



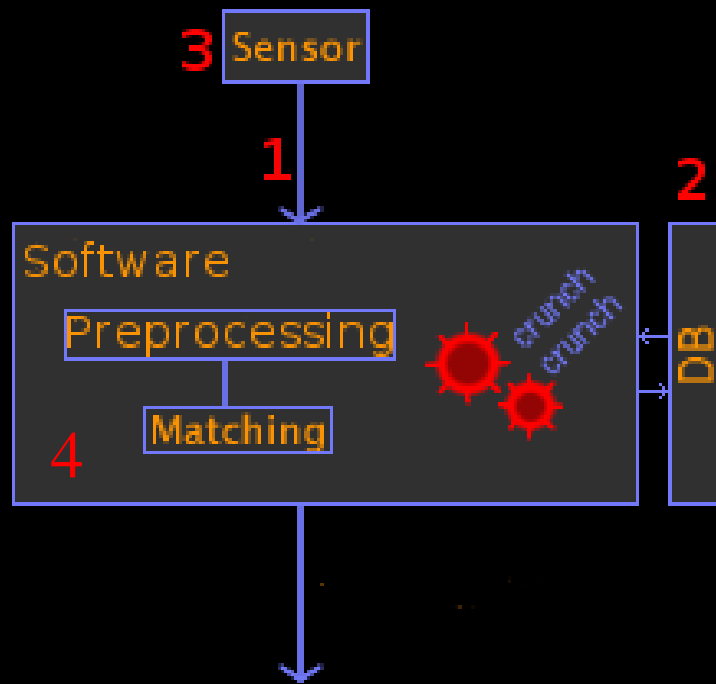
**hacking
fingerprint recognition systems**

starbug@biometrische-systeme.org

overview

- introduction
- collecting fingerprint data
- attacking the communication
- attacking the templates
- attacks using the sensor

biometric systems - types of attacks

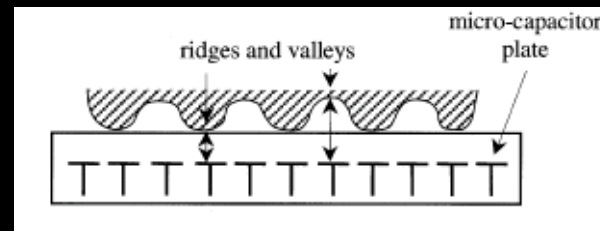


parts of biometric systems
by Lisa Thalheim

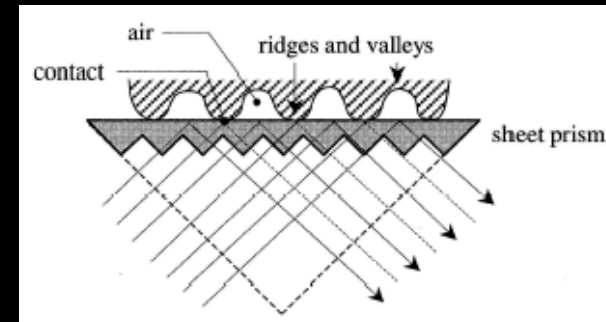
- attacking the data
 - communication data (1)
 - reference data (2)
- attacks using the sensor (3)
- attacking the software (4)
 - matcher
 - threshold
 - ...

sensor types

- capacitive
- optical
- electrical
- thermal



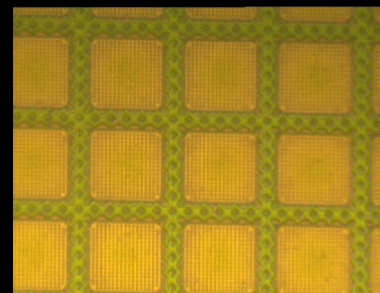
capacitive sensor



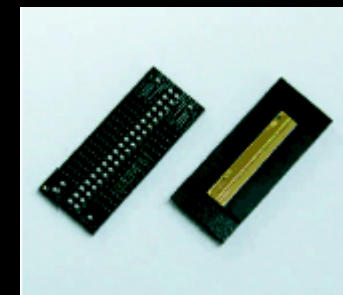
optical sensor

http://www.diva-portal.org/diva/getDocument?urn_nbn_se_liu_diva-2397-1__fulltext.pdf

- touching
- sweeping



array of capacitors



sweep sensor

collecting the data

visualisation of latent prints on glossy surfaces

- coloured or magnetic powder



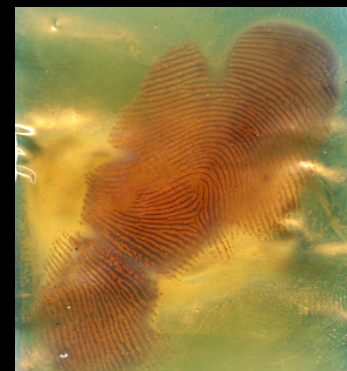
visualisation with coloured powder

- cyanoacrylate



visualisation with cyanoacrylate

- vacuum metal deposition



visualisation with sputtered gold

visualisation of latent prints on paper

- amino acid indicator
 - Ninhydrin
 - Iodide

- thermal decomposition of grease



visualisation with
Ninhydrin



visualisation of grease

sniffing the communication

- Hardware
 - USB-Agent / USB Tracker
 - directly connected to the sensor
 - GNU-Radio



USB-Agent

www.hitex.com

- Software
 - usbsnoop
 - sniffusb
 - usbmon

The screenshot shows the USBLog1 application window. The top bar indicates '364 packets' and the selected filter is 'USB\VID_0681&Pid_0005&Rev_0210&MI_00'. The main window displays a table of captured packets with columns for sequence number, direction, error status, time, function, data, and result. Below the table, a detailed view of a packet is shown, including the URB Header (length: 72), SequenceNumber (48), Function (0009 (BULK_OR_INTERRUPT_TRANSFER)), TransferFlags (0x00000001), and a large TransferBuffer (length: 4096) containing hexadecimal data.

Below the main window, a 'USB Devices' window is open, showing a list of detected USB devices. The table below is a reproduction of the data shown in this window:

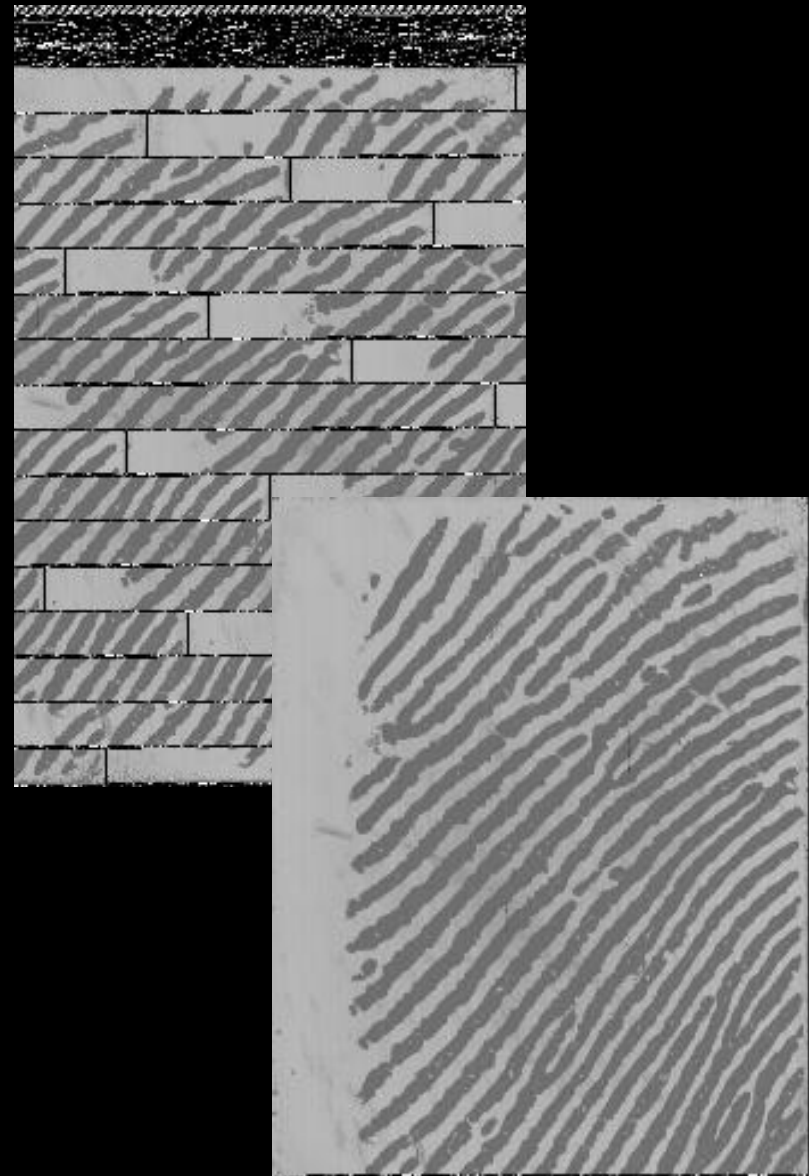
VID/PID	Snooper i...	Description
USB\ROOT_HUB\USB\OTHER_ID	-	USB-Root-Hub
USB\ROOT_HUB\USB\OTHER_ID	-	USB-Root-Hub
USB\ROOT_HUB\USB\OTHER_ID	-	USB-Root-Hub
USB\VID_0451&Pid_2036&Rev_0101...	-	Standard-USB-Hub
USB\VID_0483&Pid_1307&Rev_0170...	-	USB-Massenspeicher
USB\VID_05ac&Pid_1300&Rev_1001...	-	USB-Massenspeicher
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-Verbundergerät
USB\VID_0681&Pid_0005&Rev_0210...	-	USB-Verbundergerät
USB\VID_0681&Pid_0005&Rev_0210...	-	USB-Verbundergerät
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

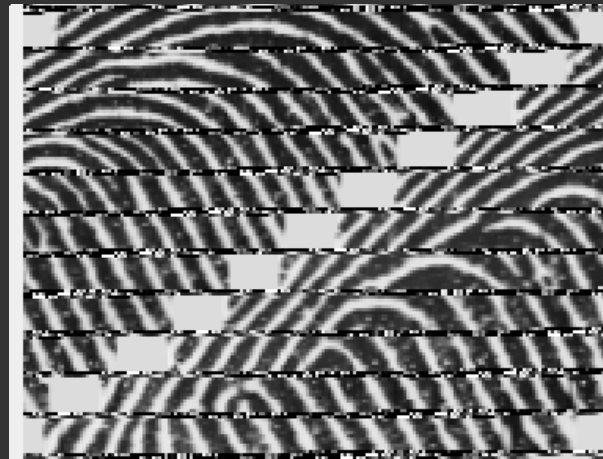


sniffing the data @ thinkpad sensor

- 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



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

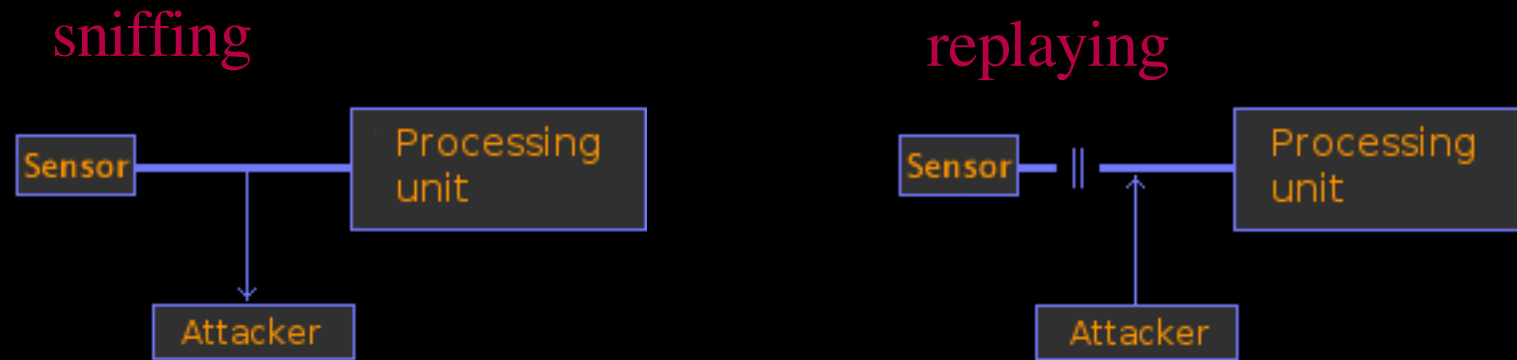
RegMon output of the enrolment

- 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



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

latent prints 2

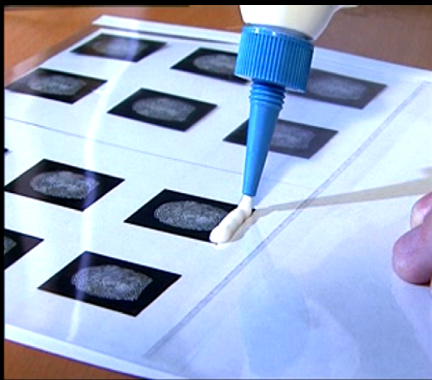
- using latent prints (not on the sensor)
 - graphite or coloured powder on adhesive tape
- not for sweeping sensors



graphite powder on adhesive tape

making a dummy finger

- gelatine, silicone
- wood glue



making a dummy finger

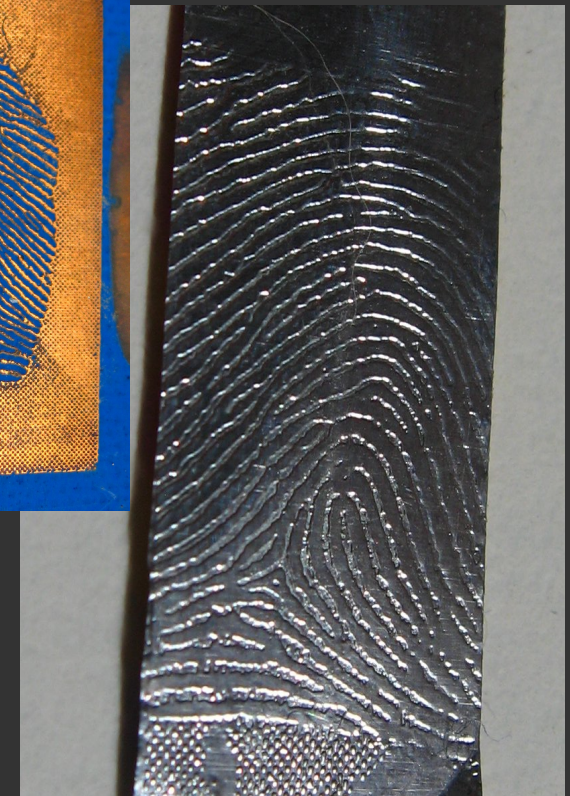
- enhancing with graphite spray

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

hacked sensors (systems)

- capacitive
 - Infineon (Siemens ID mouse)
 - UPEK (IBM Thinkpads)
- optical
 - Dermalog
 - U.are.U (Microsoft)
 - Identix
- thermal
 - 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@biometrische-systeme.org

preventing the recognition

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

