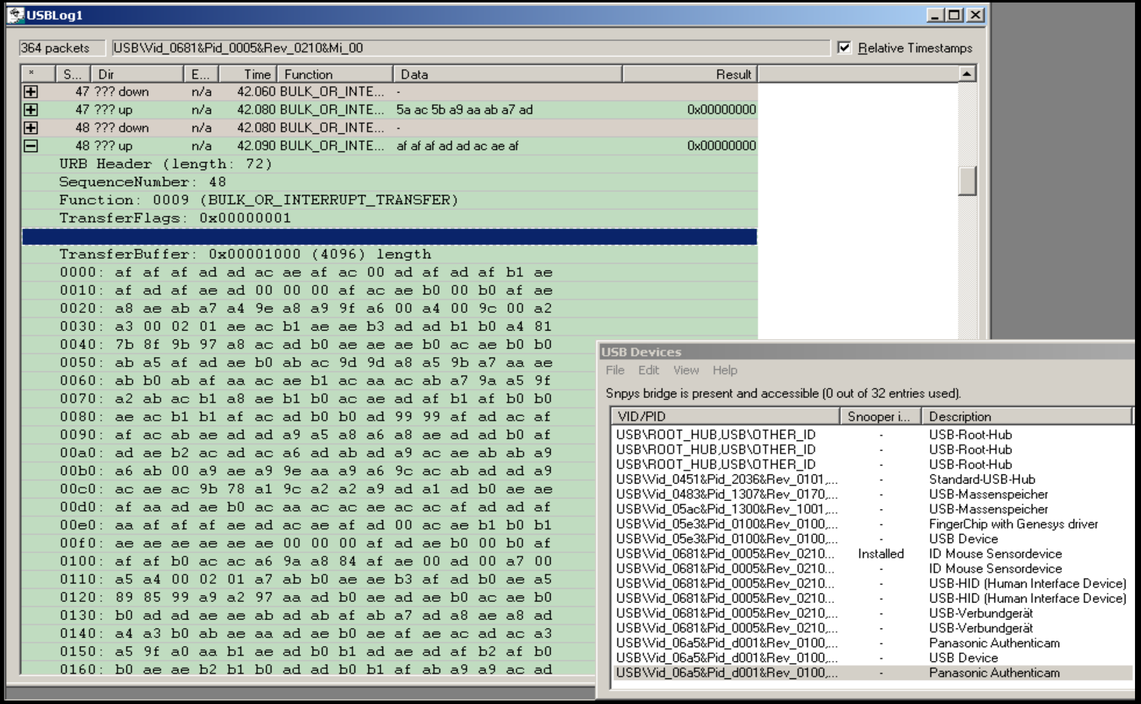
visualisation of grease

sniffing the communication

- Hardware
  - USB-Agent / USB Tracker
  - directly connected to the sensor
  - GNU-Radio
- Software
  - usbsnoop
  - sniffusb
  - usbmon

USB-Agent

www.hitex.com



364 packets USB\Vid_0681&Pid_0005&Rev_0210&Mi_00 ☑ Relative Timestamps

*	S...	Dir	E...	Time	Function	Data	Result
⊞	47	??? down	n/a	42.060	BULK_OR_INTE...	-	
⊞	47	??? up	n/a	42.080	BULK_OR_INTE...	5a ac 5b a9 aa ab a7 ad	0x00000000
⊞	48	??? down	n/a	42.080	BULK_OR_INTE...	-	
⊟	48	??? up	n/a	42.090	BULK_OR_INTE...	af af af ad ad ac ae af	0x00000000

```
URB Header (length: 72)
SequenceNumber: 48
Function: 0009 (BULK_OR_INTERRUPT_TRANSFER)
TransferFlags: 0x00000001

TransferBuffer: 0x00001000 (4096) length
0000: af af af ad ad ac ae af ac 00 ad af ad af b1 ae
0010: af ad af ae ad 00 00 00 af ac ae b0 00 b0 af ae
0020: a8 ae ab a7 a4 9e a8 a9 9f a6 00 a4 00 9c 00 a2
0030: a3 00 02 01 ae ac b1 ae ae b3 ad ad b1 b0 a4 81
0040: 7b 8f 9b 97 a8 ac ad b0 ae ae ae b0 ac ae b0 b0
0050: ab a5 af ad ae b0 ab ac 9d 9d a8 a5 9b a7 aa ae
0060: ab b0 ab af aa ac ae b1 ac aa ac ab a7 9a a5 9f
0070: a2 ab ac b1 a8 ae b1 b0 ac ae ad af b1 af b0 b0
0080: ae ac b1 b1 af ac ad b0 b0 ad 99 99 af ad ac af
0090: af ac ab ae ad ad a9 a5 a8 a6 a8 ae ad ad b0 af
00a0: ad ae b2 ac ad ac a6 ad ab ad a9 ac ae ab ab a9
00b0: a6 ab 00 a9 ae a9 9e aa a9 a6 9c ac ab ad ad a9
00c0: ac ae ac 9b 78 a1 9c a2 a2 a9 ad a1 ad b0 ae ae
00d0: af aa ad ae b0 ac aa ac ac ae ac ac af ad ad af
00e0: aa af af af ae ad ac ae af ad 00 ac ae b1 b0 b1
00f0: ae ae ae ae ae ae 00 00 00 af ad ae b0 00 b0 af
0100: af af b0 ac ac a6 9a a8 84 af ae 00 ad 00 a7 00
0110: a5 a4 00 02 01 a7 ab b0 ae ae b3 af ad b0 ae a5
0120: 89 85 99 a9 a2 97 aa ad b0 ae ad ae b0 ac ae b0
0130: b0 ad ad ae ae ab ad ab af ab a7 ad a8 ae a8 ad
0140: a4 a3 b0 ab ae aa ad ae b0 ae af ae ac ad ac a3
0150: a5 9f a0 aa b1 ae ad b0 b1 ad ae ad af b2 af b0
0160: b0 ae ae b2 b1 b0 ad ad b0 b1 af ab a9 a9 ac ad
```

Snpys bridge is present and accessible (0 out of 32 entries used).

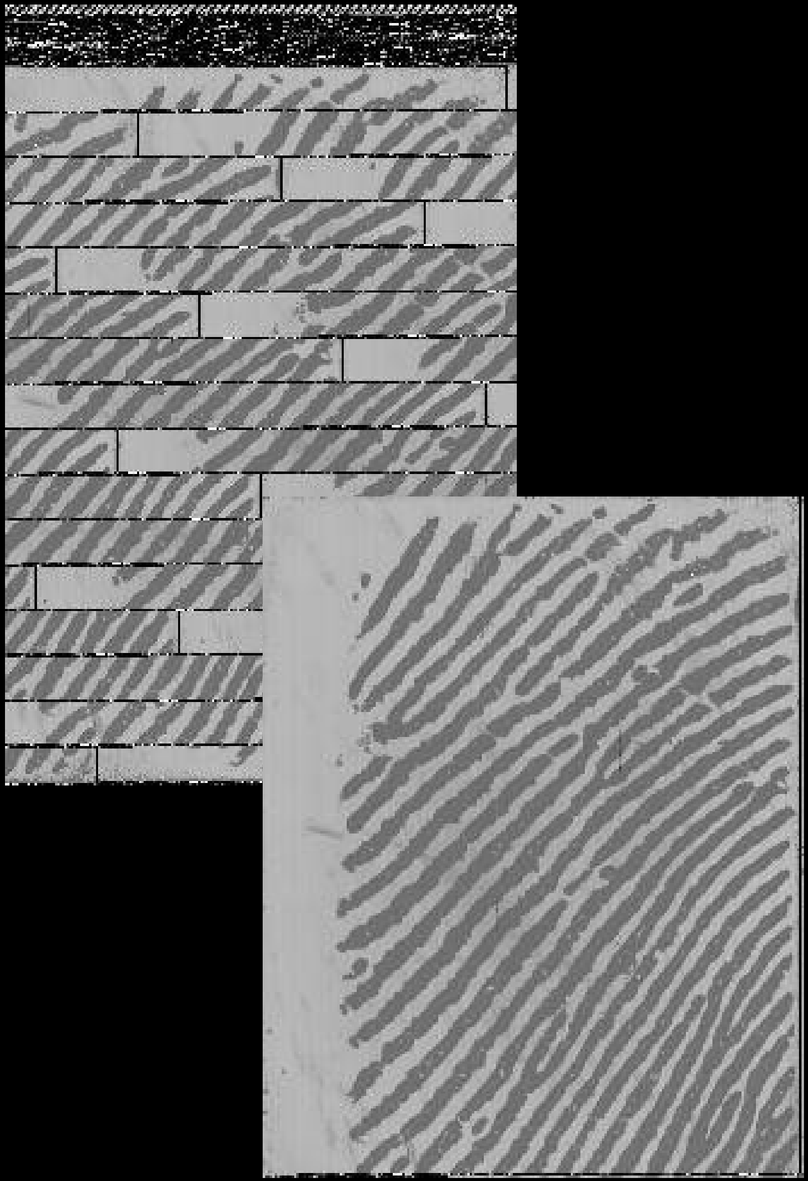
VID/PID	Snooper i...	Description
USB\ROOT_HUB,USB\OTHER_ID	-	USB-Root-Hub
USB\ROOT_HUB,USB\OTHER_ID	-	USB-Root-Hub
USB\ROOT_HUB,USB\OTHER_ID	-	USB-Root-Hub
USB\Vid_0451&Pid_2036&Rev_0101,...	-	Standard-USB-Hub
USB\Vid_0483&Pid_1307&Rev_0170,...	-	USB-Massenspeicher
USB\Vid_05ac&Pid_1300&Rev_1001,...	-	USB-Massenspeicher
USB\Vid_05e3&Pid_0100&Rev_0100,...	-	FingerChip with Genesys driver
USB\Vid_05e3&Pid_0100&Rev_0100,...	-	USB Device
USB\Vid_0681&Pid_0005&Rev_0210...	Installed	ID Mouse Sensordevice
USB\Vid_0681&Pid_0005&Rev_0210...	-	ID Mouse Sensordevice
USB\Vid_0681&Pid_0005&Rev_0210...	-	USB-HID (Human Interface Device)
USB\Vid_0681&Pid_0005&Rev_0210...	-	USB-HID (Human Interface Device)
USB\Vid_0681&Pid_0005&Rev_0210,...	-	USB-Verbundgerät
USB\Vid_0681&Pid_0005&Rev_0210,...	-	USB-Verbundgerät
USB\Vid_06a5&Pid_d001&Rev_0100,...	-	Panasonic Authenticam
USB\Vid_06a5&Pid_d001&Rev_0100,...	-	USB Device
USB\Vid_06a5&Pid_d001&Rev_0100,...	-	Panasonic Authenticam

usbsnoop

data analysis

- collecting public information
- analysing the sensor

- type of data
  - raw vs. templates
- encryption
- header
  - timestamps
  - checksums

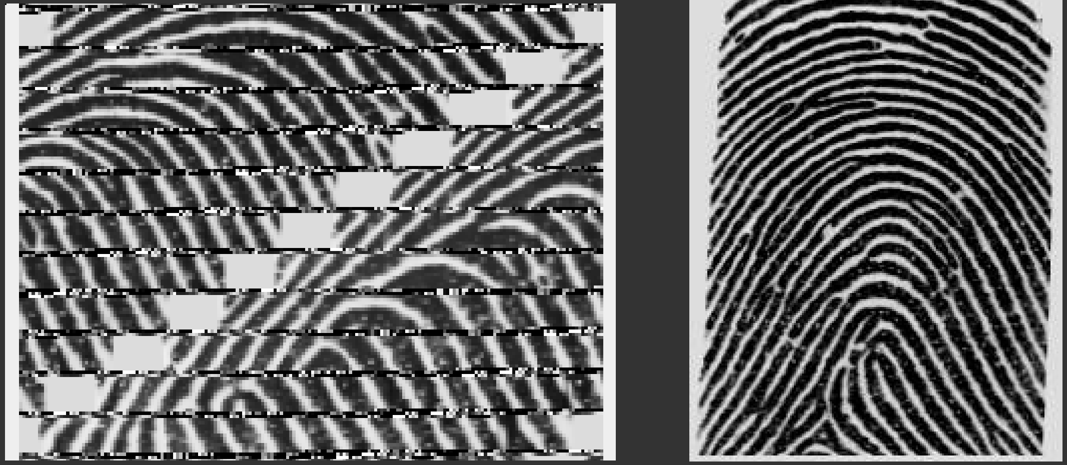


USB-sniff of the Siemens ID Mouse

sniffing the data @ thinkpad sensor

- direct sniffing not possible
  - hardware: built-in sensor
  - software: encrypted data (TPM?)
- external version of the sensor

external IBM sensor



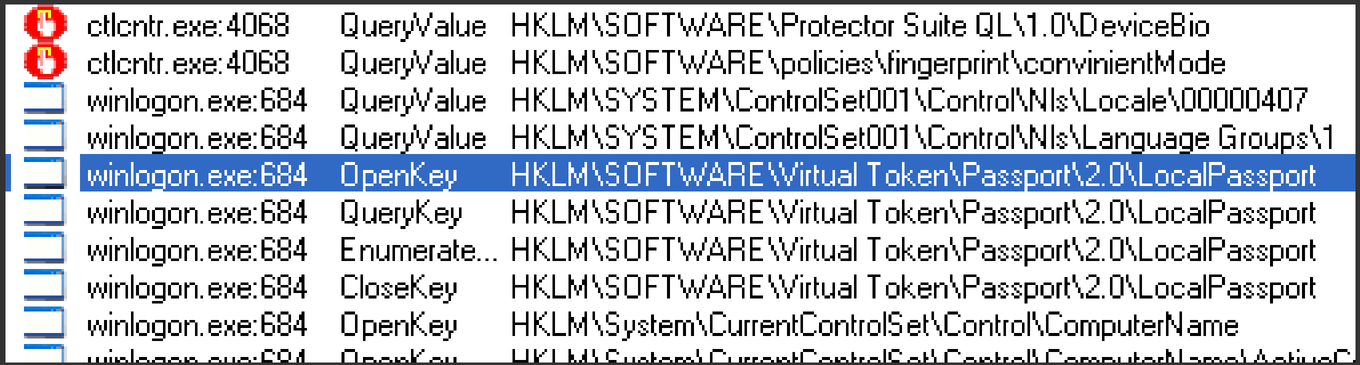
USB-sniff of the Thinkpad sensor

http://www-8.ibm.com/lenovoinfo/fingerprint/i/usb_fpr.gif

templates

- localisation
  - in the filesystem (filemon)
  - in the registry (regmon)
- analysing
  - template to user correlation
  - used algorithms
  - checksums
  - raw images

templates @ thinkpad sensor



```
ctlcntr.exe:4068   QueryValue  HKLM\SOFTWARE\Protector Suite QL\1.0\DeviceBio
ctlcntr.exe:4068   QueryValue  HKLM\SOFTWARE\policies\fingerprint\convinientMode
winlogon.exe:684   QueryValue  HKLM\SYSTEM\ControlSet001\Control\Nls\Locale\00000407
winlogon.exe:684   QueryValue  HKLM\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
winlogon.exe:684   OpenKey     HKLM\SOFTWARE\Virtual Token\Passport\2.0\LocalPassport
winlogon.exe:684   QueryKey    HKLM\SOFTWARE\Virtual Token\Passport\2.0\LocalPassport
winlogon.exe:684   Enumerate...HKLM\SOFTWARE\Virtual Token\Passport\2.0\LocalPassport
winlogon.exe:684   CloseKey    HKLM\SOFTWARE\Virtual Token\Passport\2.0\LocalPassport
winlogon.exe:684   OpenKey     HKLM\System\CurrentControlSet\Control\ComputerName
winlogon.exe:684   OpenKey     HKLM\System\CurrentControlSet\Control\ComputerName\ActiveC
```

RegMon output of the enrolment

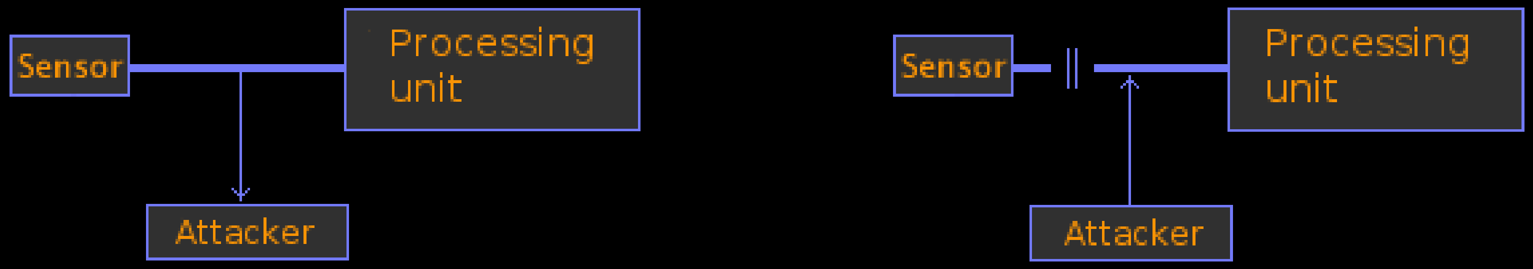
- HKEY_LOCAL_MACHINE\SOFTWARE\Virtual Token\Passport\2.0
  - \LocalPassport\User <Username>
  - \LocalPassportBio

- C:\WINDOWS\system32\config\SOFTWARE
- template starts with: 00 13 48 5b [01 02]

attacking the communication

attacking the communication

- replaying sniffed packages



sniffing

replaying

replay attack

by Lisa Thalheim

- inserting self-generated data
  - analyse template data
  - attacking the software

attacking the templates

attacking the templates

- adding or deleting a template
- two people matching one template
- changing template to person correlation
- attacking the software using a manipulated template

attacking the templates @ thinkpad sensor

- read the template in the registry
- add your own fingerprint to an existing template
- write back to the registry (biometric worm)

attacks using the sensor

latent prints 1

- reactivating latent prints on touch sensors
  - capacitive: aspirate, graphite
  - optical: coloured powder

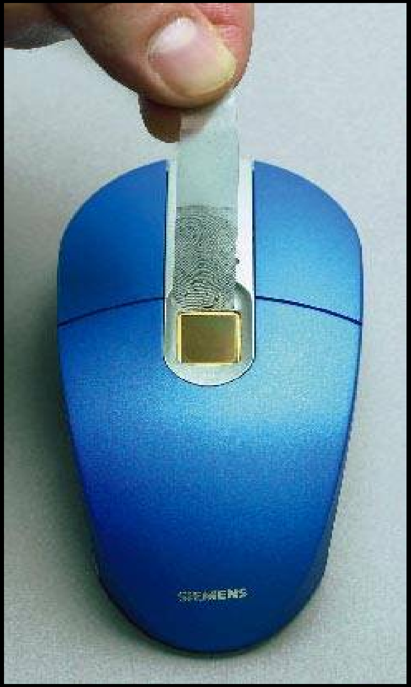
- countermeasures
  - checking minutia position of the last login

reactivating latent prints

http://www.heise.de/ct/02/11/114/

latent prints 2

- using latent prints (not on the sensor)
  - graphite or coloured powder on adhesive tape
- not for sweeping sensors



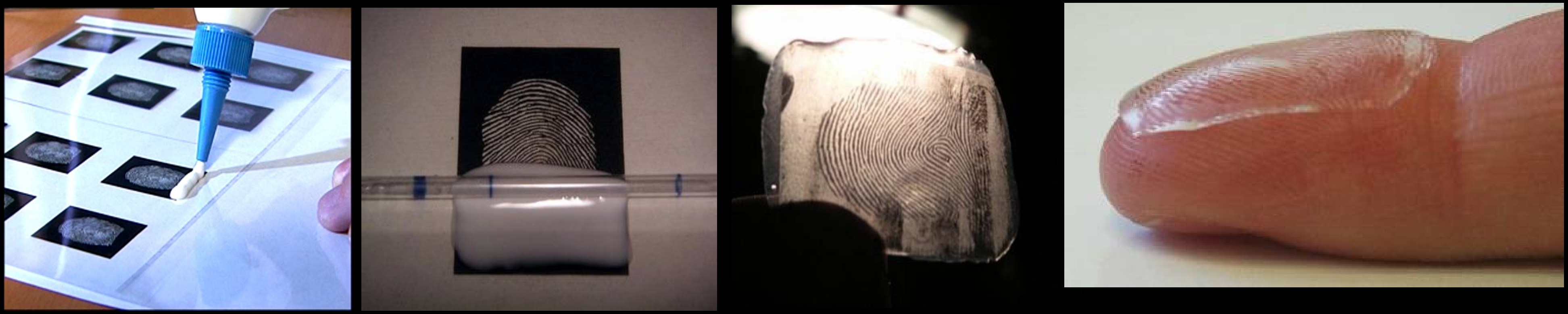
graphite powder on adhesive tape

http://www.heise.de/ct/02/11/114/

making a dummy finger

- gelatine, silicone

- wood glue

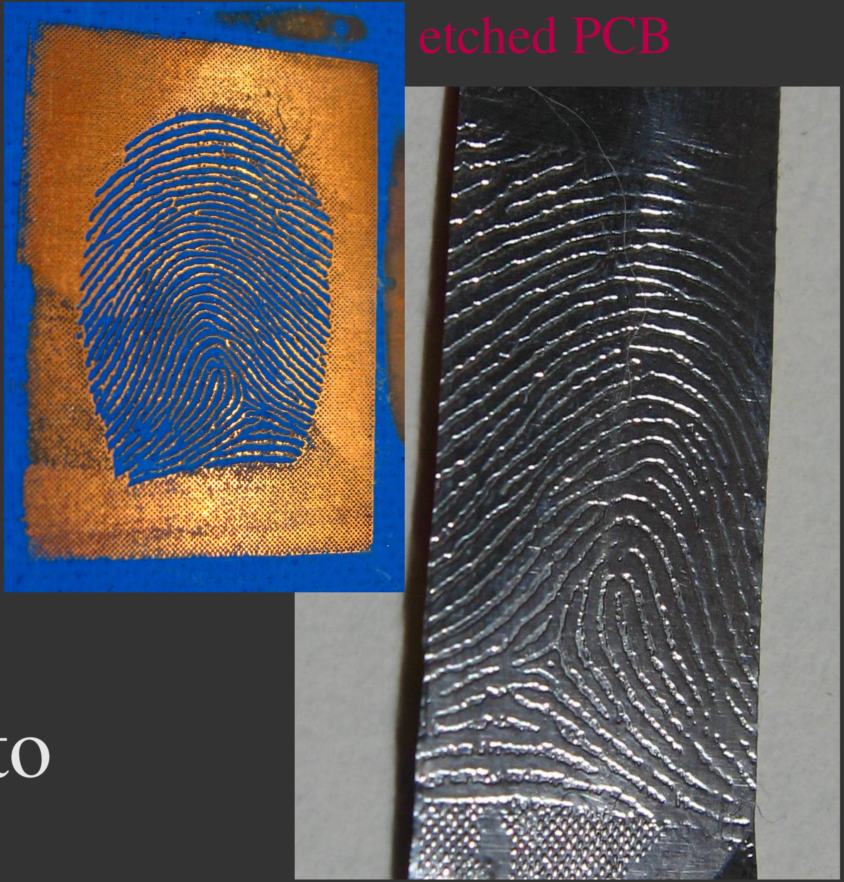


making a dummy finger

- enhancing with graphite spray

making a dummy fingers @ thinkpad sensor

- etching an optical PCB
- aluminium foil on adhesive tape
- transfer the fingerprint onto the foil



etched PCB

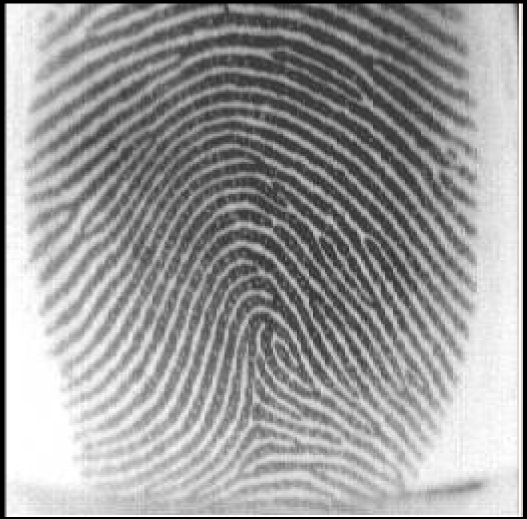
dummy finger

life check

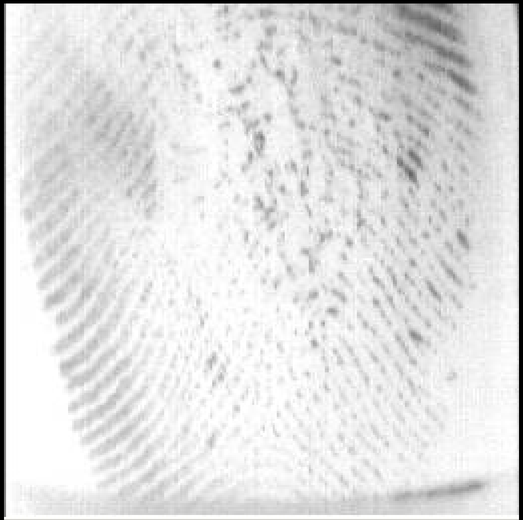
- pulse
  - IR illuminated bloodstream
  - deformation of the ridges
- property of the skin
  - electrical and thermal conductivity
  - colour
- absorption of the blood
- sweat

preventing the recognition

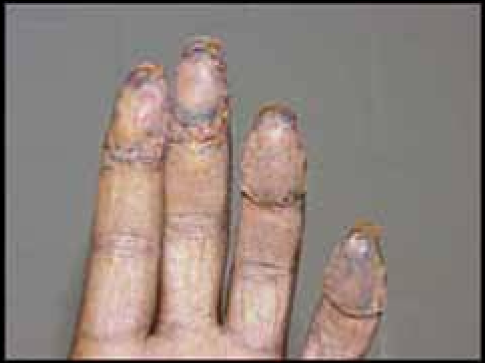
- superglue
- hard work :)
- etching
- scorching
- remove with emery paper
- transplantation



normal fingerprint



superglued fingerprint



transplanted fingertips

http://www.sploid.com/images/feetfinger.jpg

hacked sensors (systems)

- capacitive
  - Infineon (Siemens ID mouse)
  - UPEK (IBM Thinkpads)
- optical
  - Dermalog
  - U.are.U (Microsoft)
  - Identix
- thermical
  - Atmel (ekey, iPAQ)
- electrical
  - Authentec (Medion)

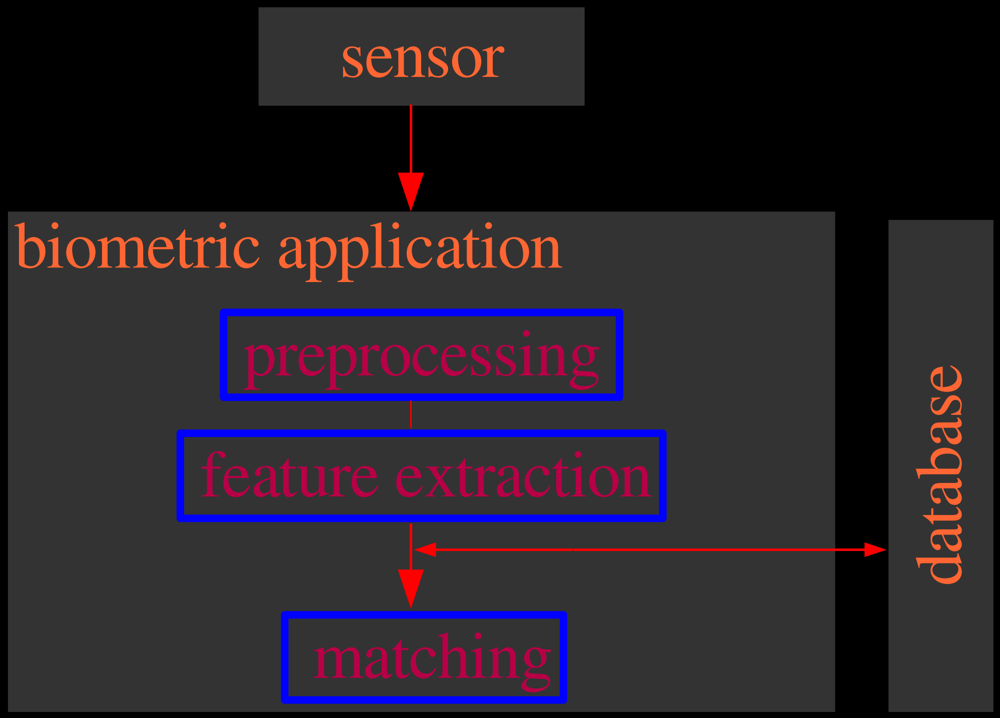
conclusion

- latent prints left on nearly every surface
- prints are easy to collect
- nearly all tested systems could be fooled with home-made dummy finger
- fall-back passwords still needed

- **Don't use fingerprint recognition systems for security relevant applications!**

Thank you.

starbug@berlin.ccc.de


sensor
biometric application
preprocessing
feature extraction
matching
database