CSE 484 / CSE M 584 (Autumn 2011)

User Authentication and Human Factors

Daniel Halperin
Tadayoshi Kohno

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

Updates, 11/14

- Lab #2
  - Due ~~Friday~~ **next Monday, 11/21**
  - If you haven't, mail cse484-tas with group ASAP
- Generally: ***mail cse484-tas*** unless you really want only me to see the mail
  - I'm on that list too; better response time overall
- ***Look ahead:*** Second security review & current event due 12/2 (extra credit for every week early)

Multi-Factor Authentication

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

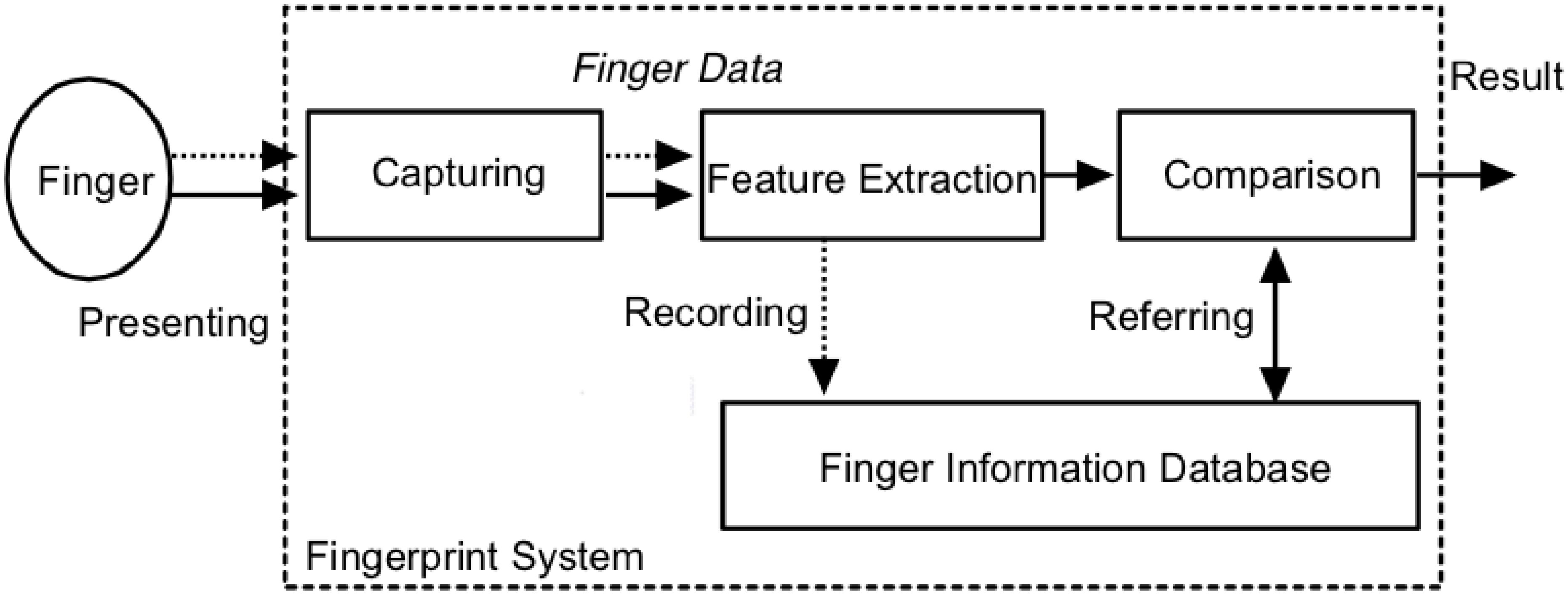
For better security, require **two or more factors:**

- 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

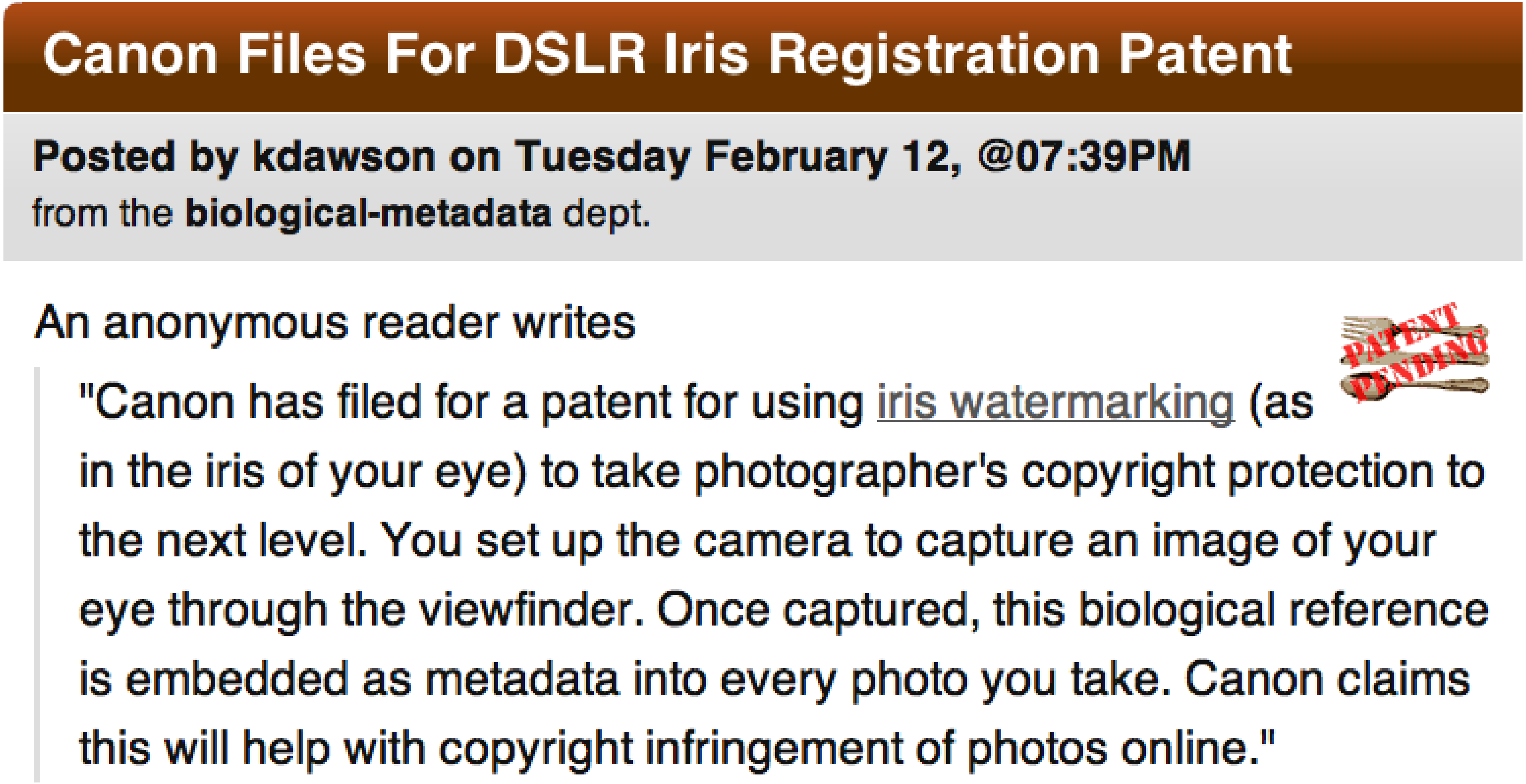
Other Biometrics

- 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?

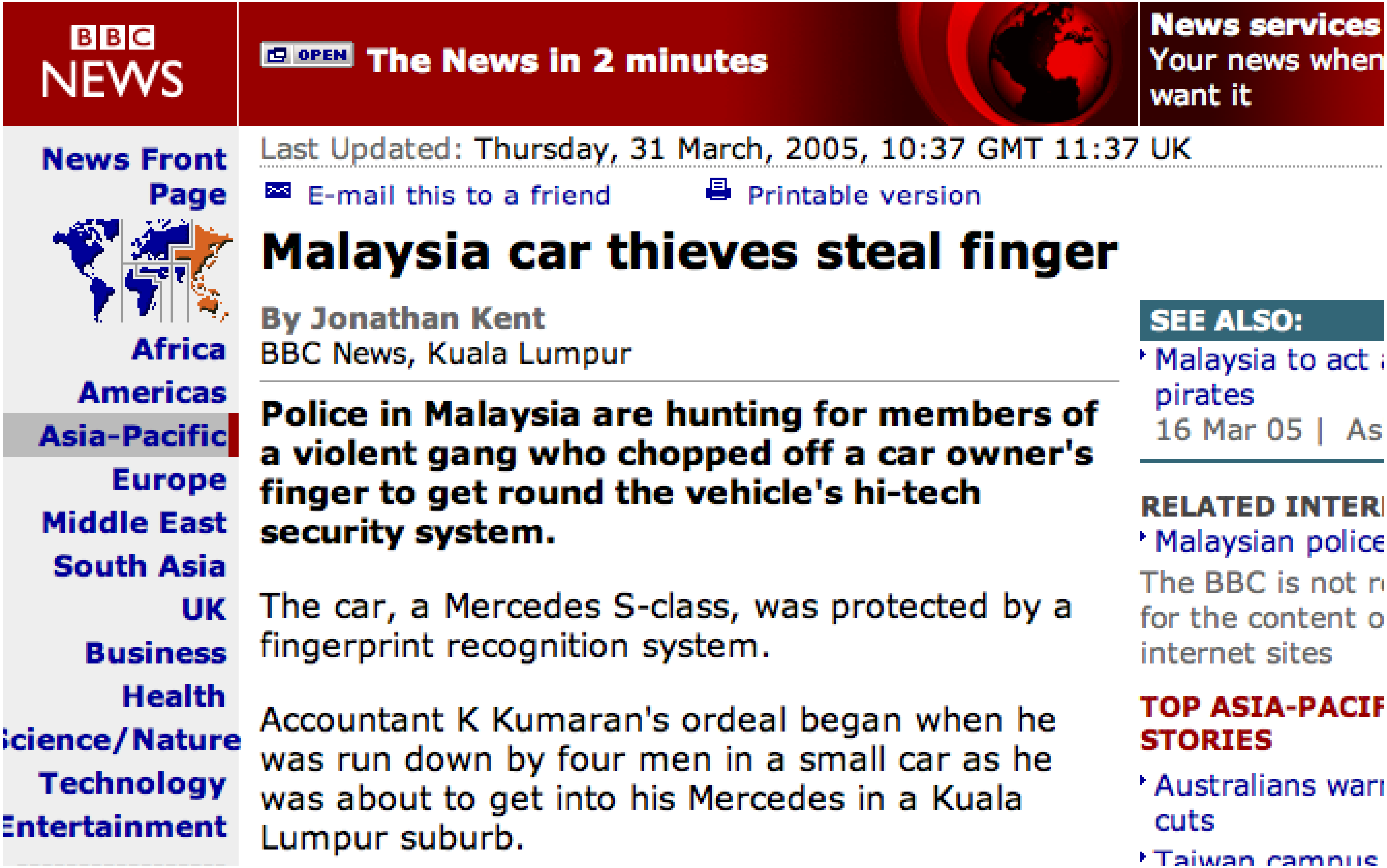
Issues with Biometrics

- 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



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.

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

RELATED INTERI
- Malaysian police

The BBC is not r for the content o internet sites

TOP ASIA-PACIF STORIES
- Australians warn cuts
- Taiwan campus

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

Biometric Error Rates (Adversarial)

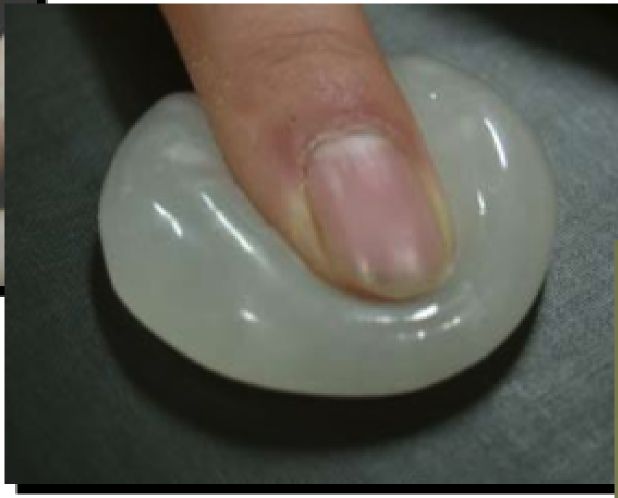
- Want to minimize “fraud” and “insult” rate
  - “Easy” to test probability of accidental misidentification (fraud)
  - But what about adversarial fraud

- 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

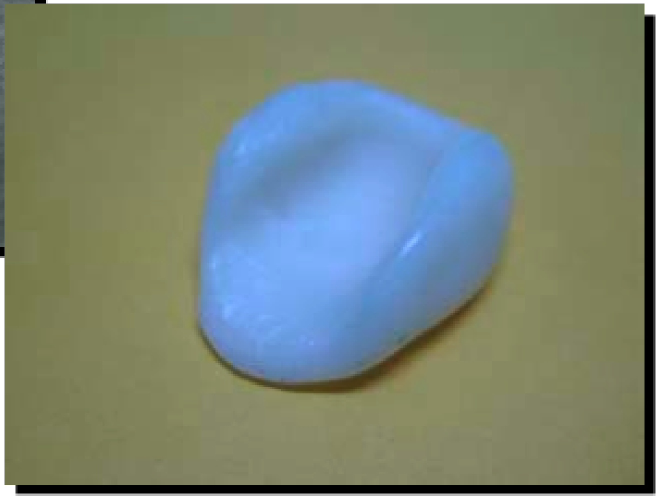
Voluntary: Making a Mold

[Matsumoto]

Put the plastic into hot water to soften it.



Press a live finger against it.



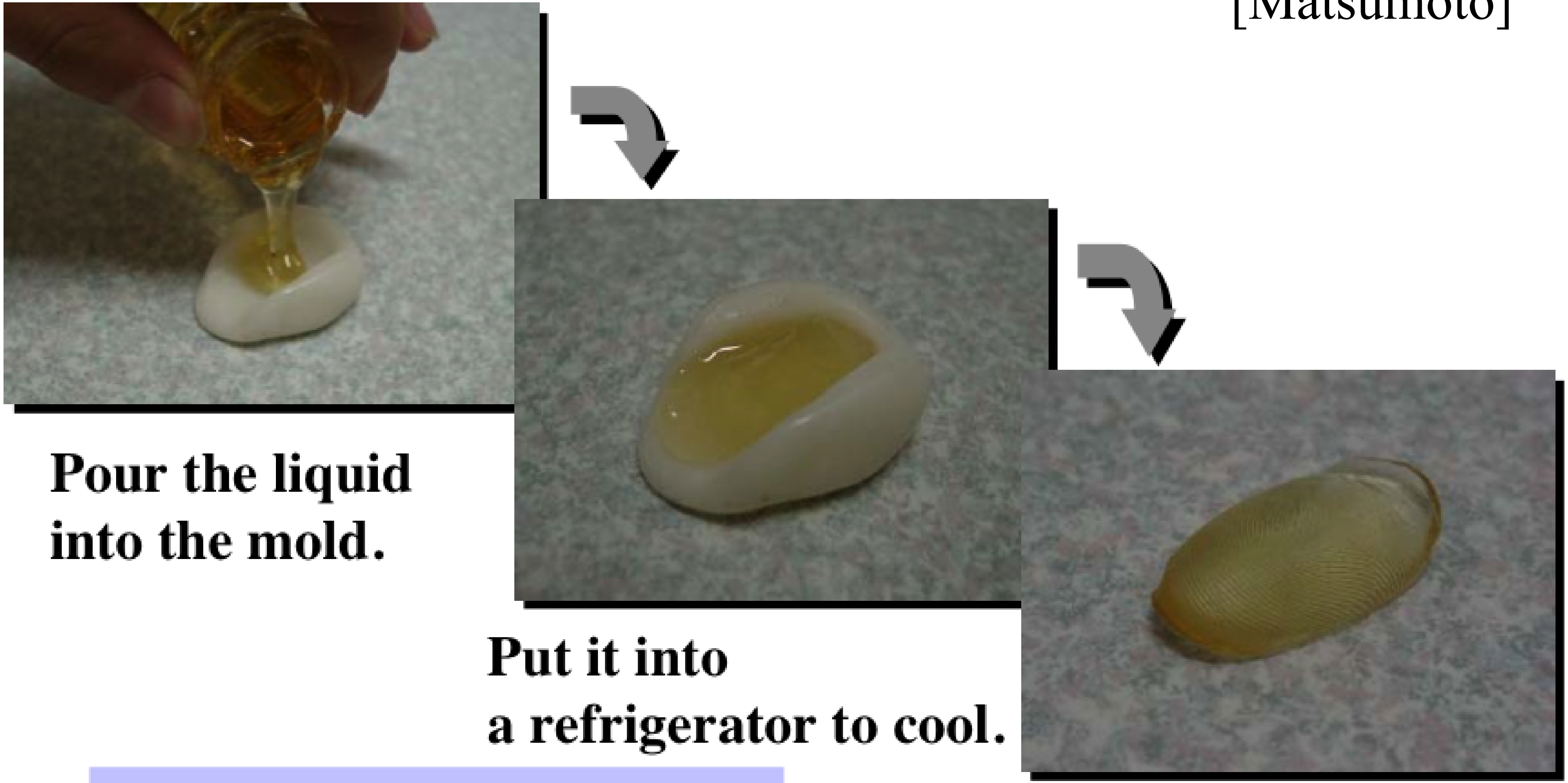
The mold

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.

Put it into a refrigerator to cool.

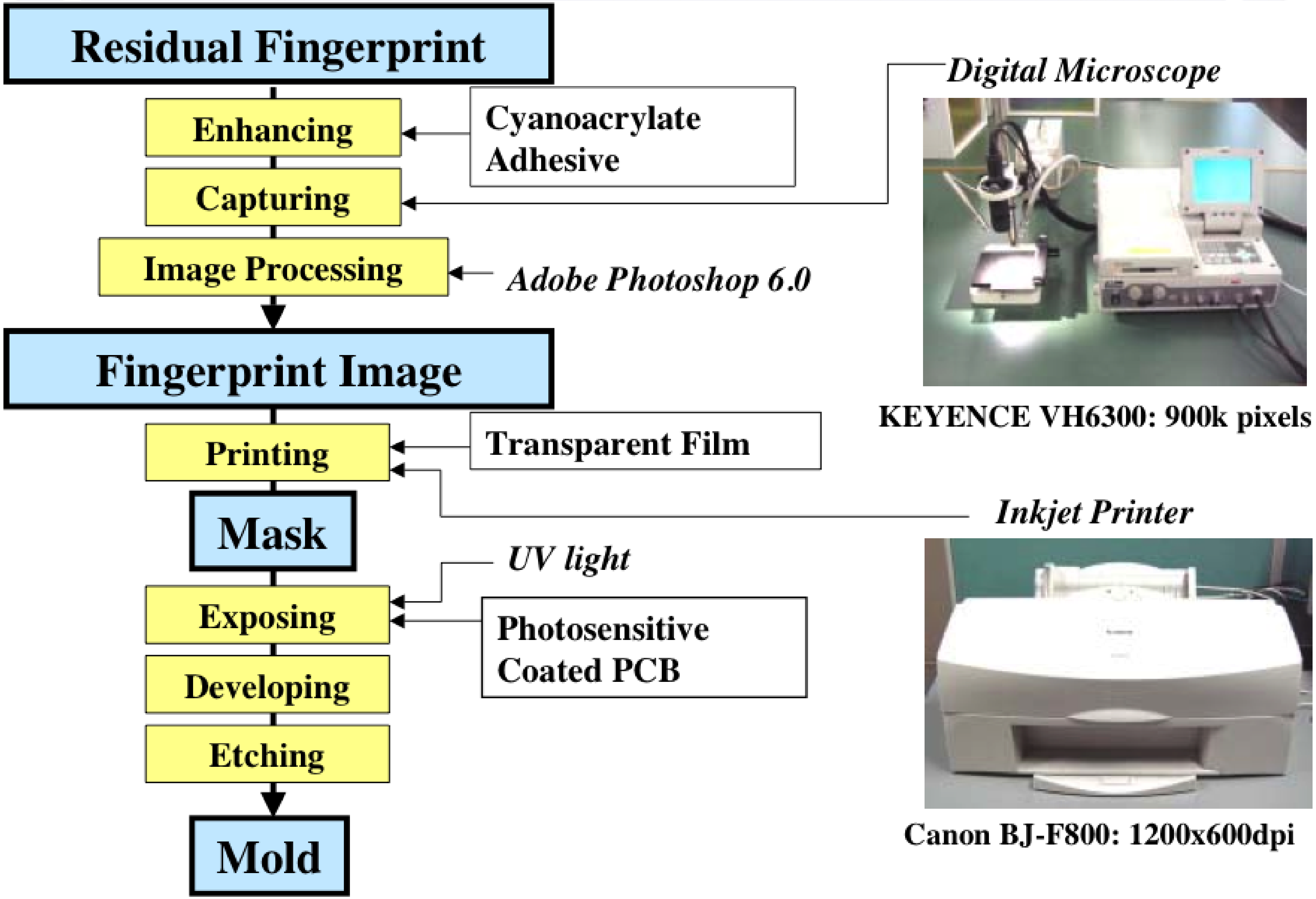
The gummy finger

It takes around 10 minutes.

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

Involuntary

[Matsumoto]



Residual Fingerprint

Enhancing

Cyanoacrylate Adhesive

Capturing

Digital Microscope

Image Processing

Adobe Photoshop 6.0

Fingerprint Image

KEYENCE VH6300: 900k pixels

Printing

Transparent Film

Inkjet Printer

Mask

UV light

Exposing

Photosensitive Coated PCB

Developing

Etching

Mold

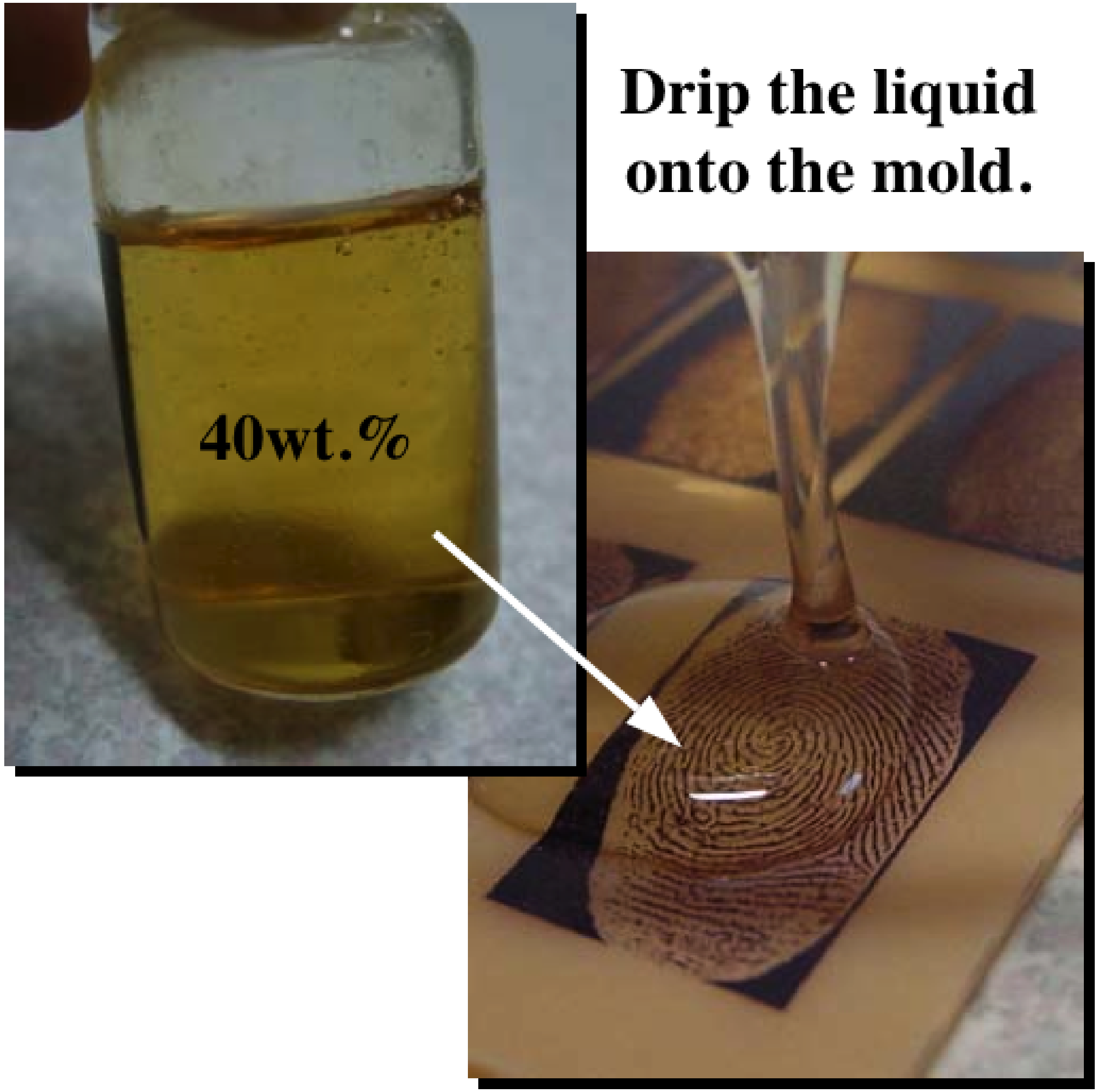
Canon BJ-F800: 1200x600dpi

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

Involuntary

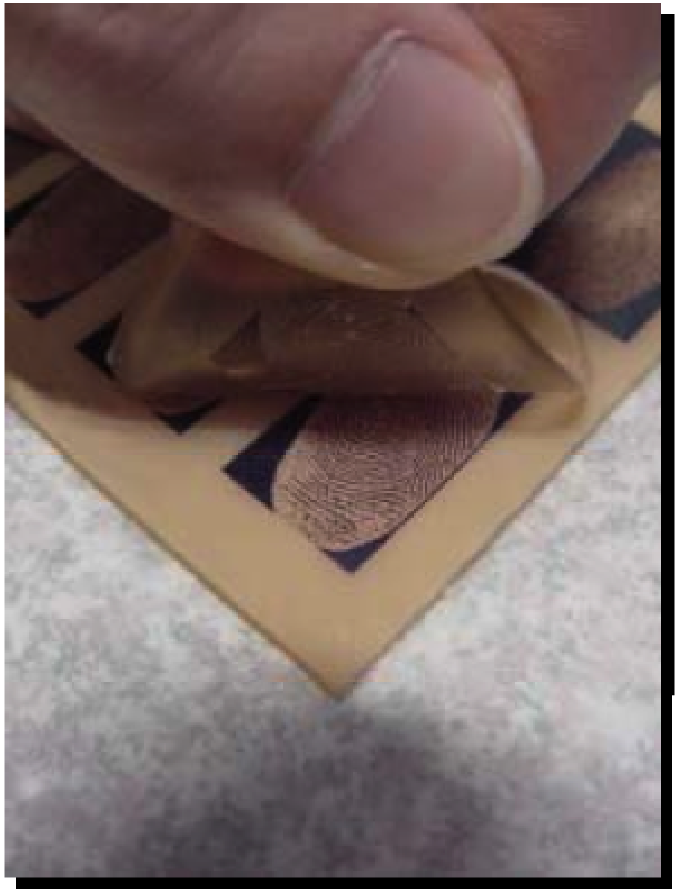
[Matsumoto]

Gelatin Liquid



Drip the liquid onto the mold.

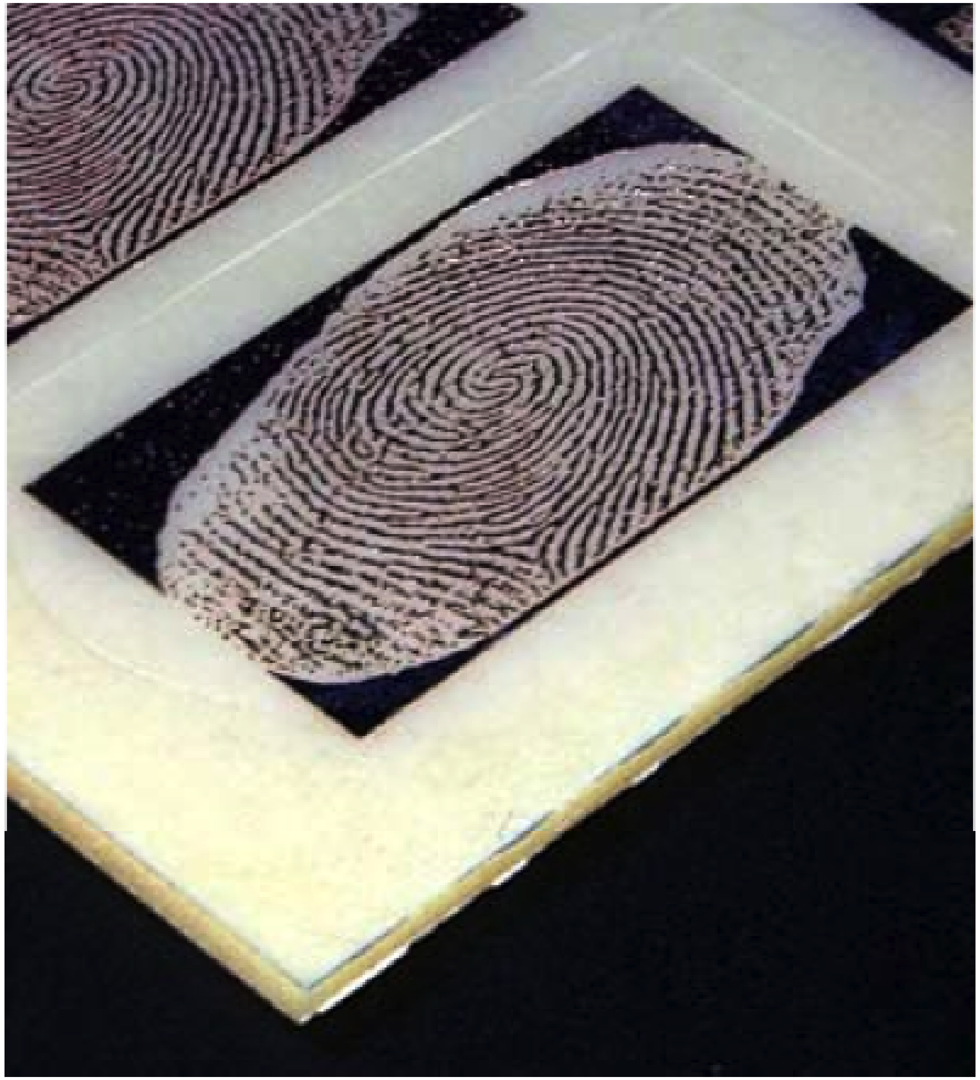
Put this mold into a refrigerator to cool, and then peel carefully.

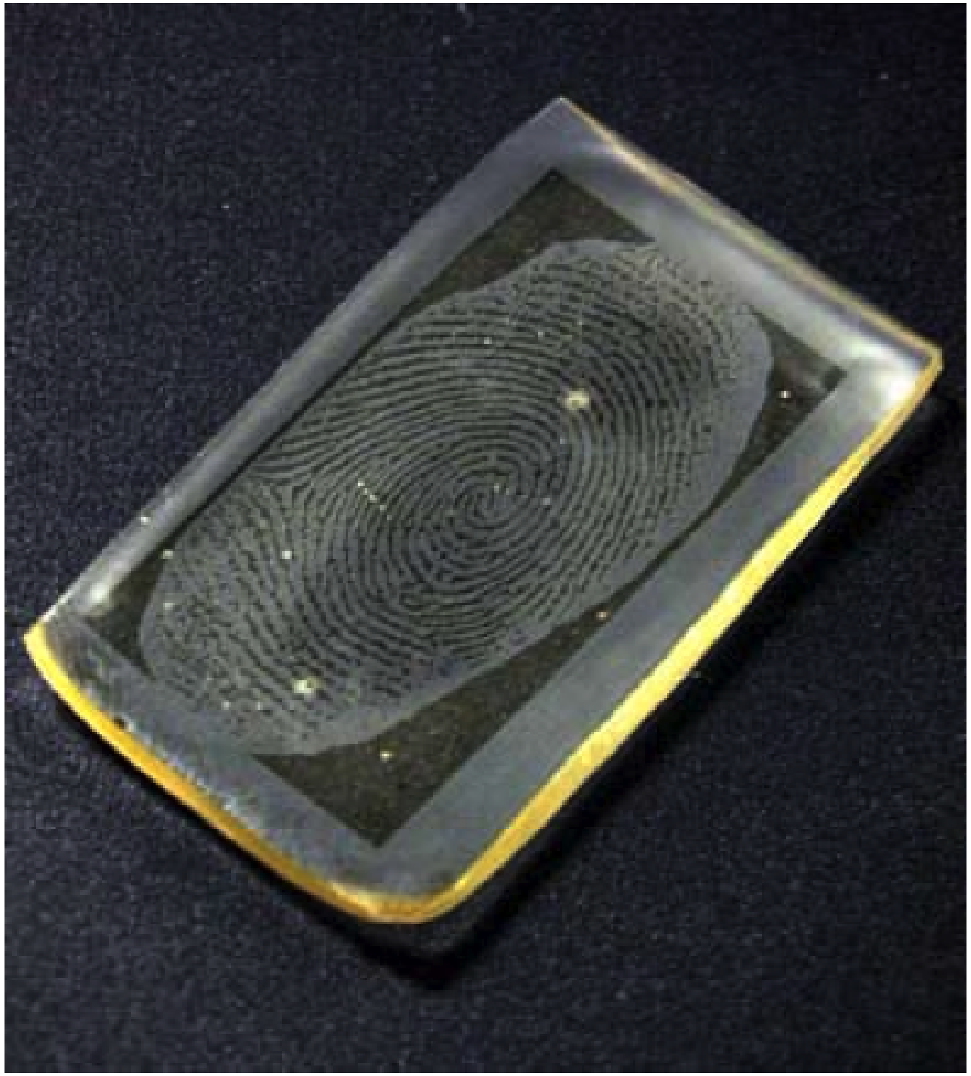


http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Involuntary

[Matsumoto]



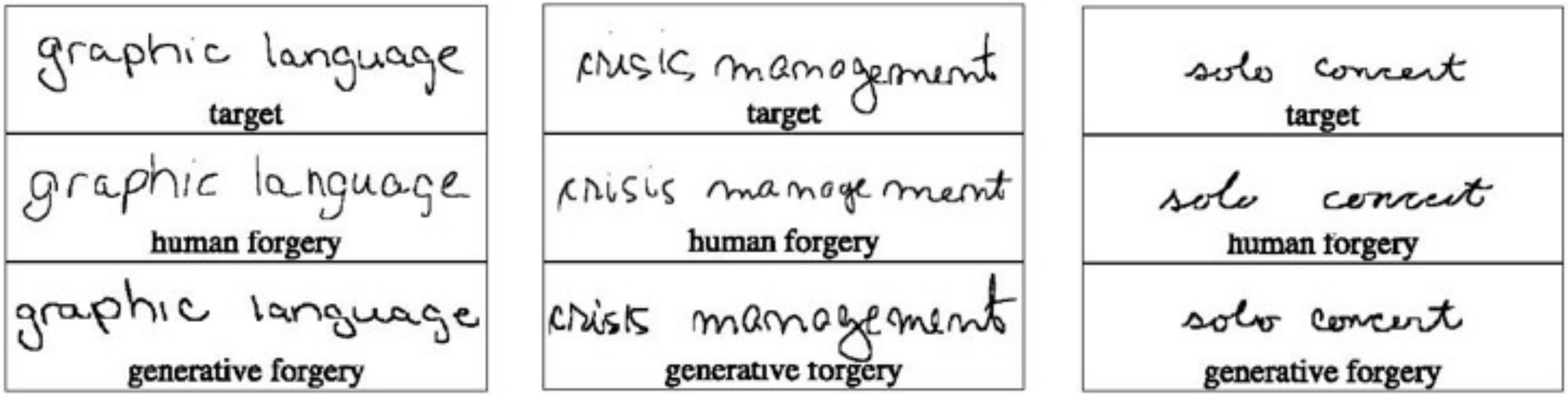


http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Authentication by Handwriting

[Ballard, Monrose, Lopresti]

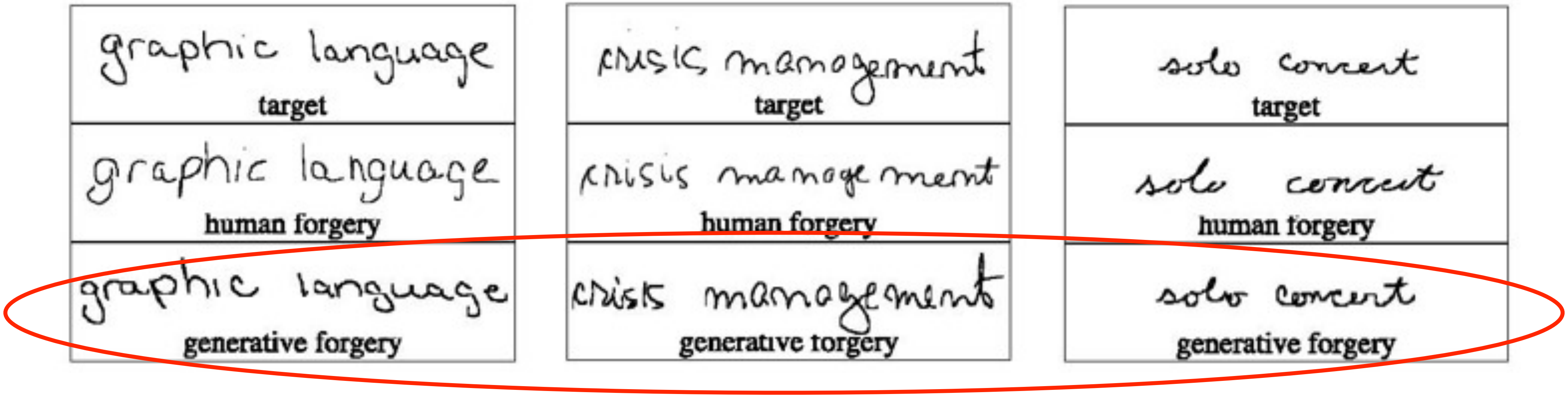
- Maybe a computer could also forge some biometrics



Authentication by Handwriting

[Ballard, Monrose, Lopresti]

- Maybe a computer could also forge some biometrics



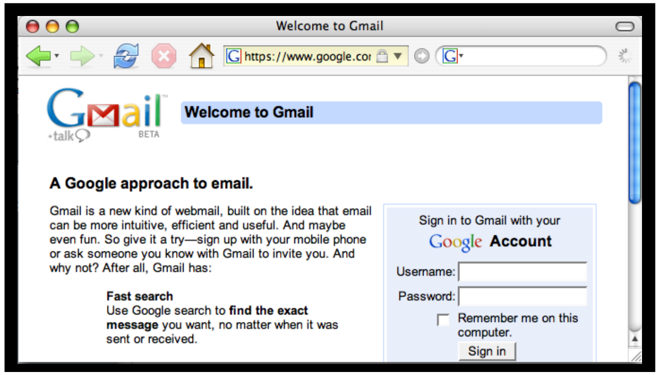
Generated by computer algorithm trained on handwriting samples

Human Factors in User Authentication

Passwords

The problem

Alice needs passwords for all the websites that she visits



Welcome to Gmail

A Google approach to email.

Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient and useful. And maybe even fun. So give it a try—sign up with your mobile phone or ask someone you know with Gmail to invite you. And why not? After all, Gmail has:

Fast search
Use Google search to **find the exact message** you want, no matter when it was sent or received.

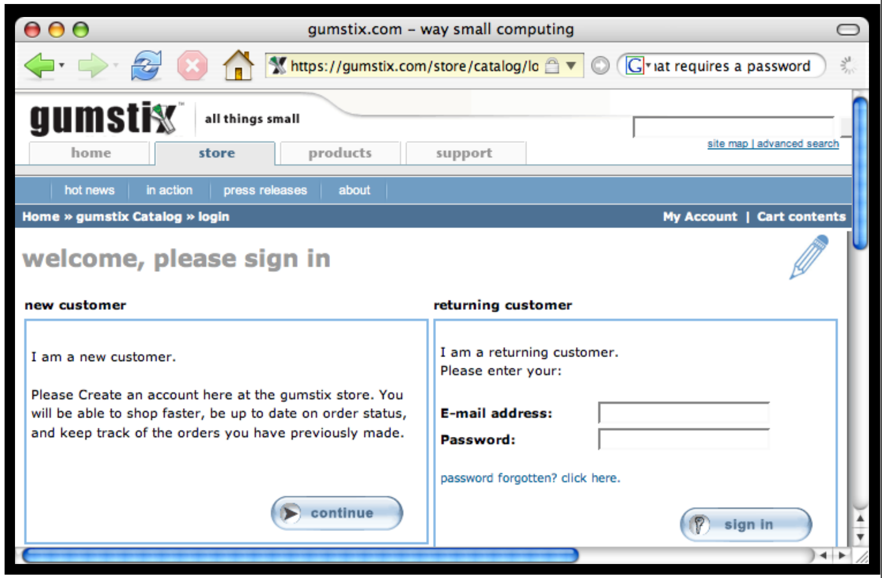
Sign in to Gmail with your Google Account

Username:

Password:

□ Remember me on this computer.

Sign in


gumstix.com – way small computing
https://gumstix.com/store/catalog/lo
ıat requires a password
gumstix
all things small
home
store
products
support
site map | advanced search
hot news
in action
press releases
about
Home » gumstix Catalog » login
My Account | Cart contents

welcome, please sign in

new customer

I am a new customer.

Please Create an account here at the gumstix store. You will be able to shop faster, be up to date on order status, and keep track of the orders you have previously made.

continue

returning customer

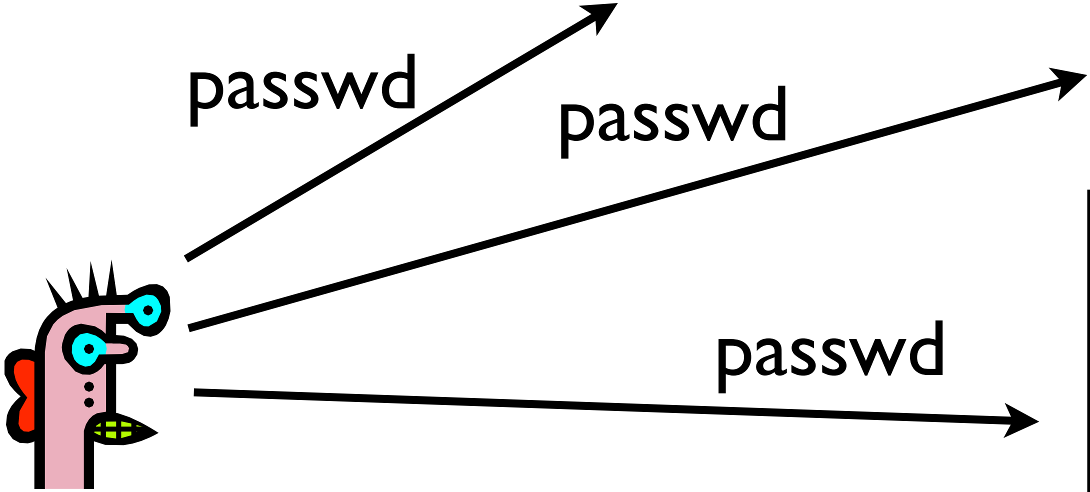
I am a returning customer.
Please enter your:

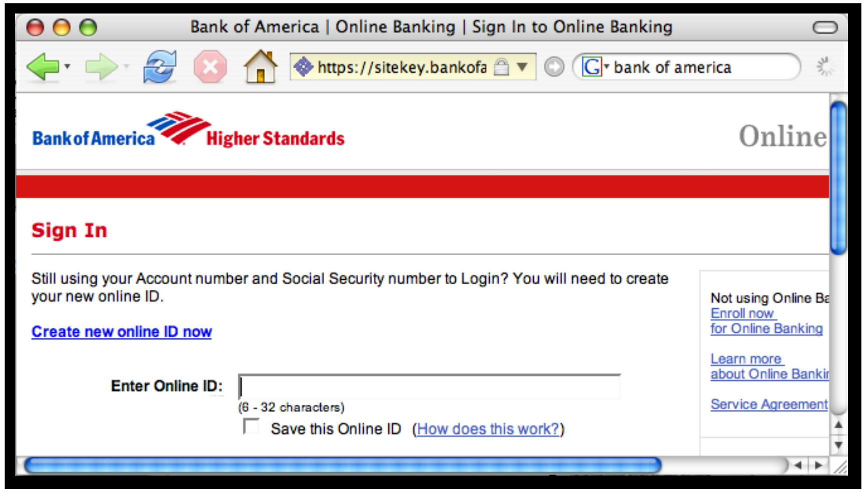
E-mail address:

Password:

password forgotten? click here.

sign in





Sign In

Still using your Account number and Social Security number to Login? You will need to create your new online ID.

Create new online ID now

Enter Online ID:

(6 - 32 characters)

□ Save this Online ID (How does this work?)

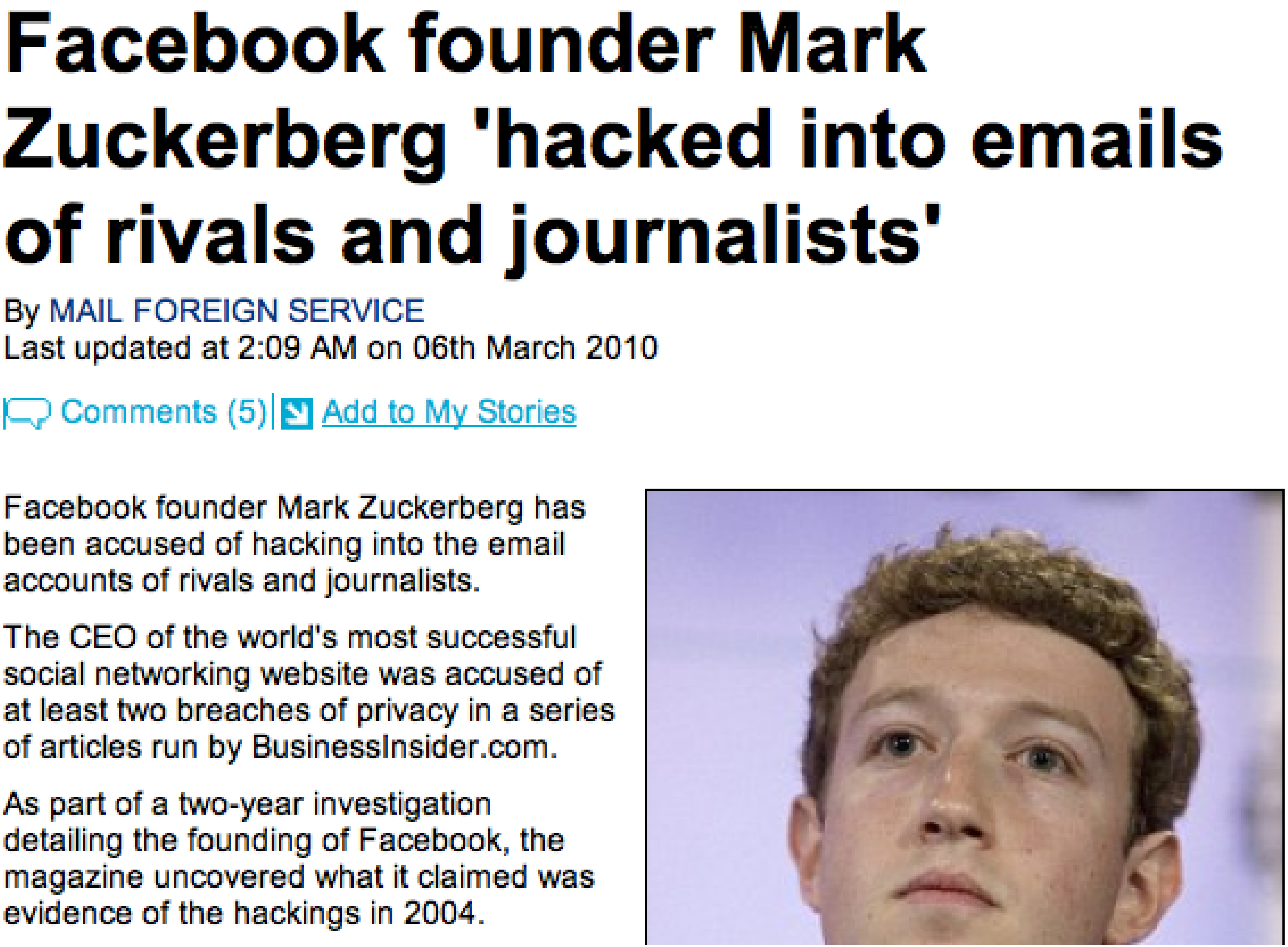
Not using Online Ba
Enroll now
for Online Banking

Learn more
about Online Bankir

Service Agreement

Possible solutions

- Easy to remember: Use same password on all websites. Use “weak” password.
  - Poor security (don’t share password between bank website and small website)
- More secure: Use different, strong passwords on all websites.
  - Hard to remember, unless write down.



Facebook founder Mark Zuckerberg 'hacked into emails of rivals and journalists'

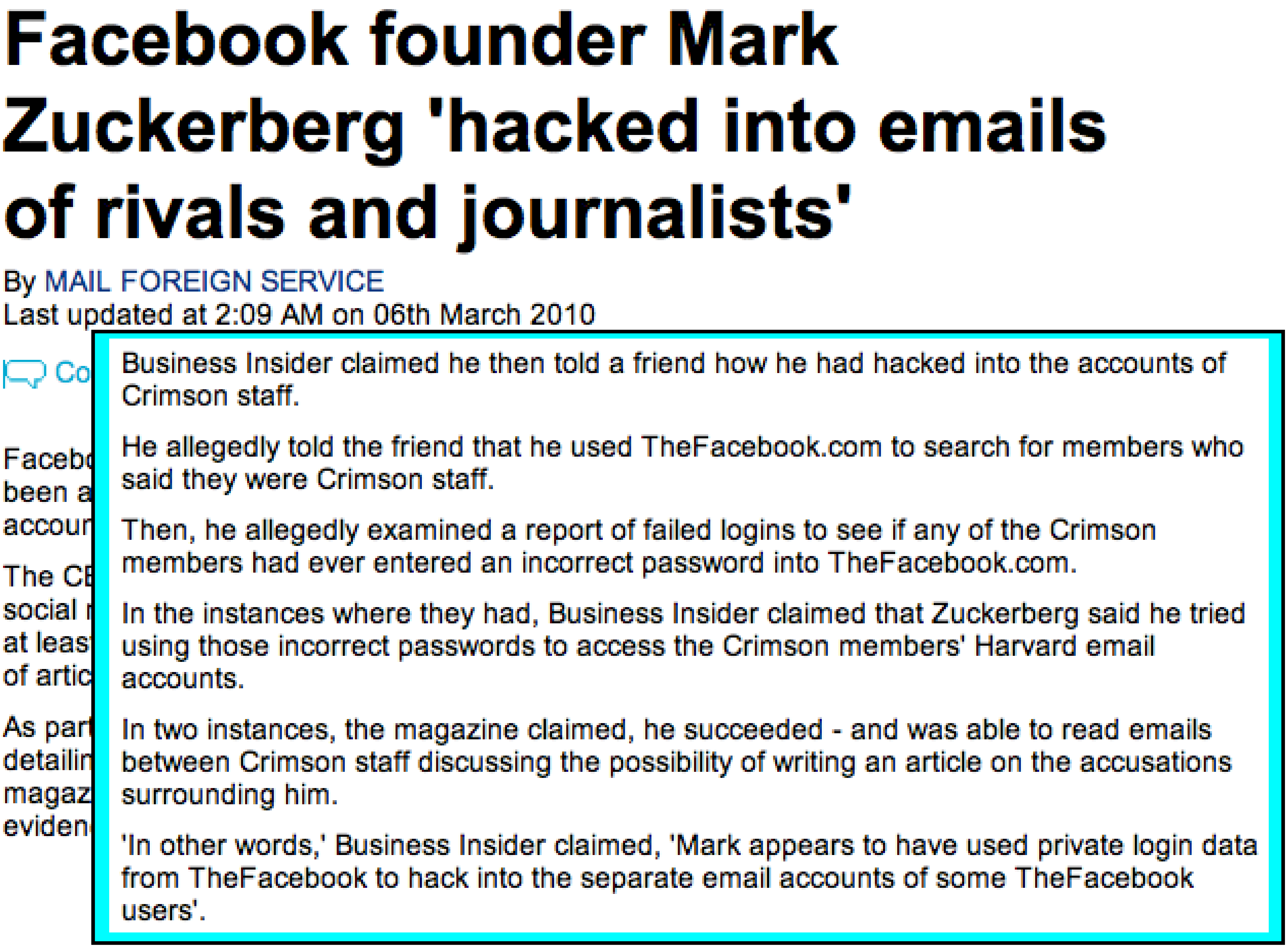
By MAIL FOREIGN SERVICE
Last updated at 2:09 AM on 06th March 2010

Comments (5) | Add to My Stories

Facebook founder Mark Zuckerberg has been accused of hacking into the email accounts of rivals and journalists.

The CEO of the world's most successful social networking website was accused of at least two breaches of privacy in a series of articles run by BusinessInsider.com.

As part of a two-year investigation detailing the founding of Facebook, the magazine uncovered what it claimed was evidence of the hackings in 2004.



Facebook founder Mark Zuckerberg 'hacked into emails of rivals and journalists'

By MAIL FOREIGN SERVICE
Last updated at 2:09 AM on 06th March 2010

Co

Facebo
been a
accour

The CE
social r
at leas
of artic

As part
detailin
magaz
eviden

Business Insider claimed he then told a friend how he had hacked into the accounts of Crimson staff.

He allegedly told the friend that he used TheFacebook.com to search for members who said they were Crimson staff.

Then, he allegedly examined a report of failed logins to see if any of the Crimson members had ever entered an incorrect password into TheFacebook.com.

In the instances where they had, Business Insider claimed that Zuckerberg said he tried using those incorrect passwords to access the Crimson members' Harvard email accounts.

In two instances, the magazine claimed, he succeeded - and was able to read emails between Crimson staff discussing the possibility of writing an article on the accusations surrounding him.

'In other words,' Business Insider claimed, 'Mark appears to have used private login data from TheFacebook to hack into the separate email accounts of some TheFacebook users'.

Classroom Survey

Who here...

- repeats I password across many sites?
- uses I password with site-specific variations?
- uses 2 passwords, one low-security and one high-security for special sites?
- uses truly unique passwords for special sites?
- uses a truly unique password on every site?
- Does something else?

Alternate solution: Password managers

- Password managers handle creating and "remembering" strong passwords
- Potentially:
  - Easier for users
  - More secure
- Examples:
  - PwdHash (Usenix Security 2005)
  - Password Multiplier (WWW 2005)

Key mechanisms

- User remembers a ***single "master" password***
- Password managers
  - On input: (1) the user's single password and (2) information about the website
  - Compute: Strong, site-specific password
- Goal: Avoid problems with passwords