Chapter 03: Authentication & Access Control

Information Security

Nguyễn Đăng Quang

Goals

Understand

Understand the importance of authentication,

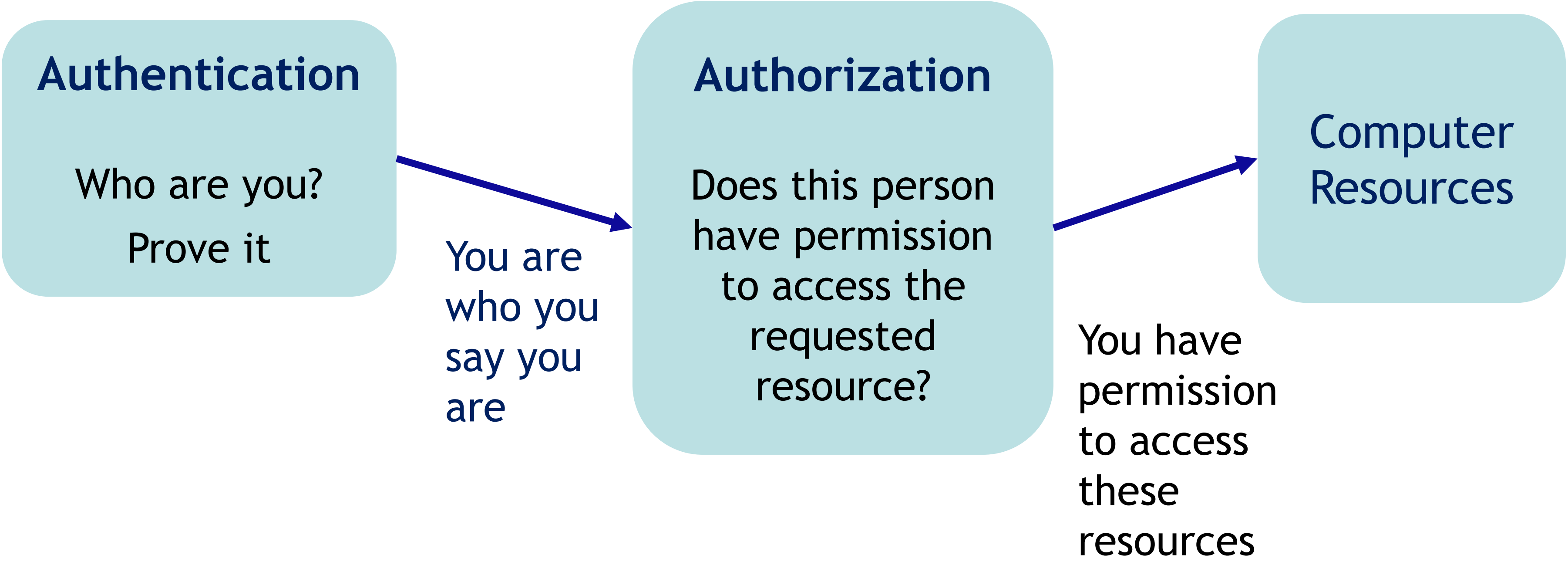
Learn

Learn how authentication can be implemented,

Understand

Understand threats to the authentication.

What is Authentication?



Authentication

Who are you?

Prove it

You are who you say you are

Authorization

Does this person have permission to access the requested resource?

You have permission to access these resources

Computer Resources

What is Authentication?

- Authentication helps us to answer the question: on whose behalf the requesting process runs?
- Includes claims about an identity and verification of the claimed identity of the user who wants to gain access to system and resource.

Authentication goals

- User/principal associated with an identity should be able to successfully authenticate itself
  - Availability
  - No false negatives
- User/principal not associated with an identity should not be able to authenticate itself
  - Authenticity
  - No false positives

Three types of Authentication

- **Knowledge-based:**
  Something a user knows

- **Possession-based:**
  Something a user has

- **Inheritance-based:**
  Something a user is

Authentication factors

- Single-factor authentication
- Two-factor authentication
- Two-factor authentication

The Importance of a Trusted Path

- The path connecting you and the TCB
- Trusted path is provided by

The OS

Or

The combination of hardware and OS

Example:

Ctrl – Alt –Del

Keyboard + Display + OS ➔ Trusted path

Password authentication

Something you know

What is password authentication?

- Password authentication is a process that involves a user inputting a unique ID and key that are then checked against stored credentials.
- Why is “something you know” more popular than “something you have” and “something you are”?
- **Cost**: passwords are free
- **Convenience**: easier for system administrator to reset password than to issue a new thumb

Trouble with Passwords?

“PASSWORDS ARE ONE OF THE BIGGEST PRACTICAL PROBLEMS FACING SECURITY ENGINEERS TODAY.”

“HUMANS ARE INCAPABLE OF SECURELY STORING HIGH-QUALITY CRYPTOGRAPHIC KEYS, AND THEY HAVE UNACCEPTABLE SPEED AND ACCURACY WHEN PERFORMING CRYPTOGRAPHIC OPERATIONS”

Keys vs Passwords

Crypto keys

- Key is 64 bits
- Then 2^{64} keys
- Choose key at random…
- …then attacker must try about 2^{63} keys

Passwords

- Passwords are 8 characters, and 256 different characters
- Then $256^8 = 2^{64}$ pwds
- Users do not select passwords at random
- Attacker has far less than 2^{63} pwds to try (**dictionary attack**)

Password Experiment

Three groups of users — each group advised to select passwords as follows

- **Group A:** At least 6 chars, 1 non-letter
- **Group B:** Password based on passphrase
- **Group C:** 8 random characters

Results

- **Group A:** About 30% of passwords easy to crack
- **Group B:** About 10% cracked, passwords easy to remember
- **Group C:** About 10% cracked, Passwords hard to remember

Best Advice

- Choose passwords based on passphrase
- Use password cracking tools to test for weak passwords

What are password alternatives

- Any sort of authentication protocol that doesn’t utilize a typical ID and key to grant user’s access
- Often fall into possession or inheritance-based methods

Implementing Password Authentication

Password-based Authentication

Method 1:

- Store a list of passwords, one for each user in a system file.
- The file is readable only by root/admin account.

Disadvantages

- If the permissions are set incorrectly, another person can read it.
- If the security is breached, the passwords are exposed to the attacker.

Password-based Authentication

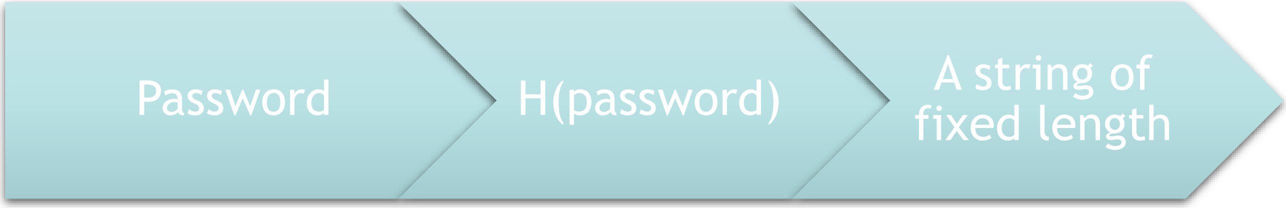
Method 2:

- Do not store passwords but stored something derived from them.

Implementation

- Use one-way hash function and store the result.
- The password file is only readable to root/admin

Cryptographic Hash function



Password

H(password)

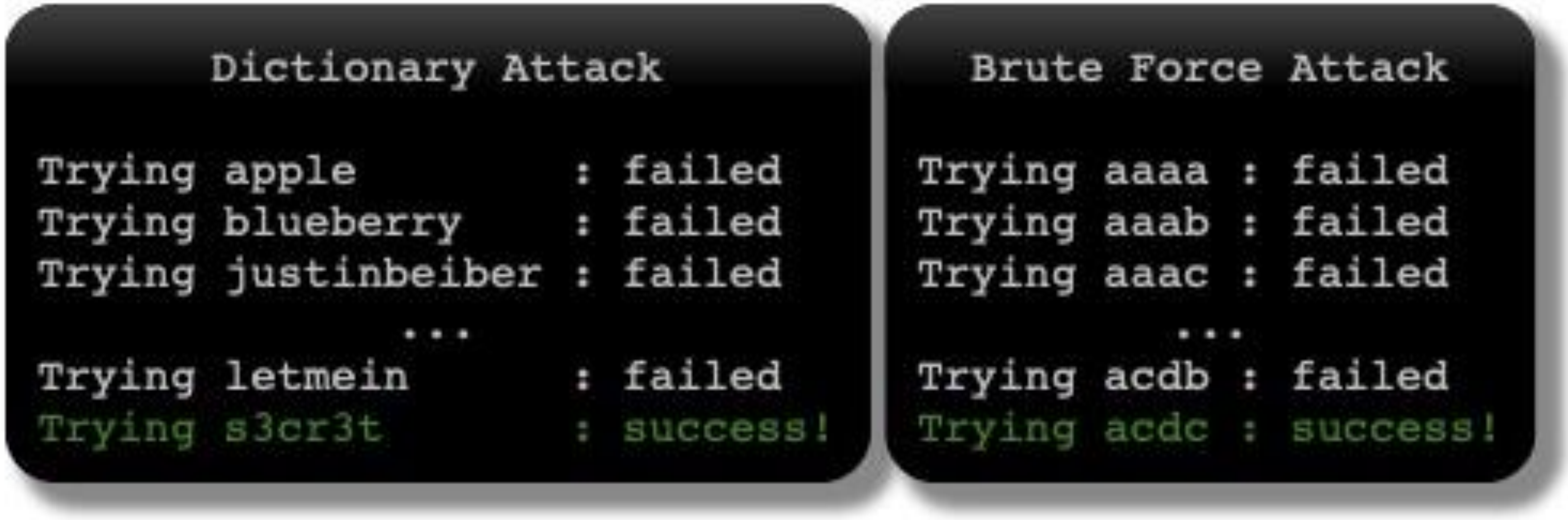
A string of fixed length

Features of hash function

- Pre-Image resistance:
  Its inverse should be very hard to compute.
- Collision Resistance (Collision Free):
  It should be hard to find two different inputs of any length that result in the same hash.

How hashes are cracked

Dictionary & Brute Force



```
      Dictionary Attack

Trying apple         : failed
Trying blueberry     : failed
Trying justinbeiber  : failed
            ...
Trying letmein       : failed
Trying s3cr3t        : success!
```

```
  Brute Force Attack

Trying aaaa : failed
Trying aaab : failed
Trying aaac : failed
        ...
Trying acdb : failed
Trying acdc : success!
```

How hashes are cracked

Lookup table

An extremely effective method for cracking many hashes of the same type very quickly.

The general idea is to **pre-compute** the hashes of the passwords in a password dictionary and store them, and their corresponding password, in a lookup table data structure. A good implementation of a lookup table can process hundreds of hash lookups per second, even when they contain many billions of hashes

Brute Force Guessing of Passwords

A 2013 attack by Xie Tao, Fanbao Liu, and Dengguo Feng breaks MD5 collision resistance in 2^{18} time (128-bit hash value). This attack runs in less than a second on a regular computer.

Password with 6 random uppercase, lowercase, and digits, there will be 62^6 possible passwords and can be guessed in about 10 minutes.

Password with 8 random characters will require about six days to guess the password.

Salt

Hash password with **salt**

Choose random salt s and compute

$$y = h(password, s)$$

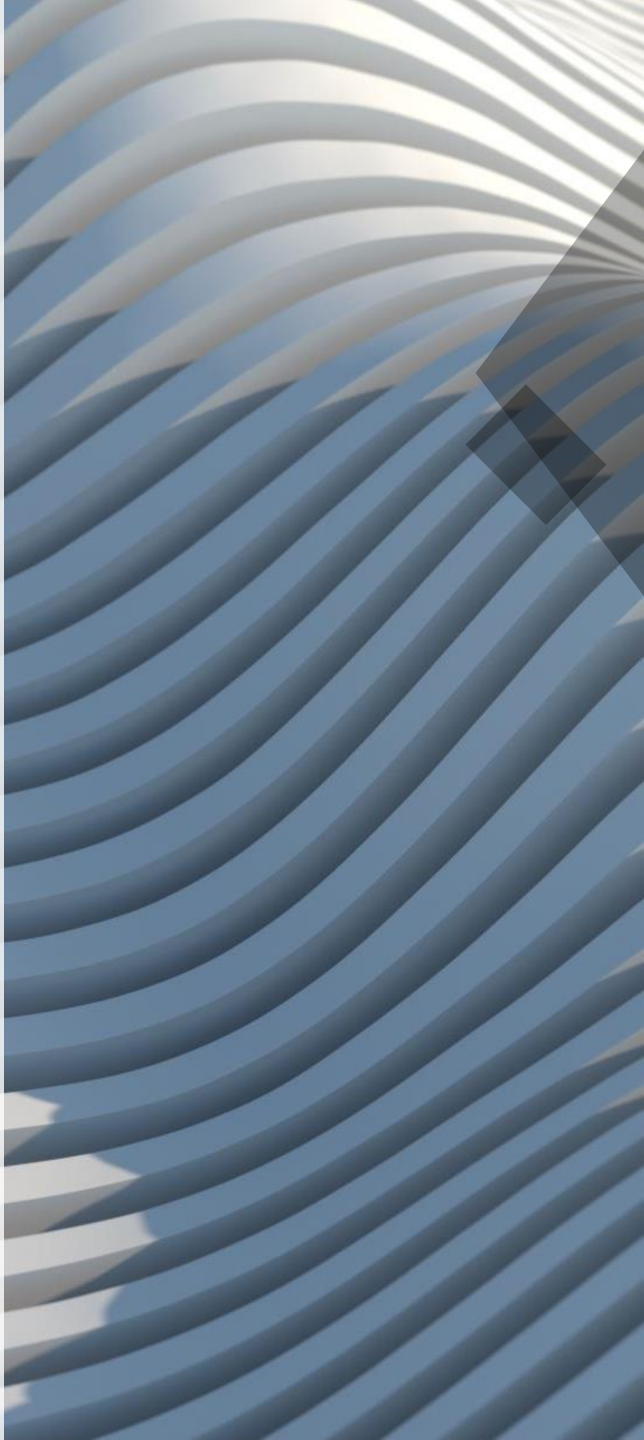
and store (s,y) in the password file

Uname	Password
user1	password123
user2	password123

Uname	Salt Value	Hashed Value = SHA256 (Password + Salt Value)
user1	E1F53135E559C253	72ae25495a7981c40622d49f9a52e4f1565c90f048f59027bd9c8c8900d5c3d8
user2	84B03D034B409D4E	b4b6603abc670967e99c7e7f1389e40cd16e78ad38eb1468ec2aa1e62b8bed3a

Password vulnerabilities

- Offline dictionary attack
- Specific account attack (user john)
- Popular password attack (against a wide range of IDs)
- Password guessing against single user (w/ previous knowledge about the user)
- Workstation hijacking
- Exploiting user mistakes
- Exploiting multiple password use
- Electronic monitoring (eavesdropping)



Password vulnerabilities

Stop unauthorized access to password file

Intrusion detection measures

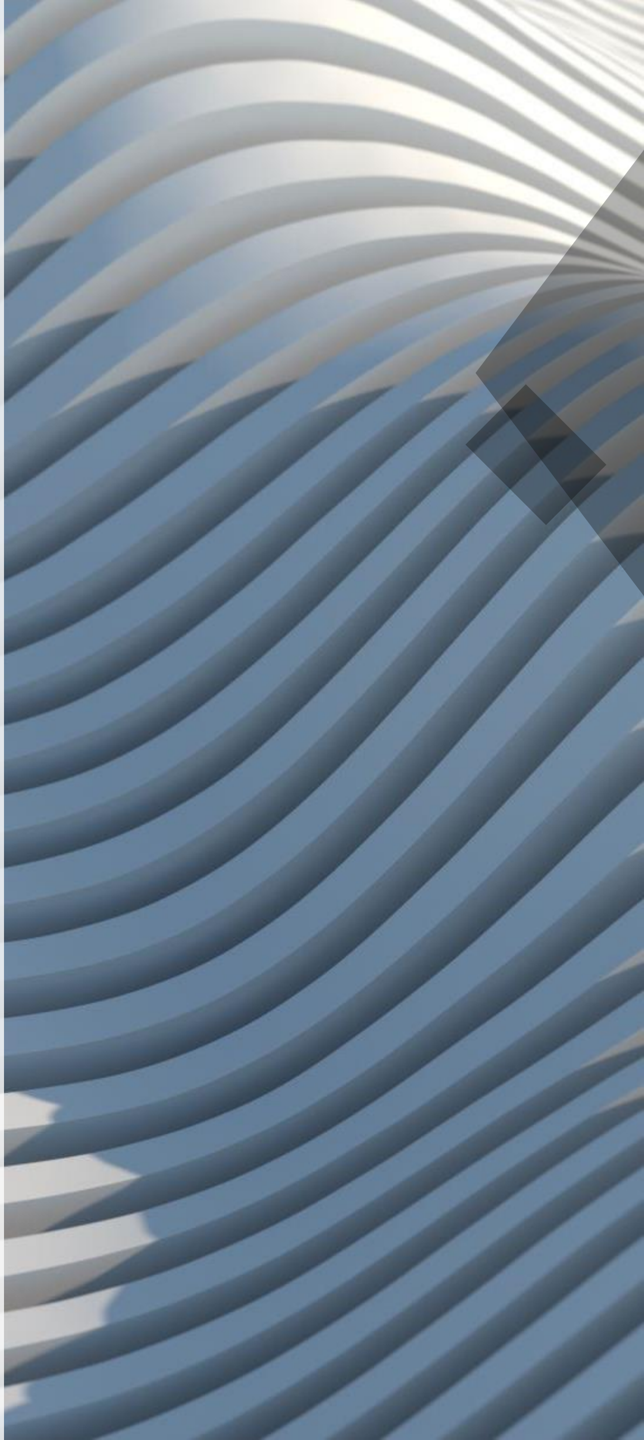
Account lockout mechanisms

Policies against using common passwords but rather hard to guess passwords

Training & enforcement of policies

Automatic workstation logout

Encrypted network links



Other password issues

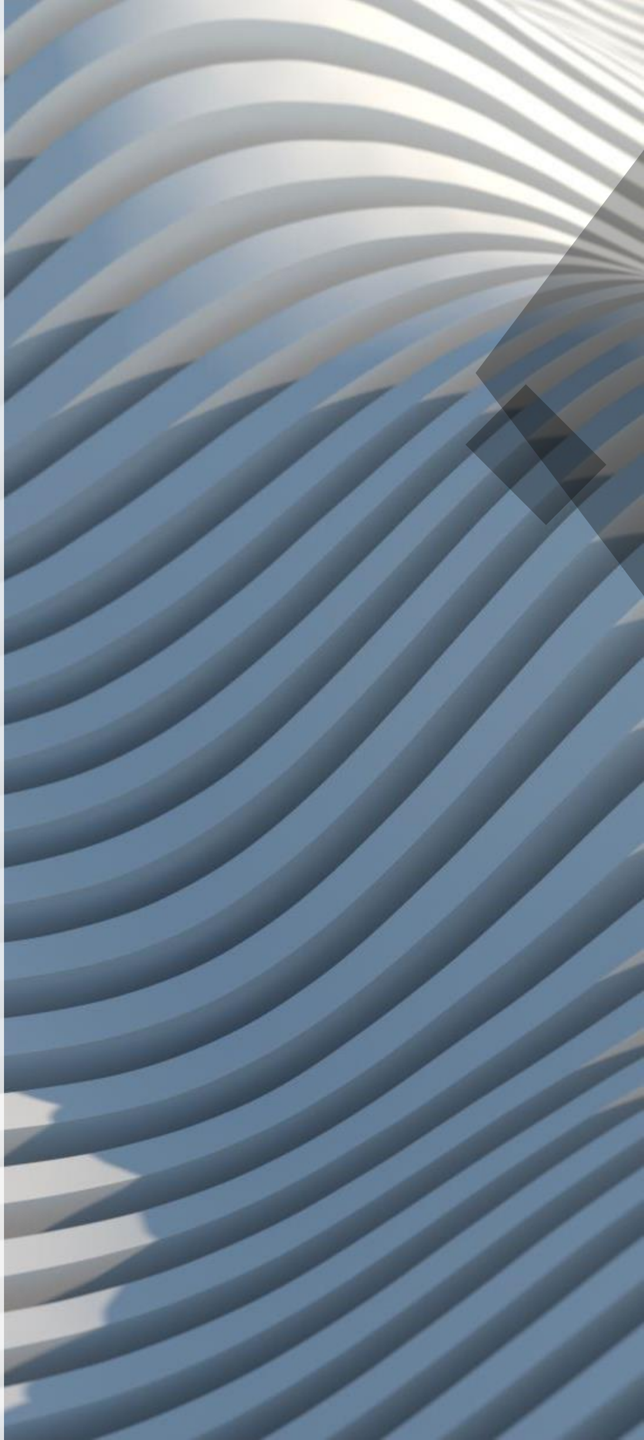
Too many passwords to remember: Results in password reuse

Failure to change default passwords

Social engineering

Error logs may contain “almost” passwords

Bugs, keystroke logging, spyware, etc.



Passwords

The bottom line…

- Password attacks are too easy
  - Often, one weak password will break security
  - Users choose bad passwords
  - Social engineering attacks, etc.
- Passwords are a **BIG** security problem
  - And will continue to be a problem

Password Cracking Tools

- Popular password cracking tools
  - Password Crackers
  - Password Portal
  - L0phtCrack and LC4 (Windows)
  - John the Ripper (Unix)
- Admins should use these tools to test for weak passwords since attackers will
- Good articles on password cracking
  - Passwords - Conerstone of Computer Security
  - Passwords revealed by sweet deal

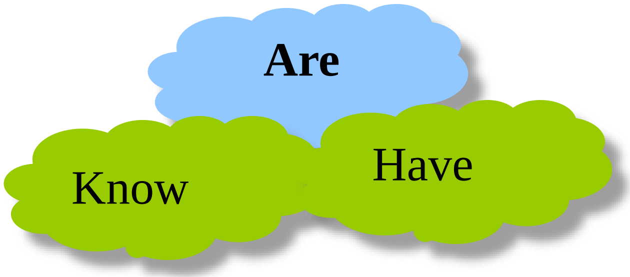
Biometrics

Something You Are

- Biometric
  - "You are your key" — Schneier

Examples

- ○ Fingerprint
- ○ Handwritten signature
- ○ Facial recognition
- ○ Speech recognition
- ○ Gait (walking) recognition
- ○ . . .



Enrollment vs Recognition

Enrollment phase

Subject's biometric info put into database

Must carefully measure the required info

OK if slow and repeated measurement needed

Must be very precise

May be a weak point in real-world use

Recognition phase

Biometric detection, when used in practice

Must be quick and simple

But must be reasonably accurate

Performance

False accept rate (FAR), or *fraud rate*: what percentage of times an invalid user is accepted by the system (false accept):
e.g. Trudy mis-authenticated as Alice

False rejection rate (FRR) or *insult rate*: the percentage of times a valid user is rejected by the system (false reject):
e.g. Alice not authenticated as Alice

Failure to enroll rate (FTE or FER).

Problems with Biometrics

Private, but not secret

Biometric passports, fingerprints and DNA on objects…

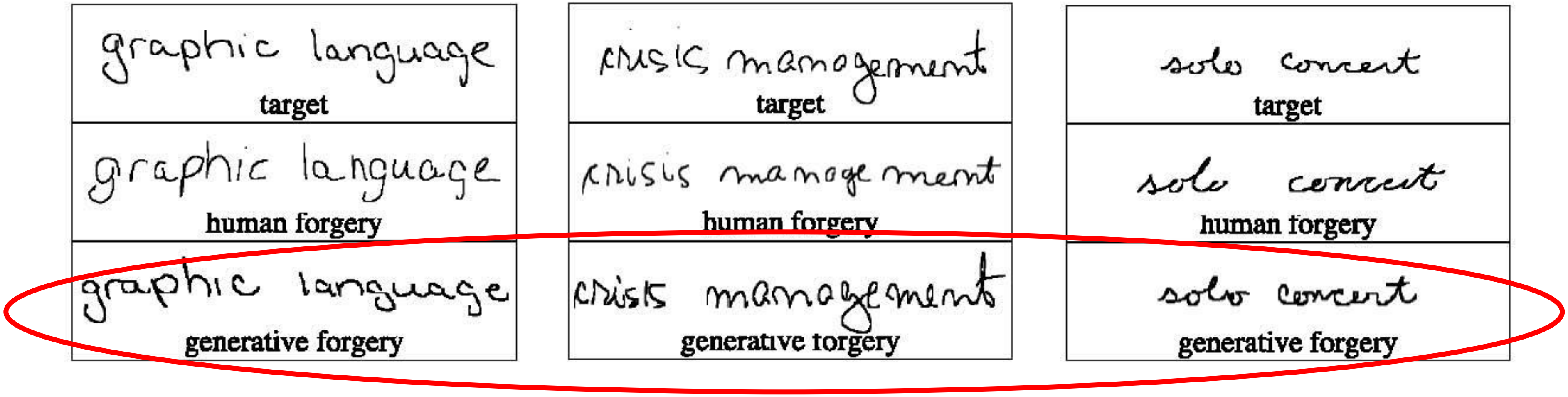
Even random-looking biometrics may not be sufficiently unique for authentication

Birthday paradox!

Potentially forgeable

Forging Handwriting

[Ballard, Monrose, Lopresti]



Generated by computer algorithm trained on handwriting samples

Biometrics

Face recognition (by a computer algorithm)

- Error rates up to 20%, given 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 a false match is 1 in 10 billion
  - No successful challenges until 2000

Biometrics

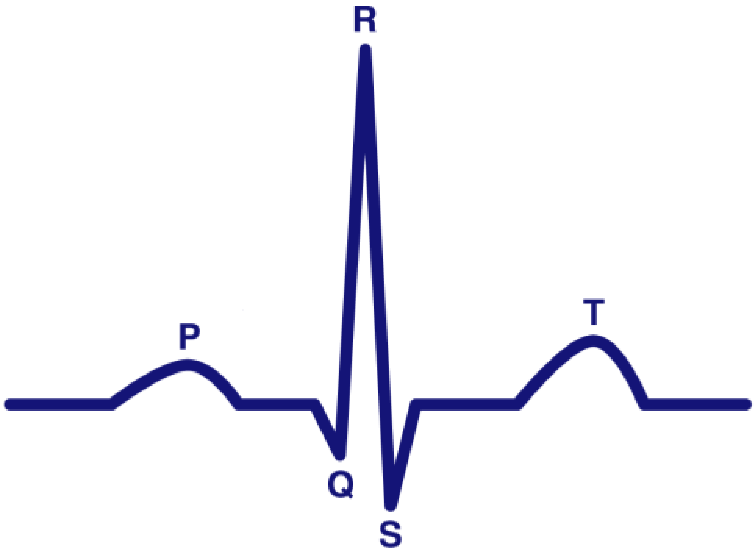
Iris scanning

- 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

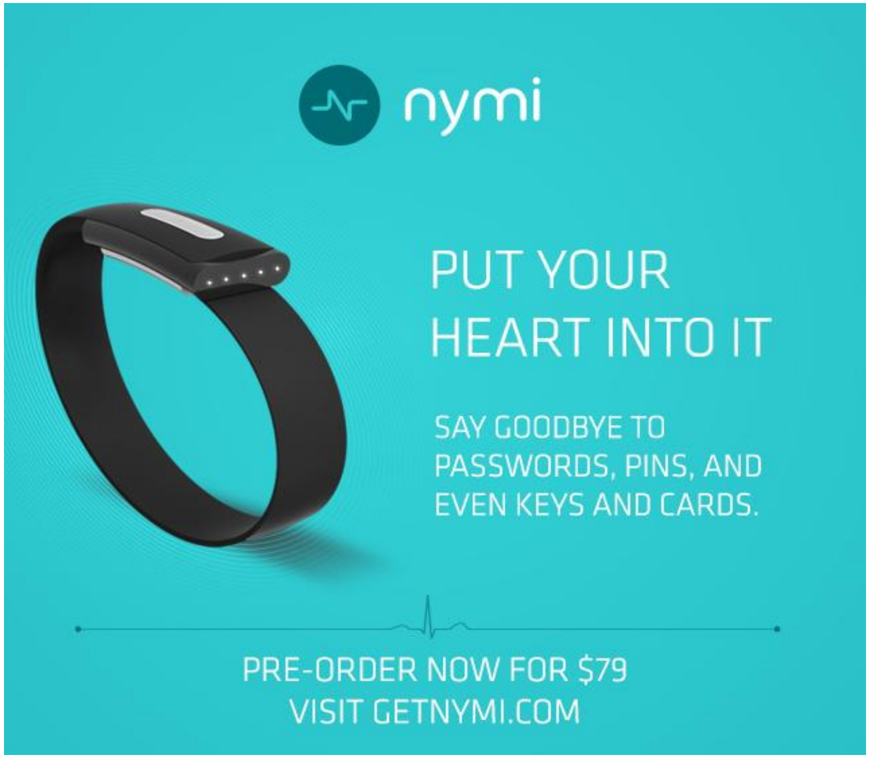
Voice, ear shape, vein pattern, face temperature

Biometrics

- Identifies wearer
- By his/her unique heartbeat pattern



Agateller for Wikipedia
Public Domain



nymi

PUT YOUR
HEART INTO IT

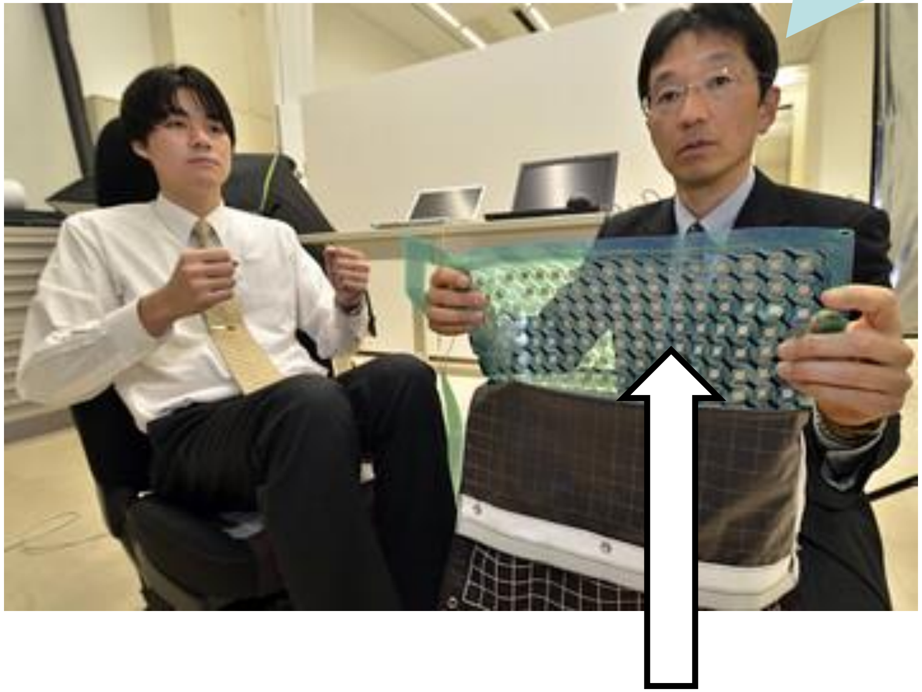
SAY GOODBYE TO
PASSWORDS, PINS, AND
EVEN KEYS AND CARDS.

PRE-ORDER NOW FOR $79
VISIT GETNYMI.COM

Biometrics

“All you need to do is sit”

[Advanced Institute of Industrial Technology, Japan]



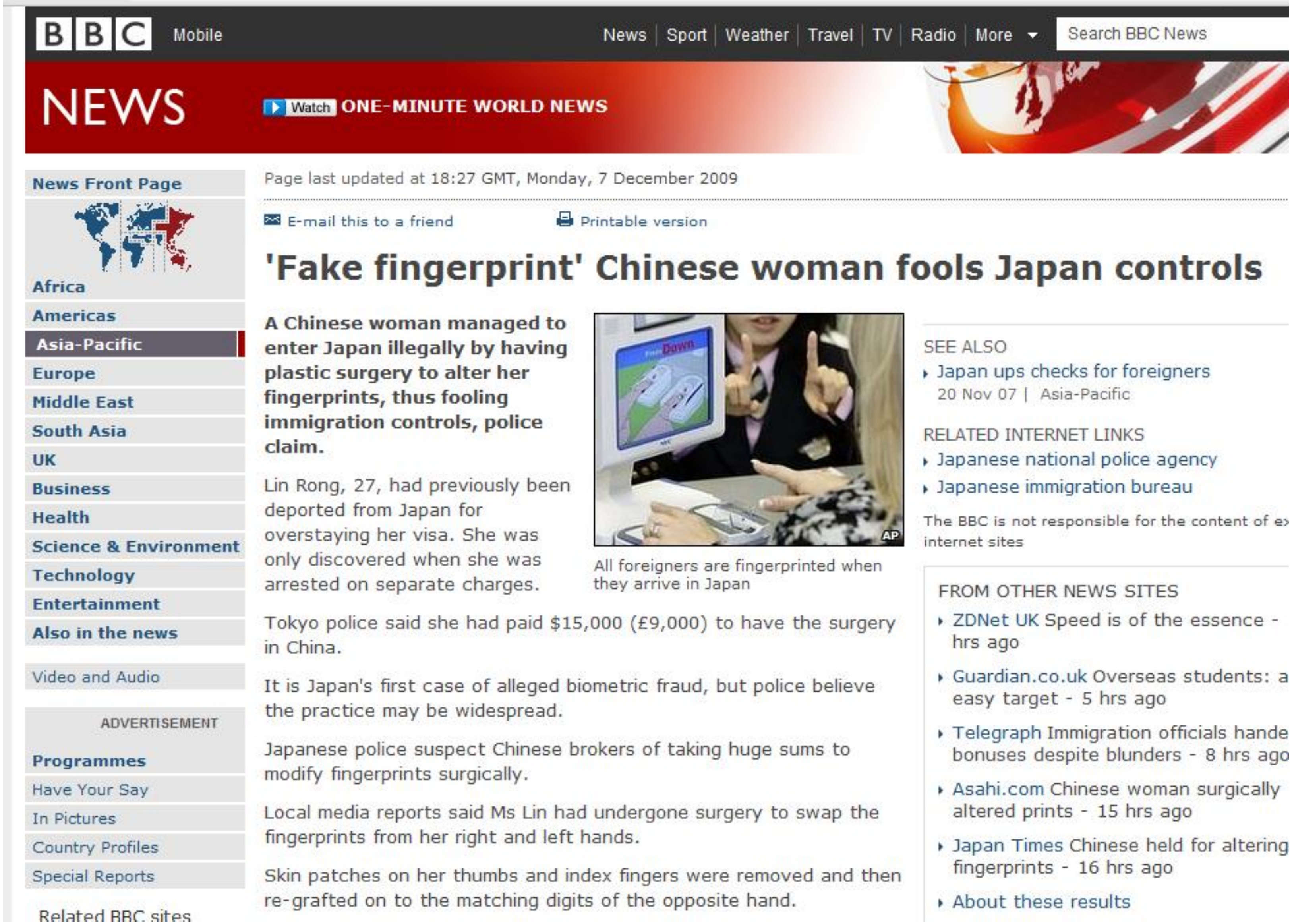
¥70,000

“Forget Fingerprints: Car Seat IDs Driver’s Rear End”

360 disc-shaped sensors identify a unique “buttprint” with 98% accuracy

Risks of Biometrics

Surgical Change



BBC
Mobile
News | Sport | Weather | Travel | TV | Radio | More
Search BBC News
NEWS
Watch ONE-MINUTE WORLD NEWS

Page last updated at 18:27 GMT, Monday, 7 December 2009

'Fake fingerprint' Chinese woman fools Japan controls

A Chinese woman managed to enter Japan illegally by having plastic surgery to alter her fingerprints, thus fooling immigration controls, police claim.

Lin Rong, 27, had previously been deported from Japan for overstaying her visa. She was only discovered when she was arrested on separate charges.

All foreigners are fingerprinted when they arrive in Japan

Tokyo police said she had paid $15,000 (£9,000) to have the surgery in China.

It is Japan's first case of alleged biometric fraud, but police believe the practice may be widespread.

Japanese police suspect Chinese brokers of taking huge sums to modify fingerprints surgically.

Local media reports said Ms Lin had undergone surgery to swap the fingerprints from her right and left hands.

Skin patches on her thumbs and index fingers were removed and then re-grafted on to the matching digits of the opposite hand.

SEE ALSO

- Japan ups checks for foreigners
  20 Nov 07 | Asia-Pacific

RELATED INTERNET LINKS

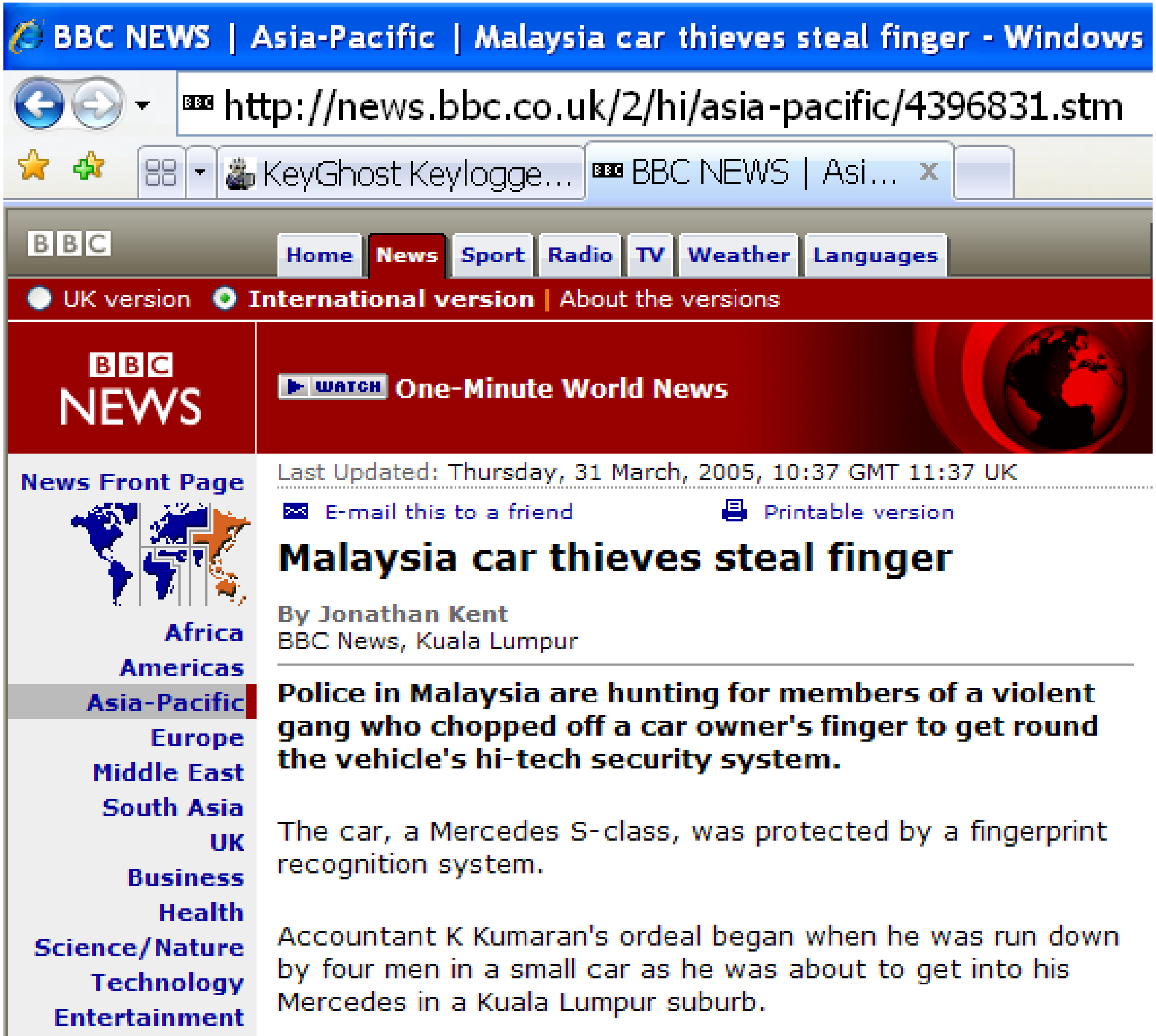
- Japanese national police agency
- Japanese immigration bureau

The BBC is not responsible for the content of ex internet sites

FROM OTHER NEWS SITES

- ZDNet UK Speed is of the essence - hrs ago
- Guardian.co.uk Overseas students: a easy target - 5 hrs ago
- Telegraph Immigration officials hande bonuses despite blunders - 8 hrs ago
- Asahi.com Chinese woman surgically altered prints - 15 hrs ago
- Japan Times Chinese held for altering fingerprints - 16 hrs ago
- About these results

Stealing Biometrics



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

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

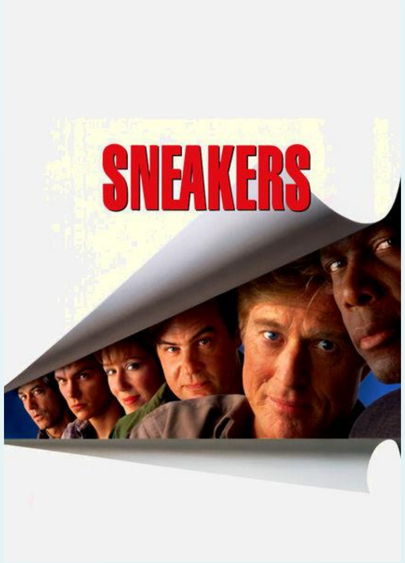
Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

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

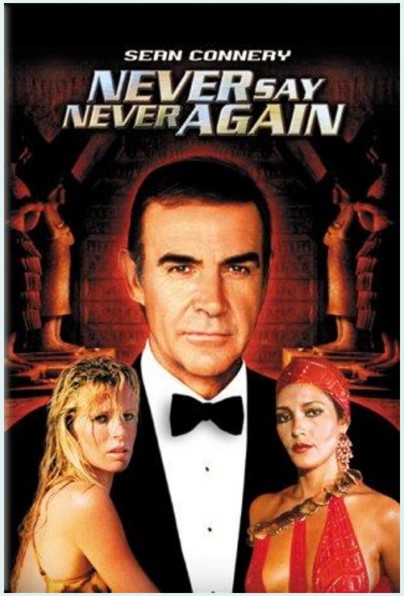
Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.

Involuntary Cloning

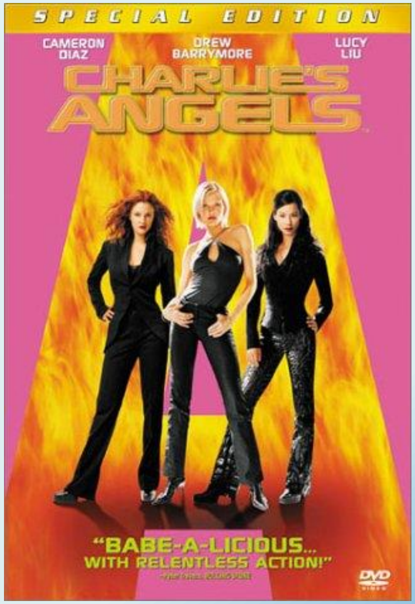
Clone a biometric without victim’s knowledge or assistance



“my voice is my password”



cloned retina

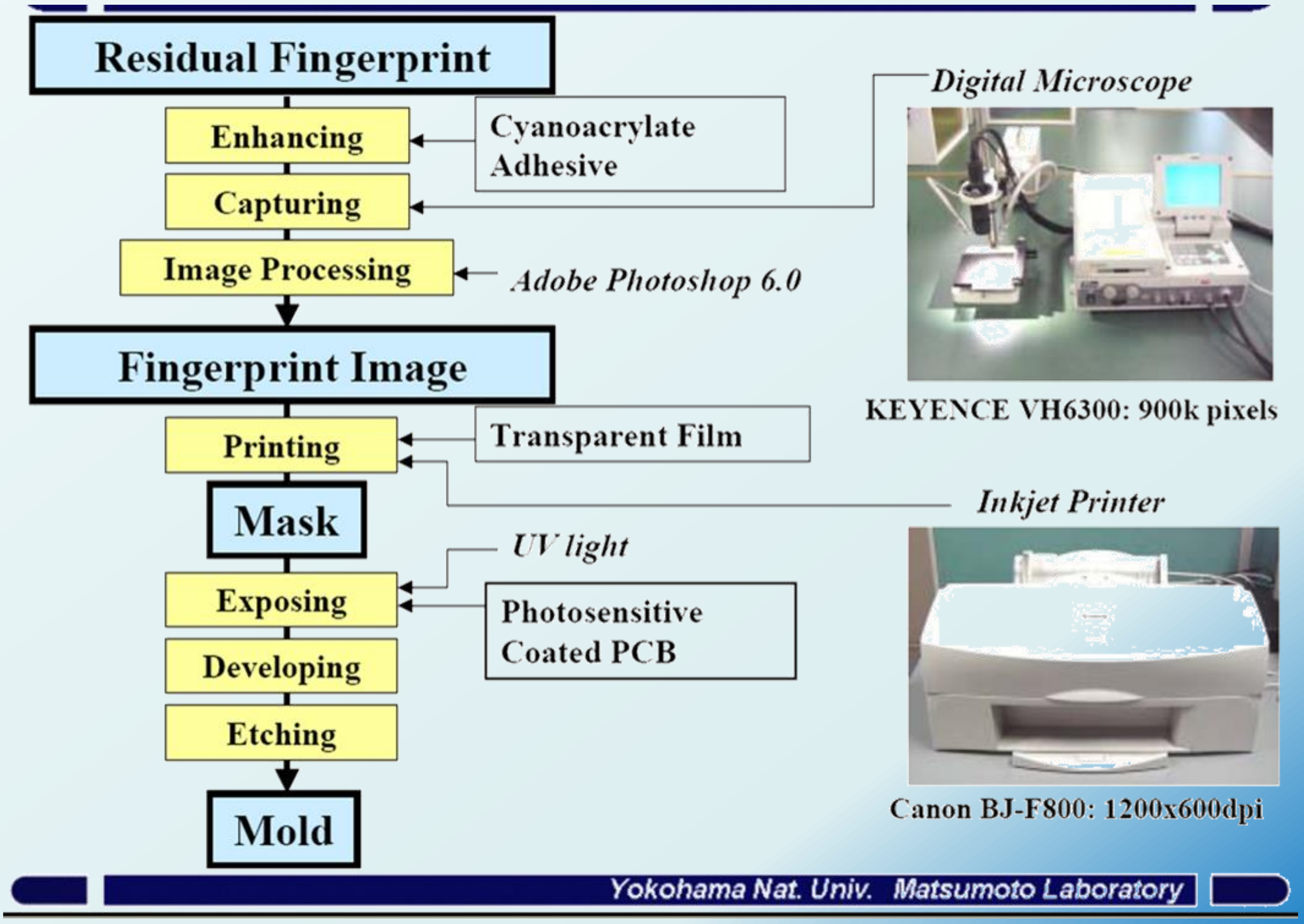


Fingerprints from beer bottles

Eye laser scan

Bad news: it works!

Cloning Process (Involuntary)



Residual Fingerprint

Enhancing

Capturing

Image Processing

Fingerprint Image

Printing

Mask

Exposing

Developing

Etching

Mold

Cyanoacrylate Adhesive

Digital Microscope

Adobe Photoshop 6.0

KEYENCE VH6300: 900k pixels

Transparent Film

Inkjet Printer

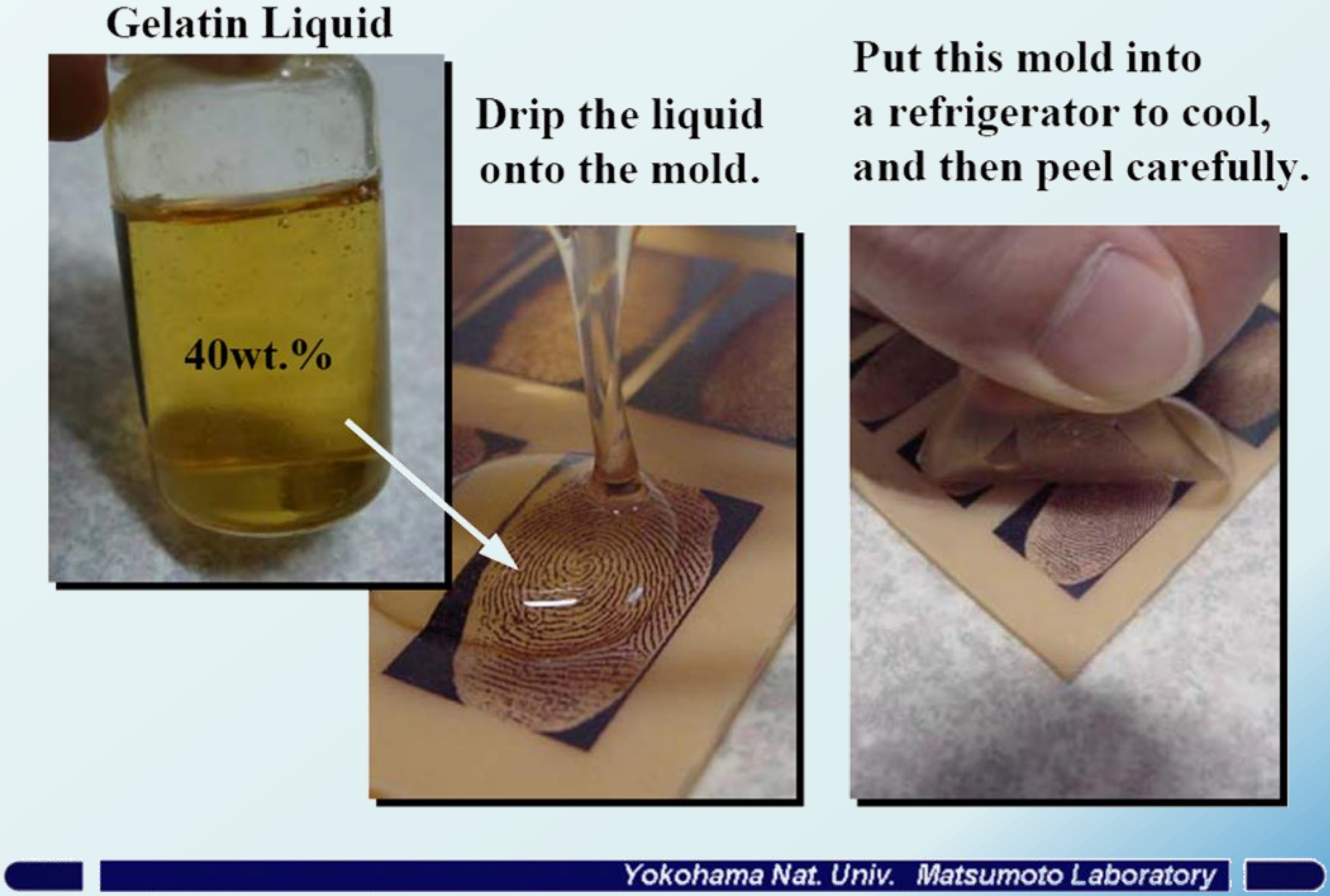
UV light

Photosensitive Coated PCB

Canon BJ-F800: 1200x600dpi

Yokohama Nat. Univ. Matsumoto Laboratory

Molding (Involuntary)



Gelatin Liquid

Drip the liquid onto the mold.

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

Yokohama Nat. Univ. Matsumoto Laboratory

Making a Mold (Voluntary)

[Matsumoto]

Put the plastic into hot water to soften it.

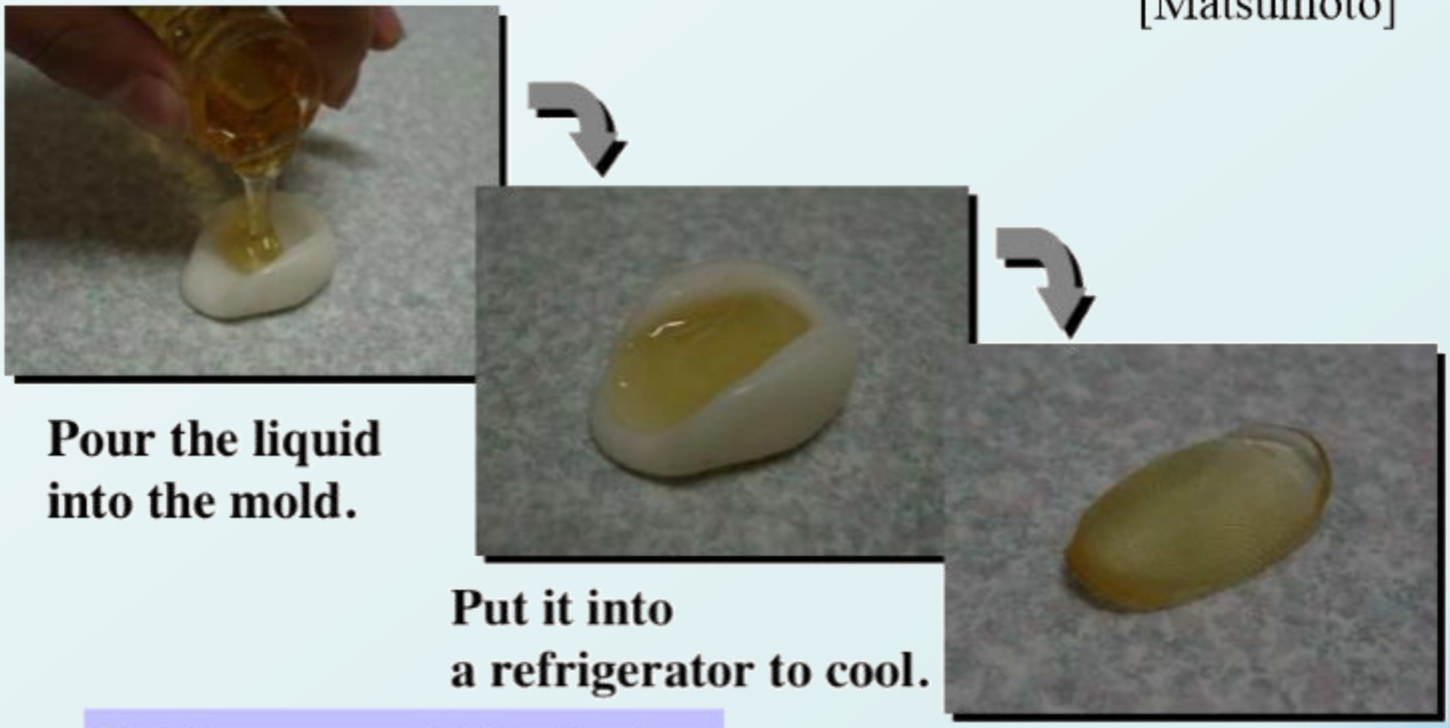
Press a live finger against it.

The mold

It takes around 10 minutes.

Making a Finger (Voluntary)

[Matsumoto]



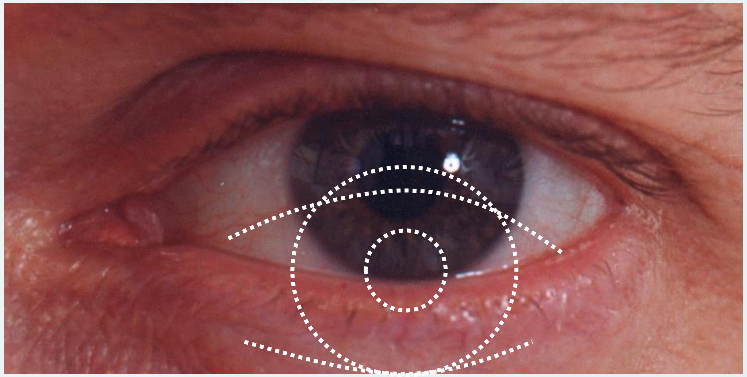
Pour the liquid
into the mold.

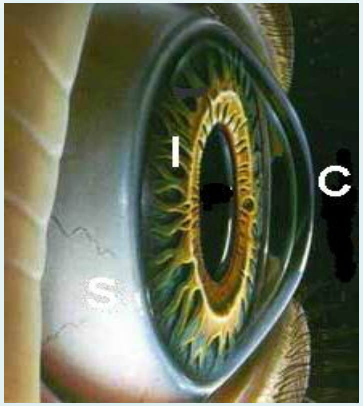
Put it into
a refrigerator to cool.

The gummy finger

It takes around 10 minutes.

Iris Patterns

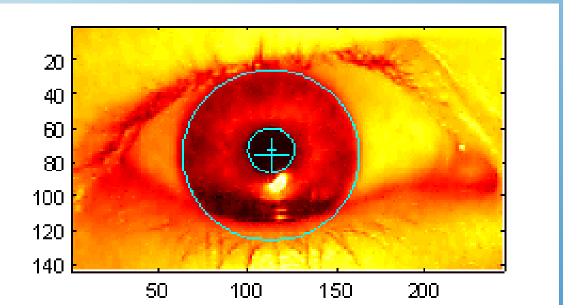


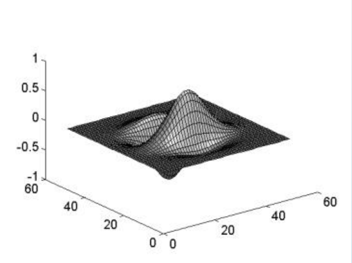


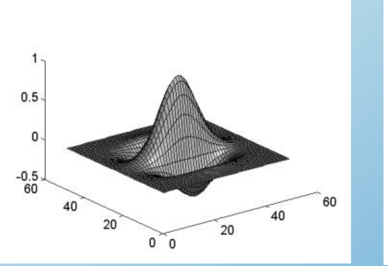
- Iris pattern development is “chaotic”
- Little or no genetic influence
- Even for identical twins, uncorrelated
- Pattern is stable through lifetime

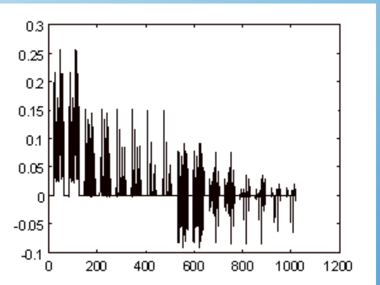
Iris Scan

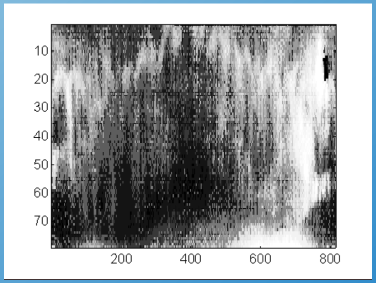
- Scanner locates iris
- Take b/w photo
- Use polar coordinates…
- 2-D wavelet transform
- Get 256 byte iris code











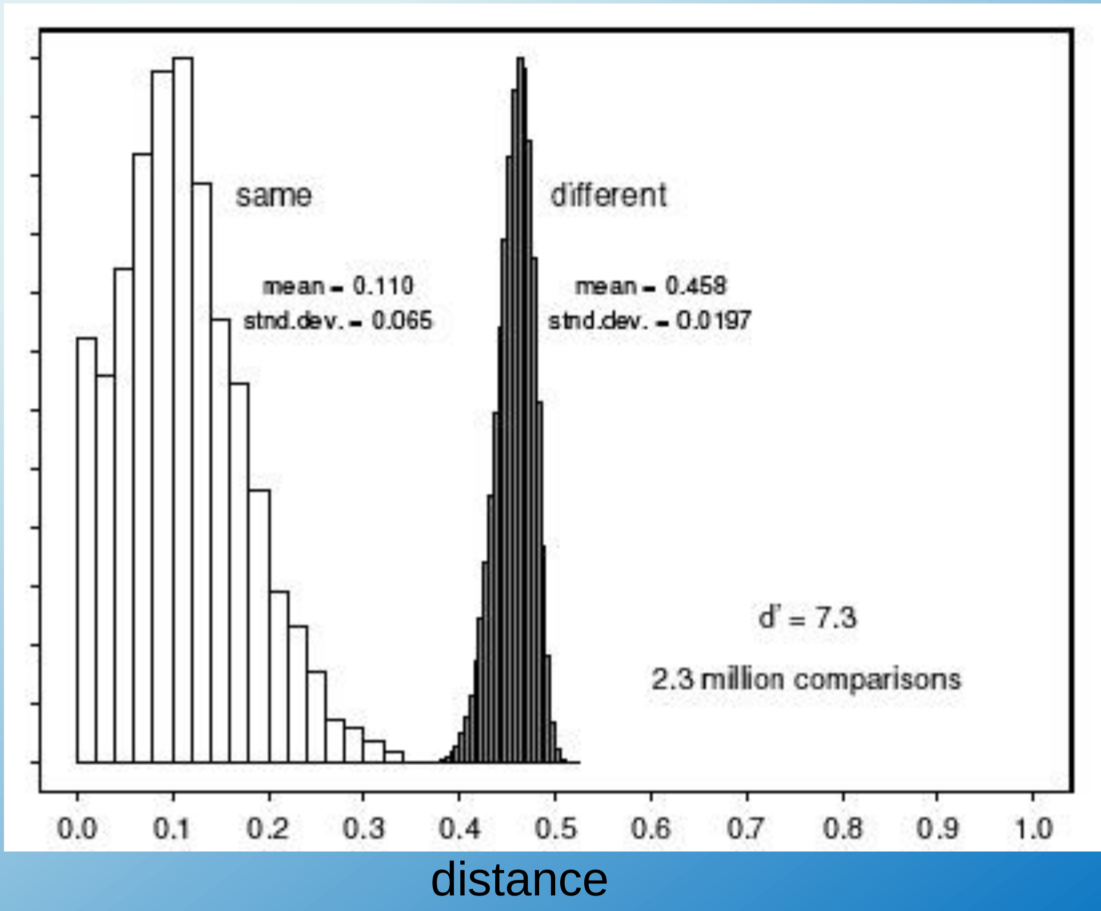
Measuring Iris Similarity

- Based on Hamming distance
- Define $d(x,y)$ to be
  - # of non-match bits / # of bits compared
  - $d(0010,0101) = 3/4$ and $d(101111,101001) = 1/3$
- Compute $d(x,y)$ on 2048-bit iris code
  - Perfect match is $d(x,y) = 0$
  - For same iris, expected distance is 0.08
  - At random, expect distance of 0.50
  - Accept iris scan as match if distance < 0.32

Iris Scan Error Rate

distance	Fraud rate
0.29	1 in $1.3*10^{10}$
0.30	1 in $1.5*10^{9}$
0.31	1 in $1.8*10^{8}$
0.32	1 in $2.6*10^{7}$
0.33	1 in $4.0*10^{6}$
✶ 0.34	1 in $6.9*10^{5}$
0.35	1 in $1.3*10^{5}$

✶ == equal error rate



Attack on Iris Scan

- Good **photo** of eye can be scanned
  - Attacker could use photo of eye
- ❑ Afghan woman was authenticated by iris scan of old photo
  - o Story can be found here
- ❑ To prevent attack, scanner could use light to be sure it is a “live” iris

Equal Error Rate Comparison

- Equal error rate (EER): fraud == insult rate
- **Fingerprint** biometrics used in practice have EER ranging from about 10^{-3} to as high as 5%
- **Hand geometry** has EER of about 10^{-3}
- In theory, **iris scan** has EER of about 10^{-6}
  - Enrollment phase may be critical to accuracy
- Most biometrics much worse than fingerprint!

Biometrics: The Bottom Line

- Biometrics are hard to forge
- But attacker could
  - Steal Alice’s thumb
  - Photocopy Bob’s fingerprint, eye, etc.
  - Subvert software, database, “trusted path” …
- And how to revoke a “broken” biometric?
- **Biometrics are not foolproof**
- Biometric use is relatively limited today
- That should change in the (near?) future