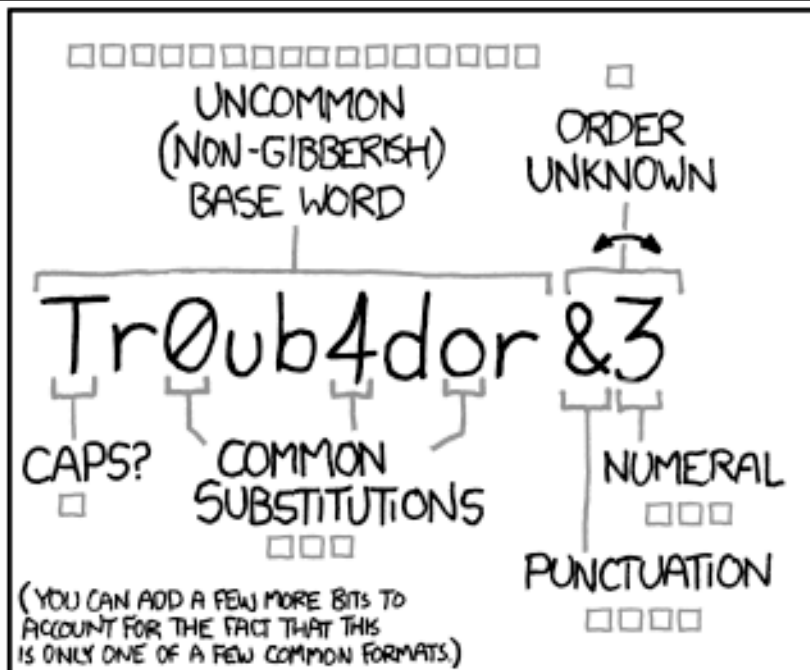# User Authentication

Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Goals for Today

◆ User Authentication

◆ Lab 2 due next Friday

Password Reuse

Panel 1:
UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN

Tr0ub4dor &3

CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

Panel 2:
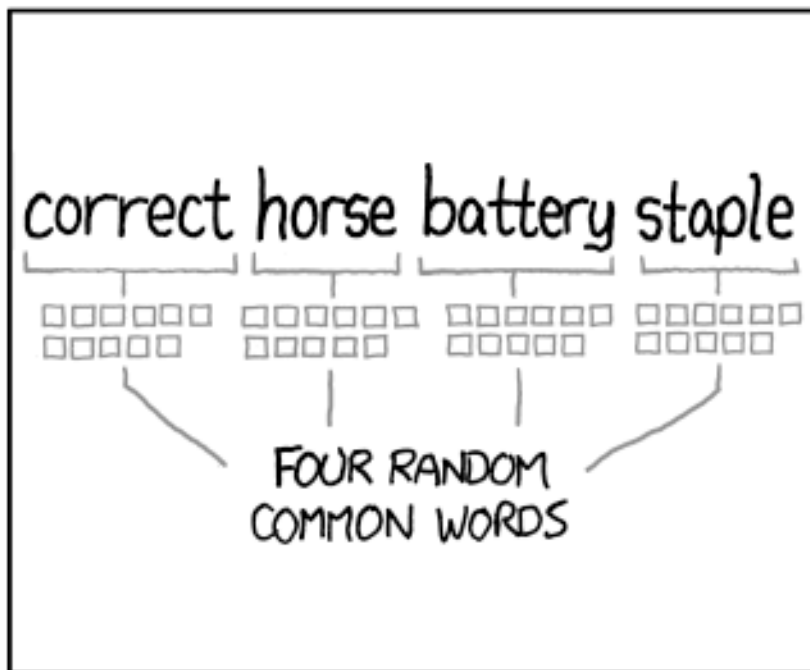~28 BITS OF ENTROPY

2^{28} = 3 DAYS AT 1000 GUESSES/SEC

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:
EASY

Panel 3:
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:
HARD

Panel 4:
correct horse battery staple

FOUR RANDOM COMMON WORDS

Panel 5:
~44 BITS OF ENTROPY

2^{44} = 550 YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS:
HARD

Panel 6:
THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

PHP "0-day"

◆ Add ?-s to end of php script:

- http://..../config.php?-s

◆ History (as I understand it):

- Someone found it and told PHP developers 6 months ago
- PHP developer accidentally marked bug as public before it was fixed
- Some versions of php-cgi pass the command line arguments directly to the php-cgi binary
  – "-s" is "show source"

Graphical Passwords

- ◆ Images are easy for humans to process and remember
  - Especially if you invent a memorable story to go along with the images
- ◆ Dictionary attacks on graphical passwords are difficult
  - Images are believed to be very "random" (is this true?)
- ◆ Still not a perfect solution
  - Need infrastructure for displaying and storing images
  - Shoulder surfing

Empirical Results

- Experimental study of 154 computer science students at Johns Hopkins and Carnegie Mellon
- Conclusions:
  - "… faces chosen by users are highly affected by the race of the user… the gender and attractiveness of the faces bias password choice… In the case of male users, we found this bias so severe that we do not believe it possible to make this scheme secure against an online attack…"
- 2 guesses enough for 10% of male users
- 8 guesses enough for 25% of male users

User Quotes

- ◆ "I chose the images of the ladies which appealed the most"
- ◆ "I simply picked the best lookin girl on each page"
- ◆ "In order to remember all the pictures for my login (after forgetting my 'password' 4 times in a row) I needed to pick pictures I could EASILY remember... So I chose beautiful women. The other option I would have chosen was handsome men, but the women are much more pleasing to look at"

More User Quotes

- "I picked her because she was female and Asian and being female and Asian, I thought I could remember that"
- "I started by deciding to choose faces of people in my own race…"
- "… Plus he is African-American like me"

- Recommendation: system picks passfaces
- But is that still memorable? What issues could arise?

What about multiple passwords?

- 109 participants in a 5 week study
- Email-based prompts to access the study website and authenticate
- Study emails were sent on Tuesday, Wednesday, Thursday, and Friday
- Participants were allowed a maximum of three login attempts

Study Conditions

Frequency, interference, and training do play a role in memorability

Variants...

◆ Recall that there also exist: click-based graphical passwords, drawing-based passwords, ...

Uses of graphical passwords?

◆ For what applications might graphical passwords be particularly useful?

Multi-Factor Authentication

Passwords are easy to steal from users, often guessable, and websites get broken into all the time.

For better security, require **two or more factors:**

◆ Something you **know** (e.g., password)
◆ Something you **have** (e.g., key, smart card, phone)
◆ Something you **are** (biometrics)

What About Biometrics?

◆ Authentication: **What you are**

◆ Unique identifying characteristics to authenticate user or create credentials

- Biological and physiological: Fingerprints, iris scan
- Behaviors characteristics - how perform actions: Handwriting, typing, gait

◆ Advantages:

- Nothing to remember
- Passive
- Can't share (generally)
- With perfect accuracy, could be fairly unique

Overview [from Matsumoto]
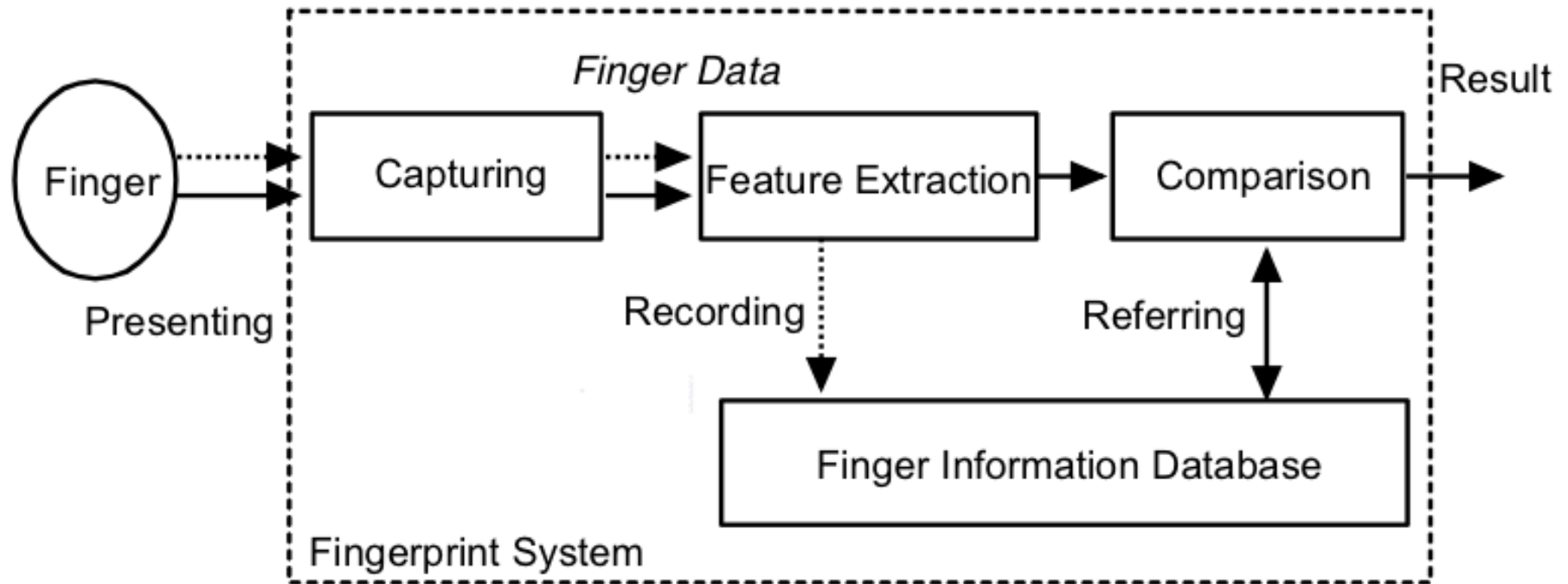
Tsutomu Matsumoto's image, from http://web.mit.edu/6.857/ OldStuff/Fall03/ref/gummy-slides.pdf

Dashed lines for enrollment; solid for verification or identification

Biometric Error Rates (Non-Adversarial)

◆ "Fraud rate" vs. "insult rate"
  - Fraud = system incorrectly accepts (false accept)
  - Insult = system rejects valid user (false reject)

◆ Increasing acceptance threshold increases fraud rate, decreases insult rate

◆ For biometrics, U.K. banks set target fraud rate of 1%, insult rate of 0.01%   [Ross Anderson]

Biometrics

◆ Face recognition (by a computer algorithm)

- High error rates even under reasonable variations in lighting, viewpoint and expression

◆ Fingerprints

- Traditional method for identification
- 1911: first US conviction on fingerprint evidence
- U.K. traditionally requires 16-point match
  - Probability of false match is 1 in 10 billion
  - No successful challenges until 2000
- Fingerprint damage impairs recognition

Other Biometrics

◆ Iris scanning

- Irises are very random, but stable through life
  - Different between the two eyes of the same individual
- 256-byte iris code based on concentric rings between the pupil and the outside of the iris
- Equal error rate better than 1 in a million
- Among best biometric mechanisms

◆ Hand geometry

- Used in nuclear premises entry control, INSPASS (discontinued in 2002)

Other Biometrics

- ◆ Vein
  - Pattern on back of hand
- ◆ Handwriting
- ◆ Typing
  - Timings for character sequences
- ◆ Gait
- ◆ DNA

Any issues with this?

Canon Files For DSLR Iris Registration Patent

Posted by kdawson on Tuesday February 12, @07:39PM
from the **biological-metadata** dept.

An anonymous reader writes

"Canon has filed for a patent for using iris watermarking (as in the iris of your eye) to take photographer's copyright protection to the next level. You set up the camera to capture an image of your eye through the viewfinder. Once captured, this biological reference is embedded as metadata into every photo you take. Canon claims this will help with copyright infringement of photos online."

Issues with Biometrics

◆ Private, but not secret
  - Maybe encoded on the back of an ID card?
  - Maybe encoded on your glass, door handle, ...
  - Sharing between multiple systems?

◆ Revocation is difficult (impossible?)
  - Sorry, your iris has been compromised, please create a new one...

◆ Physically identifying
  - Soda machine to cross-reference fingerprint with DMV?

Issues with Biometrics

◆ Criminal gives an inexperienced policeman fingerprints in the wrong order

- Record not found; gets off as a first-time offender

◆ Can be attacked using recordings

- Ross Anderson: in countries where fingerprints are used to pay pensions, there are persistent tales of "Granny's finger in the pickle jar" being the most valuable property she bequeathed to her family

◆ Birthday paradox

- With false accept rate of 1 in a million, probability of false match is above 50% with only 1609 samples

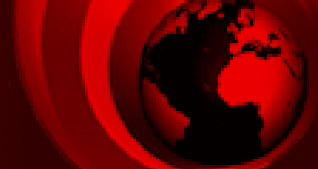# Issues with Biometrics

◆ Anecdotally, car jackings went up when it became harder to steal cars without the key
◆ But what if you need your fingerprint to start your car?

- Stealing cars becomes harder
- So what would the car thieves have to do?

Risks of Biometrics

OPEN **The News in 2 minutes**

News services
Your news when
want it

Last Updated: Thursday, 31 March, 2005, 10:37 GMT 11:37 UK

✉ E-mail this to a friend   🖶 Printable version

News Front
Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.

SEE ALSO:
▸ Malaysia to act
pirates
16 Mar 05 | As

RELATED INTER
▸ Malaysian police
The BBC is not r
for the content o
internet sites

**TOP ASIA-PACIF
STORIES**
▸ Australians war
cuts
▸ Taiwan campus

http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

Biometric Error Rates (Adversarial)

◆ Want to minimize "fraud" and "insult" rate

- "Easy" to test probability of accidental misidentification (fraud)
- But what about adversarial fraud

◆ An adversary might try to steal the biometric information

- Malicious fingerprint reader
  - Consider when biometric is used to derive a cryptographic key
- Residual fingerprint on a glass

Voluntary: Making a Mold

[Matsumoto]

Put the plastic into hot water to soften it.

Press a live finger against it.

The mold

It takes around 10 minutes.

http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Voluntary: Making a Finger

[Matsumoto]

Pour the liquid into the mold.

It takes around 10 minutes.

Put it into a refrigerator to cool.

The gummy finger

http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Involuntary

Residual Fingerprint → Enhancing ← Cyanoacrylate Adhesive

Enhancing → Capturing ←

Capturing → Image Processing ← Adobe Photoshop 6.0

Fingerprint Image → Printing ← Transparent Film

Printing → Mask

Mask → Exposing ← UV light

Exposing ← Photosensitive Coated PCB

Exposing → Developing

Developing → Etching

Etching → Mold

Digital Microscope

KEYENCE VH6300: 900k pixels

Inkjet Printer

Canon BJ-F800: 1200x600dpi

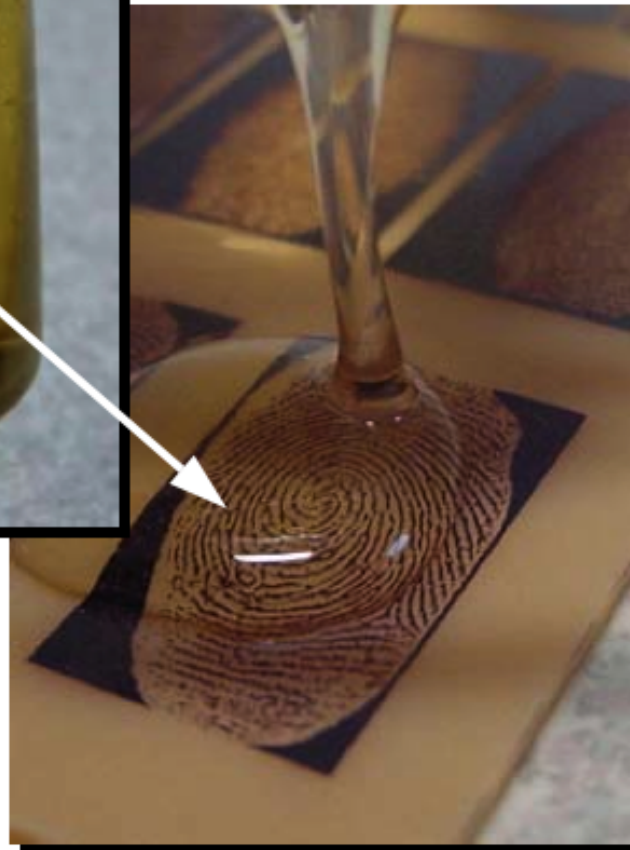http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Involuntary

[Matsumoto]

Gelatin Liquid

40wt.%
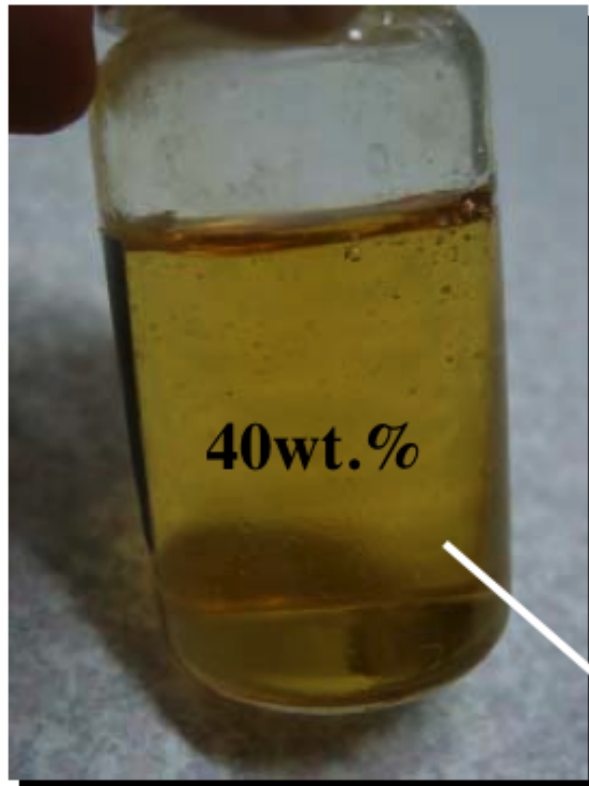
Drip the liquid onto the mold.

Put this mold into a refrigerator to cool, and then peel carefully.

http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Involuntary

http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf
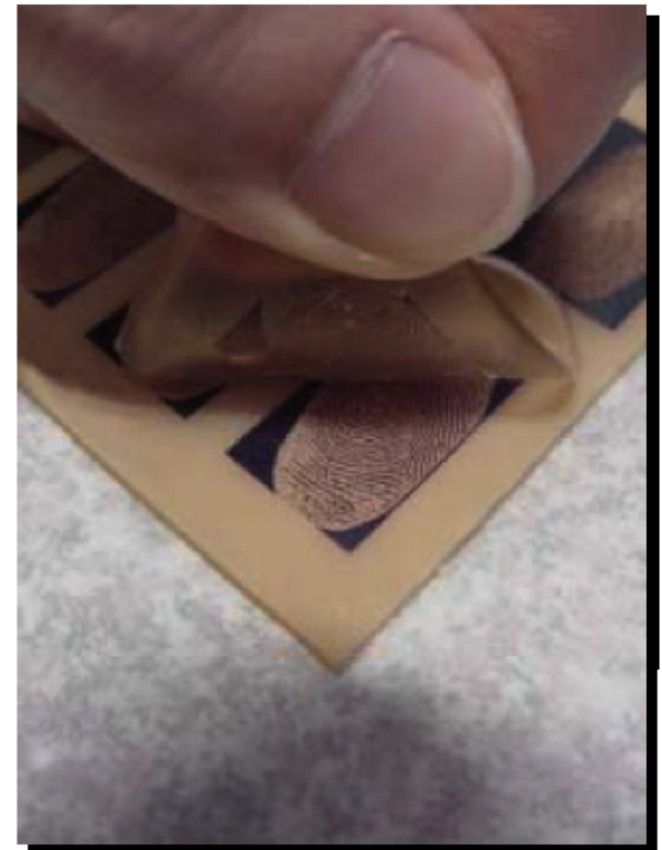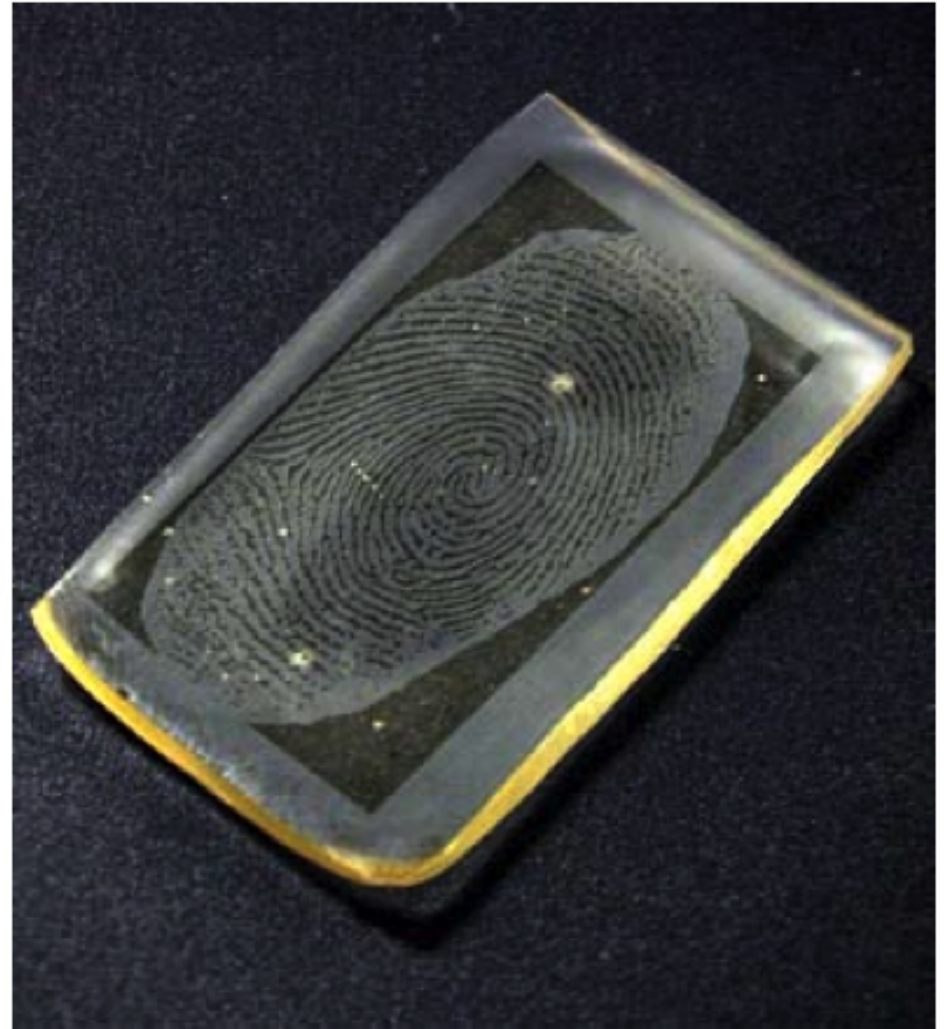
Authentication by Handwriting

◆ Maybe a computer could also forge some biometrics

Generated by computer algorithm trained on handwriting samples