CSE 484 and CSE M 584 (Winter 2009)

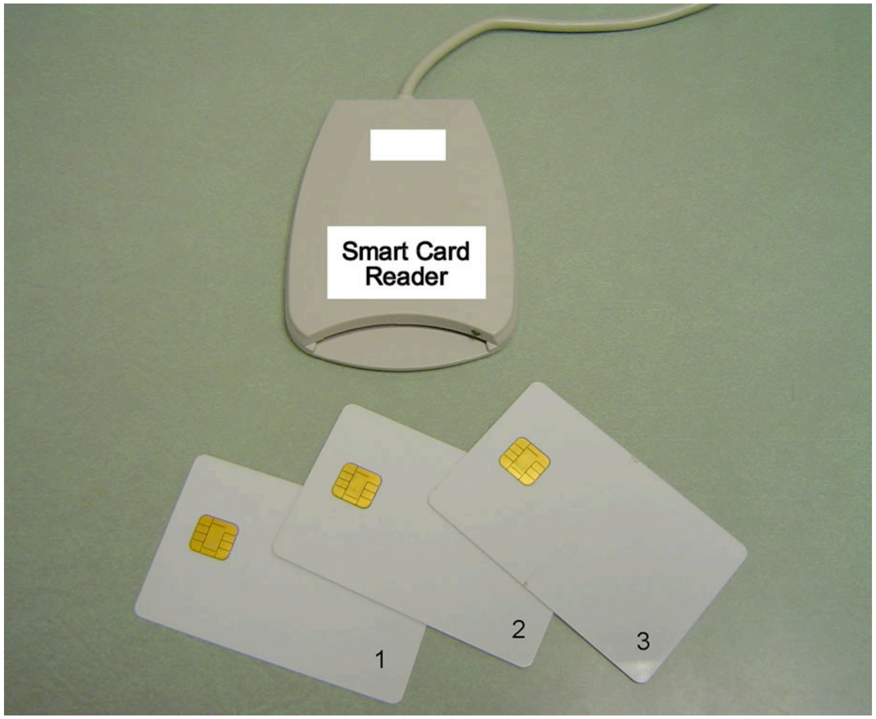
Authentication

Tadayoshi Kohno

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

What You Have

- Smartcard
  - Little computer chip in credit card form factor



Magstripe Writer

http://www.tyner.com/magnetic/msr206-1.jpg

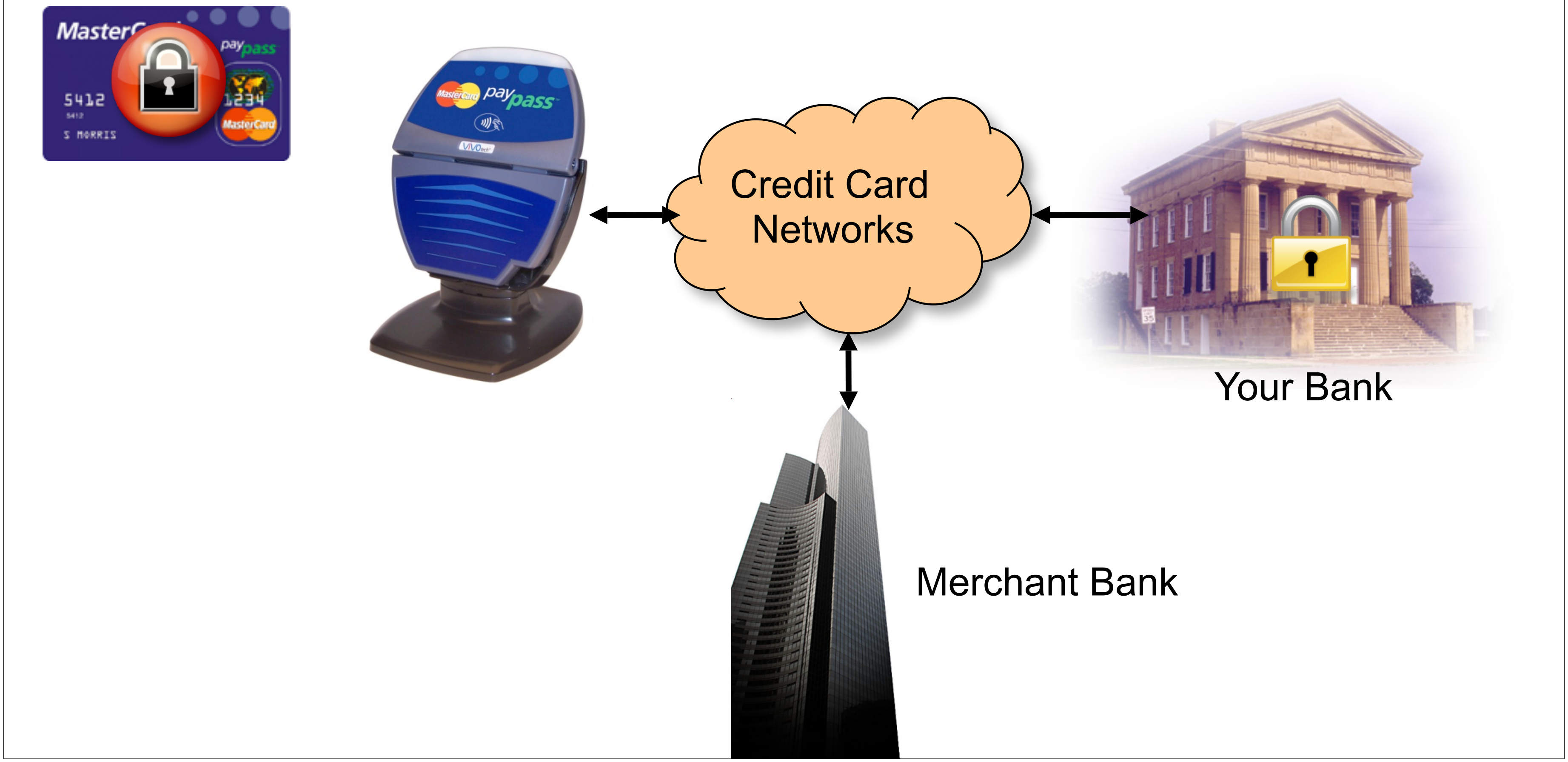
Cloning Attack

MasterCard
paypass
5412 3456 7890 1234
12-05
S MORRIS
MasterCard paypass
MasterCard paypass

RFID reader

Slides from Karl Koscher; CCS 2008 Czeskis, Koscher, Smith, Kohno

Use Encryption?

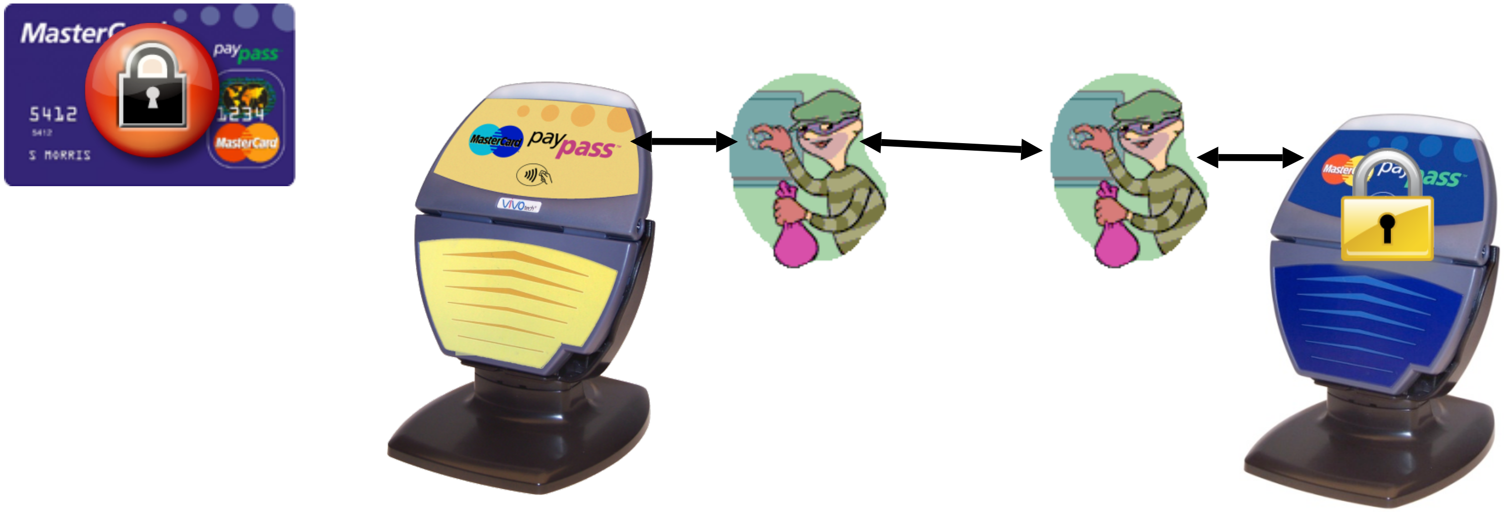


Credit Card Networks

Your Bank

Merchant Bank

Relaying Attack



Slides from Karl Koscher; CCS 2008 Czeskis, Koscher, Smith, Kohno

Smartcard Bank Cards [Drimer and Murdoch]

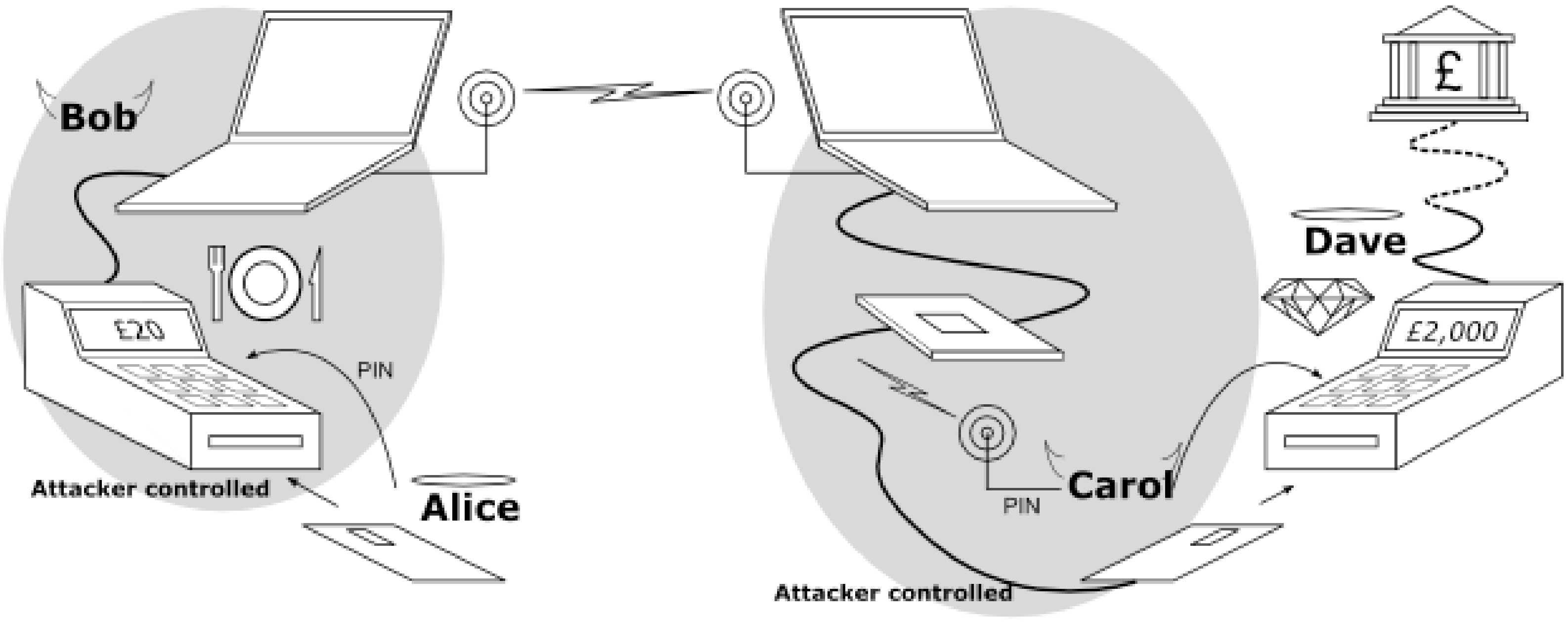


Image from http://www.cl.cam.ac.uk/research/security/projects/banking/relay/

Smartcard Bank Cards [Drimer and Murdoch]

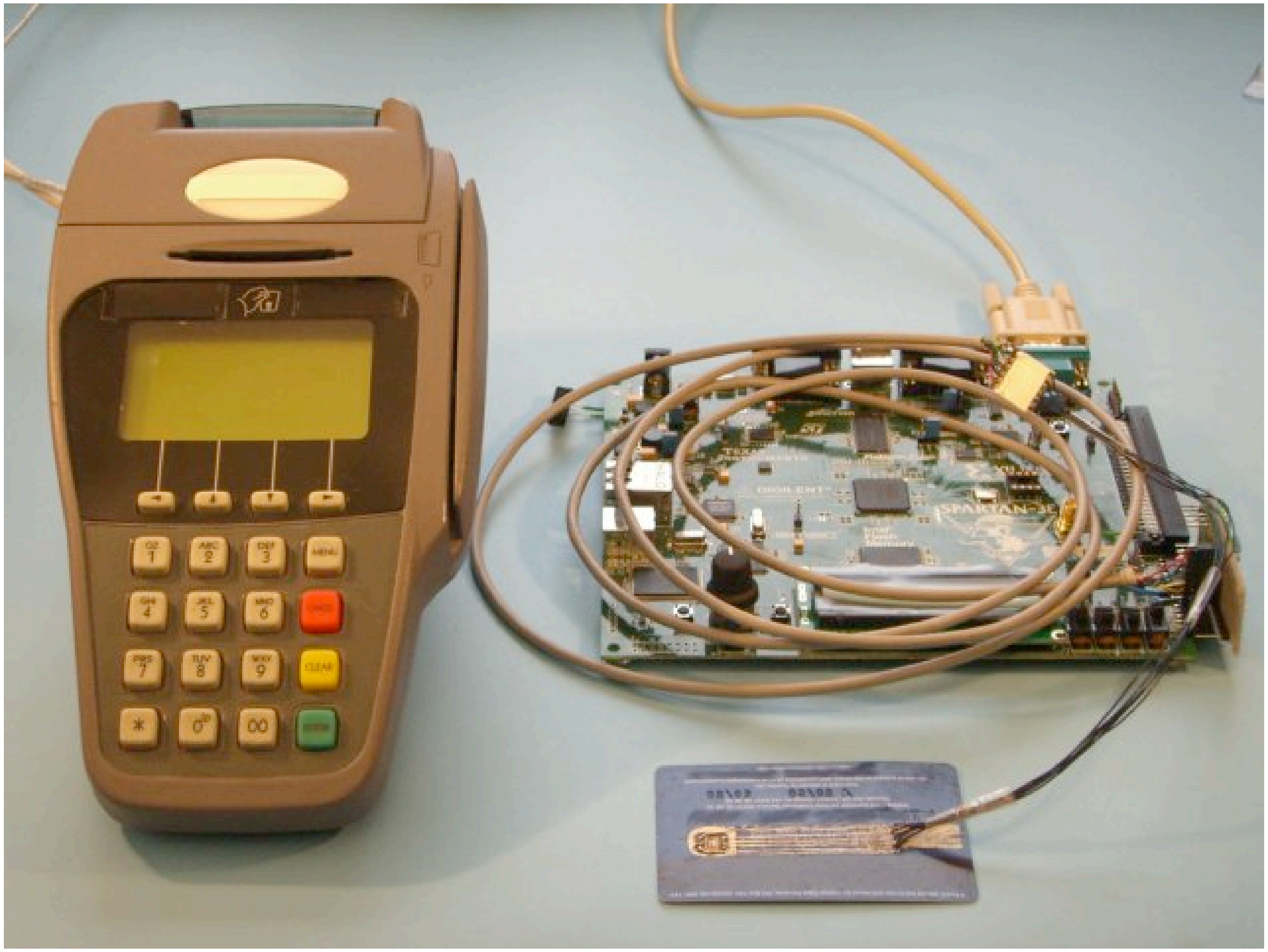


Image from http://www.cl.cam.ac.uk/research/security/projects/banking/relay/

Some Approaches

- Can control tags with:
  - Sleeves
  - Buttons
  - Multi-factor authentication
  - Distance bounding
- First three change the usage model – might be highly inconvenient
- Distance bounding isn't backwards-compatible and requires systemic changes

Slides from Karl Koscher; CCS 2008 Czeskis, Koscher, Smith, Kohno

Sensing Intent

- What if the tags could sense when you wanted them to talk – without changing the entire system?
- We observe many people perform unique gestures when using their tags
  - Usually a wave in front of the antenna
  - Hip twist, others, etc.

- Can we base tag activation on these?

Slides from Karl Koscher; CCS 2008 Czeskis, Koscher, Smith, Kohno

Our Solution

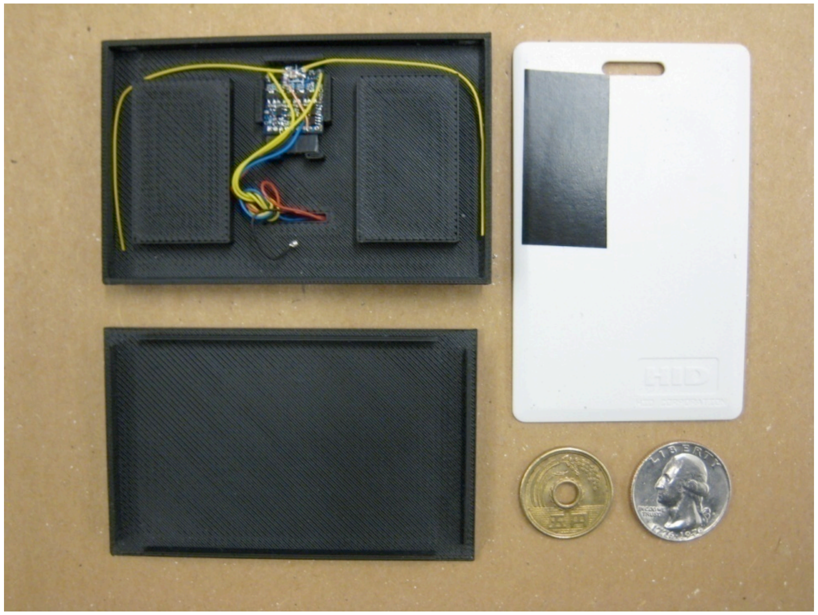
- Detecting all gestures might be too hard
- What if we only change the usage model slightly and require **specific** gestures?

- We developed a **completely passive** tag to detect these specific gestures, which we call **secret handshakes**

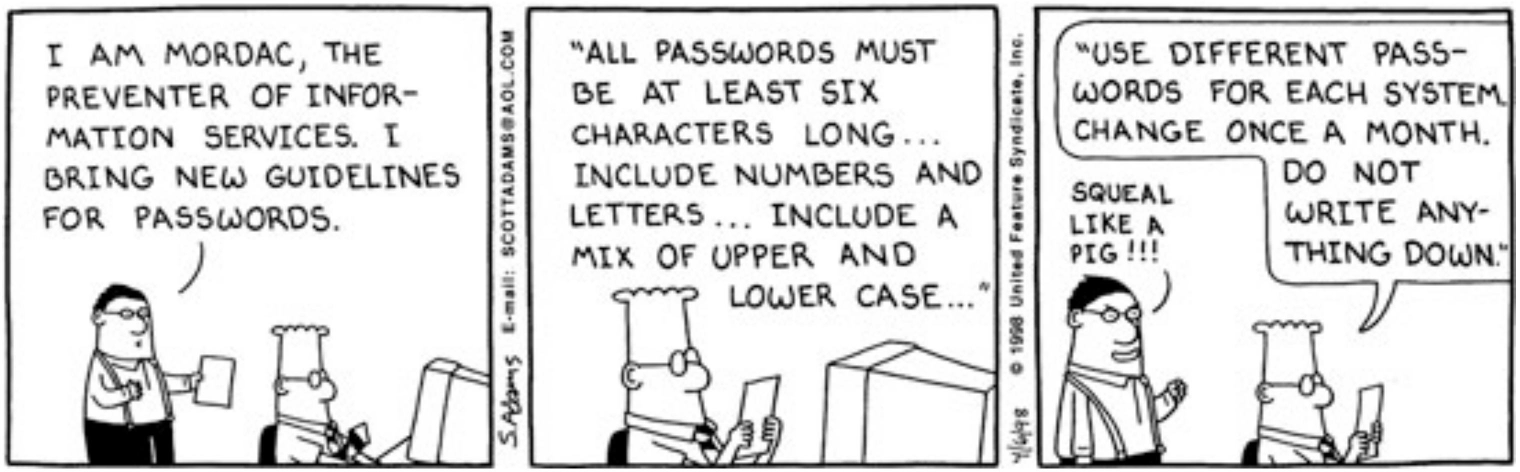
Slides from Karl Koscher; CCS 2008 Czeskis, Koscher, Smith, Kohno

Our Prototype

- We use the Intel WISP – a platform for RFID research
- Fully-programmable microcontroller (TI MSP 430)
- Built-in accelerometer
- **Completely passive**



Slides from Karl Koscher; CCS 2008 Czeskis, Koscher, Smith, Kohno


I AM MORDAC, THE PREVENTER OF INFORMATION SERVICES. I BRING NEW GUIDELINES FOR PASSWORDS.
S. Adams E-mail: SCOTTADAMS@AOL.COM
"ALL PASSWORDS MUST BE AT LEAST SIX CHARACTERS LONG... INCLUDE NUMBERS AND LETTERS... INCLUDE A MIX OF UPPER AND LOWER CASE..."
© 1998 United Feature Syndicate, Inc.
"USE DIFFERENT PASSWORDS FOR EACH SYSTEM. CHANGE ONCE A MONTH. DO NOT WRITE ANYTHING DOWN."
SQUEAL LIKE A PIG!!!

“Improving” Passwords

- Add biometrics
  - For example, keystroke dynamics or voiceprint
  - Revocation is often a problem with biometrics
- Graphical passwords
  - Goal: increase the size of memorable password space

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

Motivation

- Text Passwords are hard to remember
- Reuse & recording passwords is insecure
- People are good at recognizing faces
- Facial Passwords leverage this, but multiple facial passwords have not been studied

Slides from Kate Everitt; CHI 2009, Everitt, Bragin, Fogarty, Kohno

Graphical Password Systems

- *Cognometric schemes*
  - present a set of images,
  - authentication requires selection of correct images
- *Locimetric Schemes*
  - presents a single image, with authentication requiring clicking on regions of the image
- *Drawmetric Schemes*
  - require drawing figures or doodles to authenticate.

Slides from Kate Everitt; CHI 2009, Everitt, Bragin, Fogarty, Kohno

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”

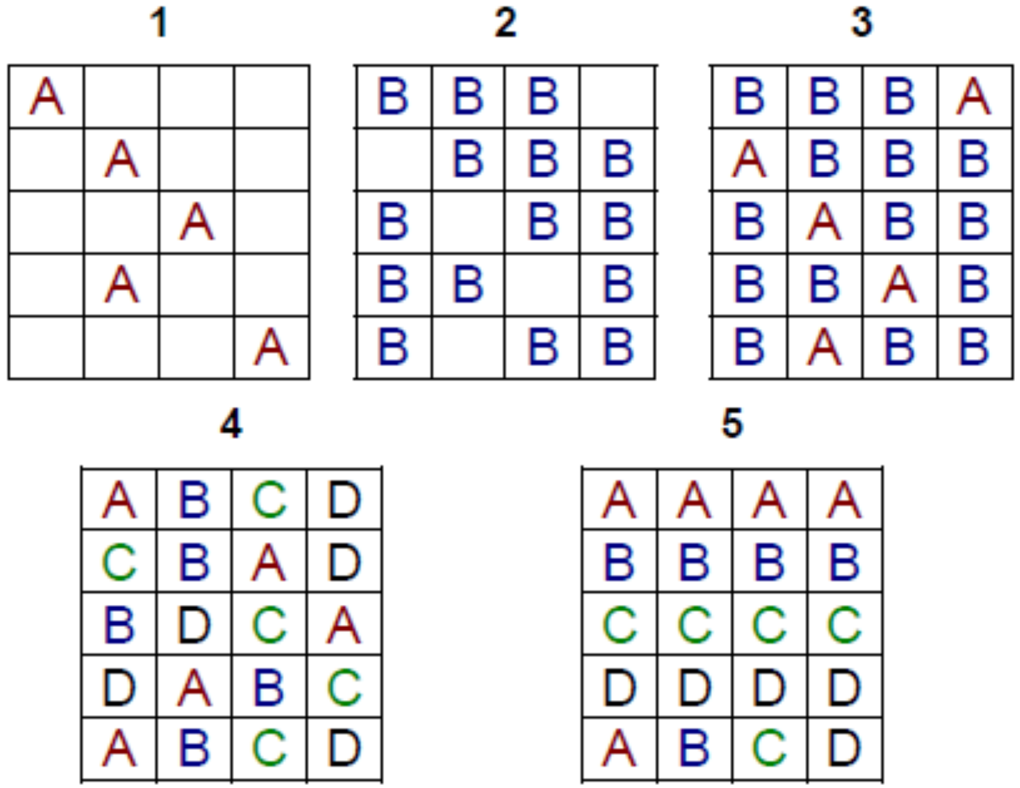
- Recommendation: system picks passfaces
- But is that still memorable? What issues could arise?

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

Slides from Kate Everitt; CHI 2009, Everitt, Bragin, Fogarty, Kohno

Study Conditions



1

A			
	A		
		A	
	A		
			A

2

B	B	B	
	B	B	B
B		B	B
B	B		B
B		B	B

3

B	B	B	A
A	B	B	B
B	A	B	B
B	B	A	B
B	A	B	B

4

A	B	C	D
C	B	A	D
B	D	C	A
D	A	B	C
A	B	C	D

5

A	A	A	A
B	B	B	B
C	C	C	C
D	D	D	D
A	B	C	D

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

Slides from Kate Everitt; CHI 2009, Everitt, Bragin, Fogarty, Kohno

Variants...

- http://arima.okoze.net/illusion/
- (Plus click-based graphical passwords, drawing-based passwords)

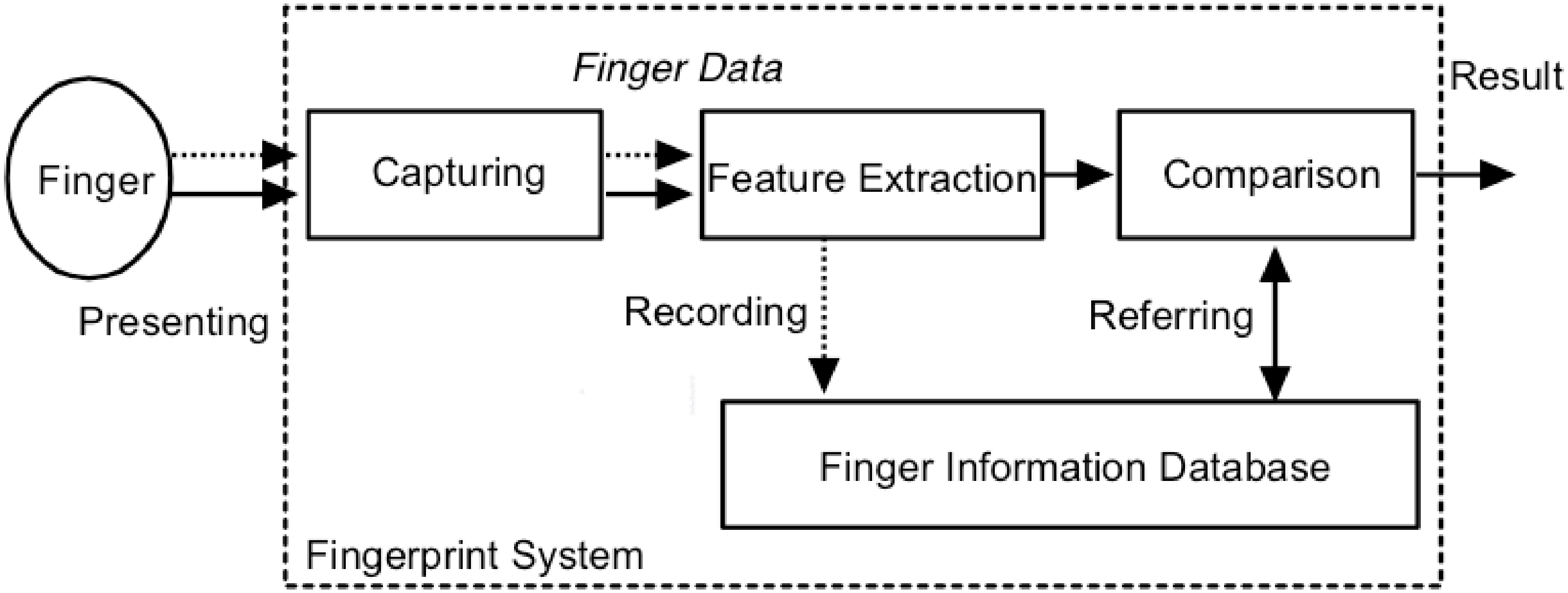
Uses of graphical passwords?

- For what applications might graphical passwords be particularly useful?

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 [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)
  - 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 false match is 1 in 10 billion
    - No successful challenges until 2000
  - Fingerprint damage impairs recognition
    - Ross Anderson’s scar crashes FBI scanner

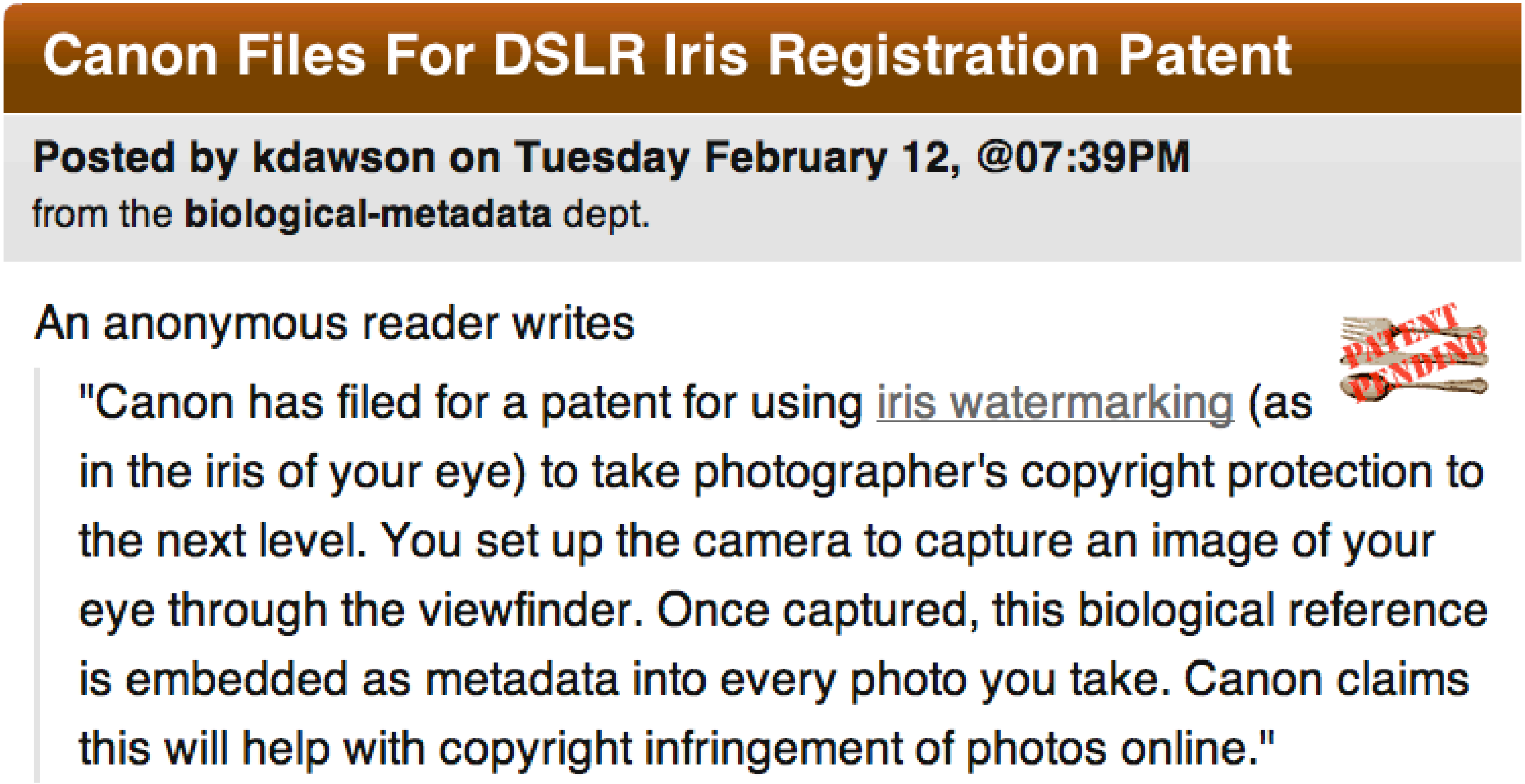
Other Biometrics

- 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
  - Best biometric mechanism currently known
- 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?

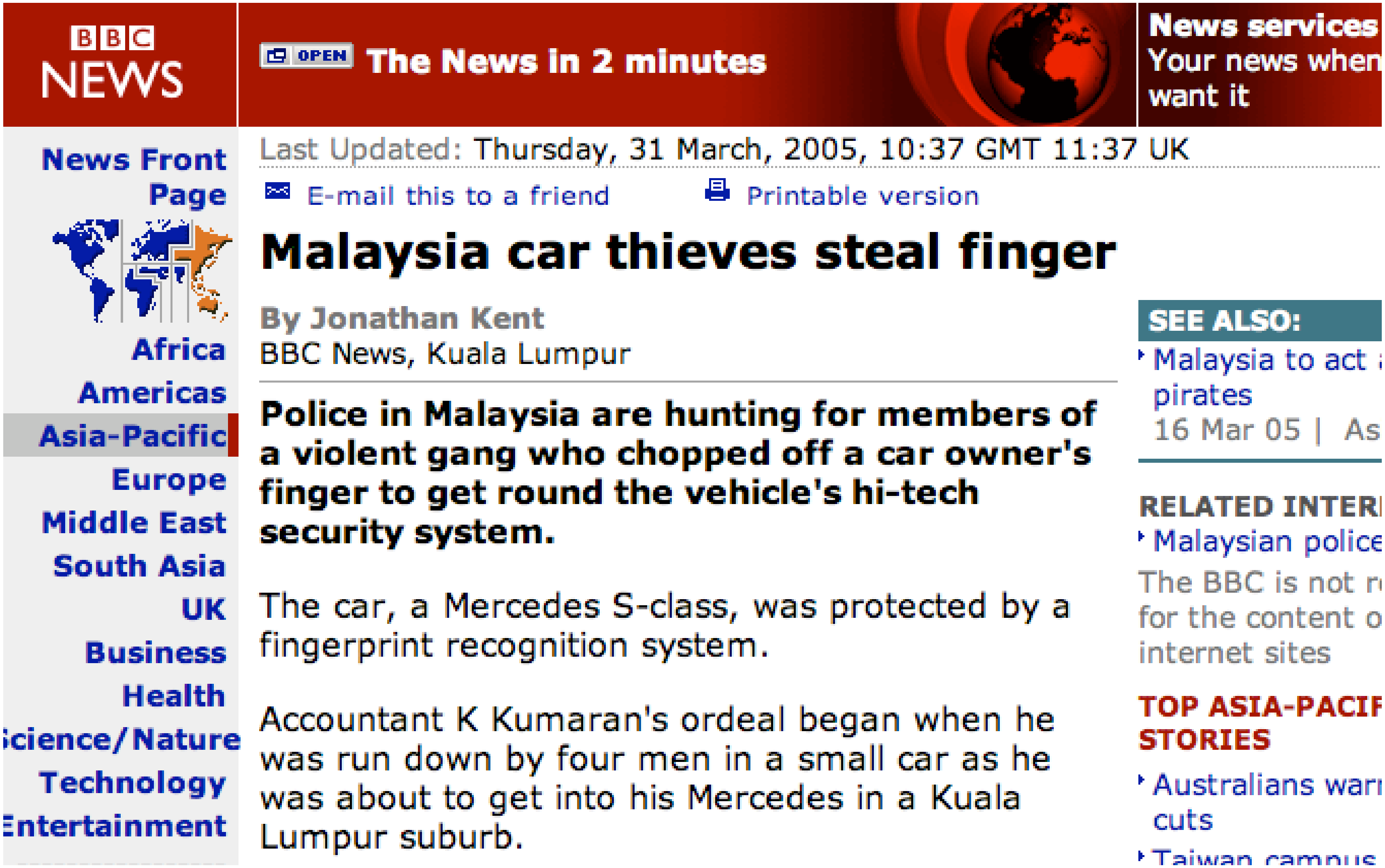
Issues with Biometrics

- 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.

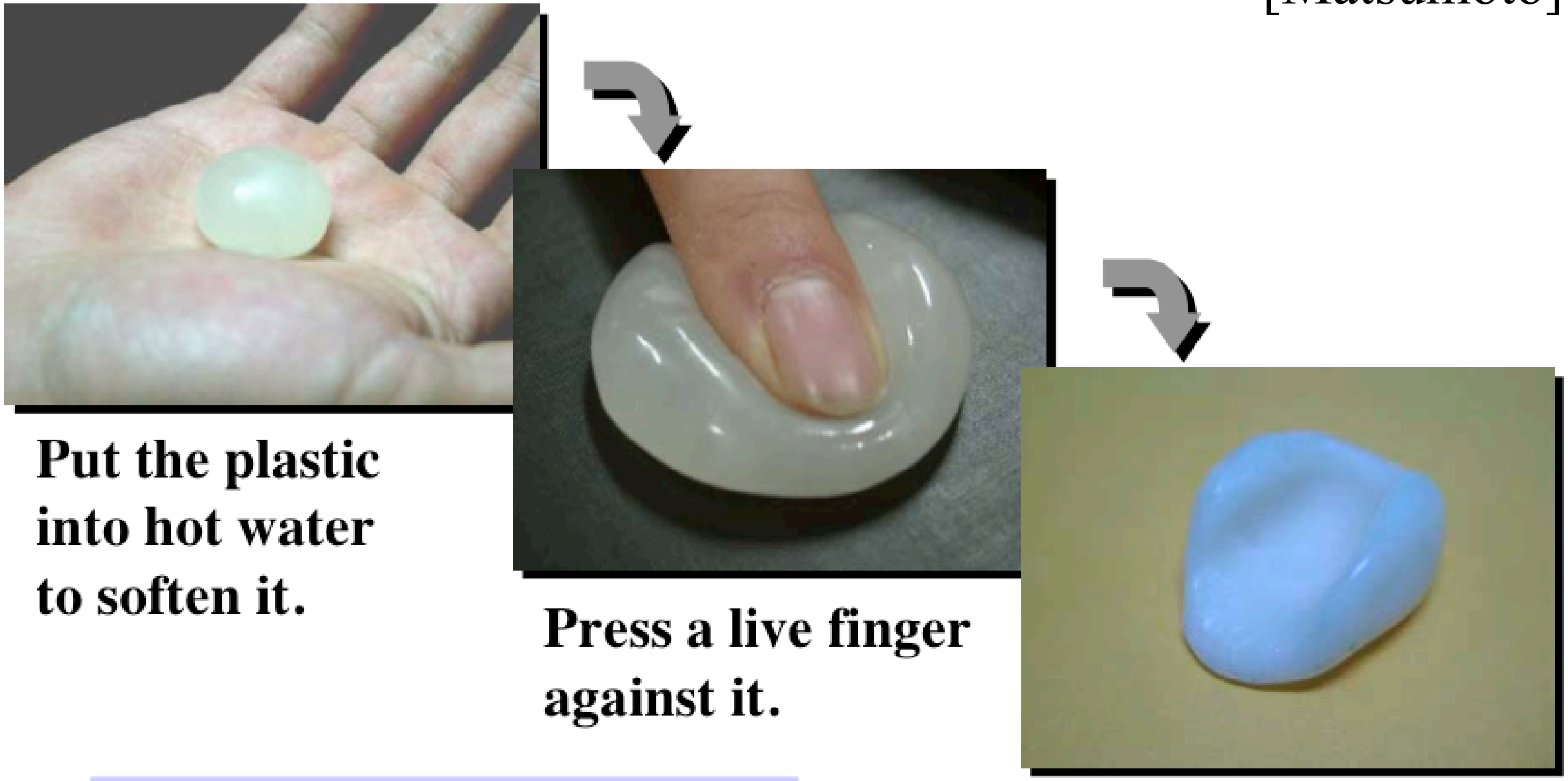
http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

Biometric Error Rates (Adversarial)

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

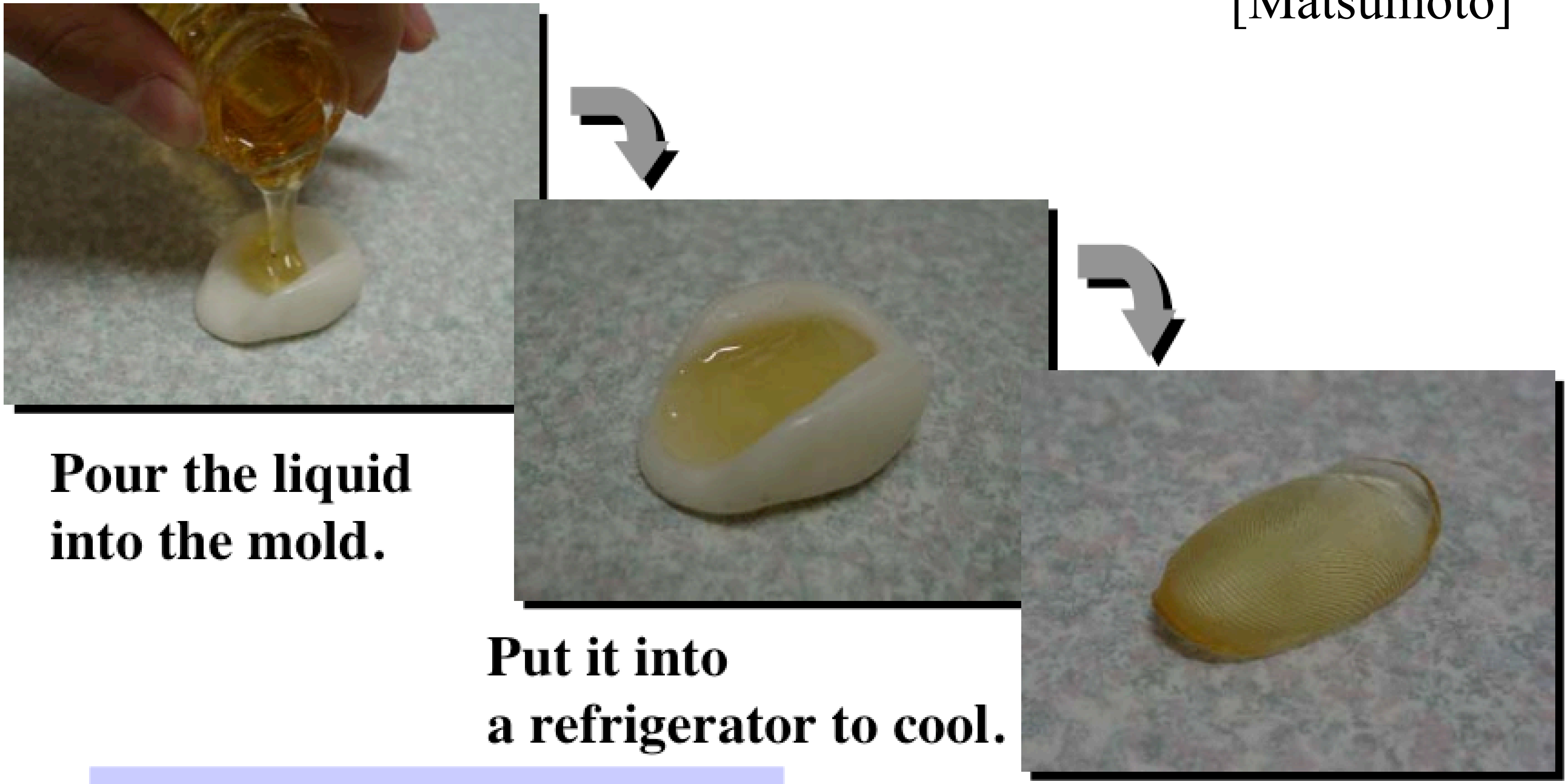
The mold

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.

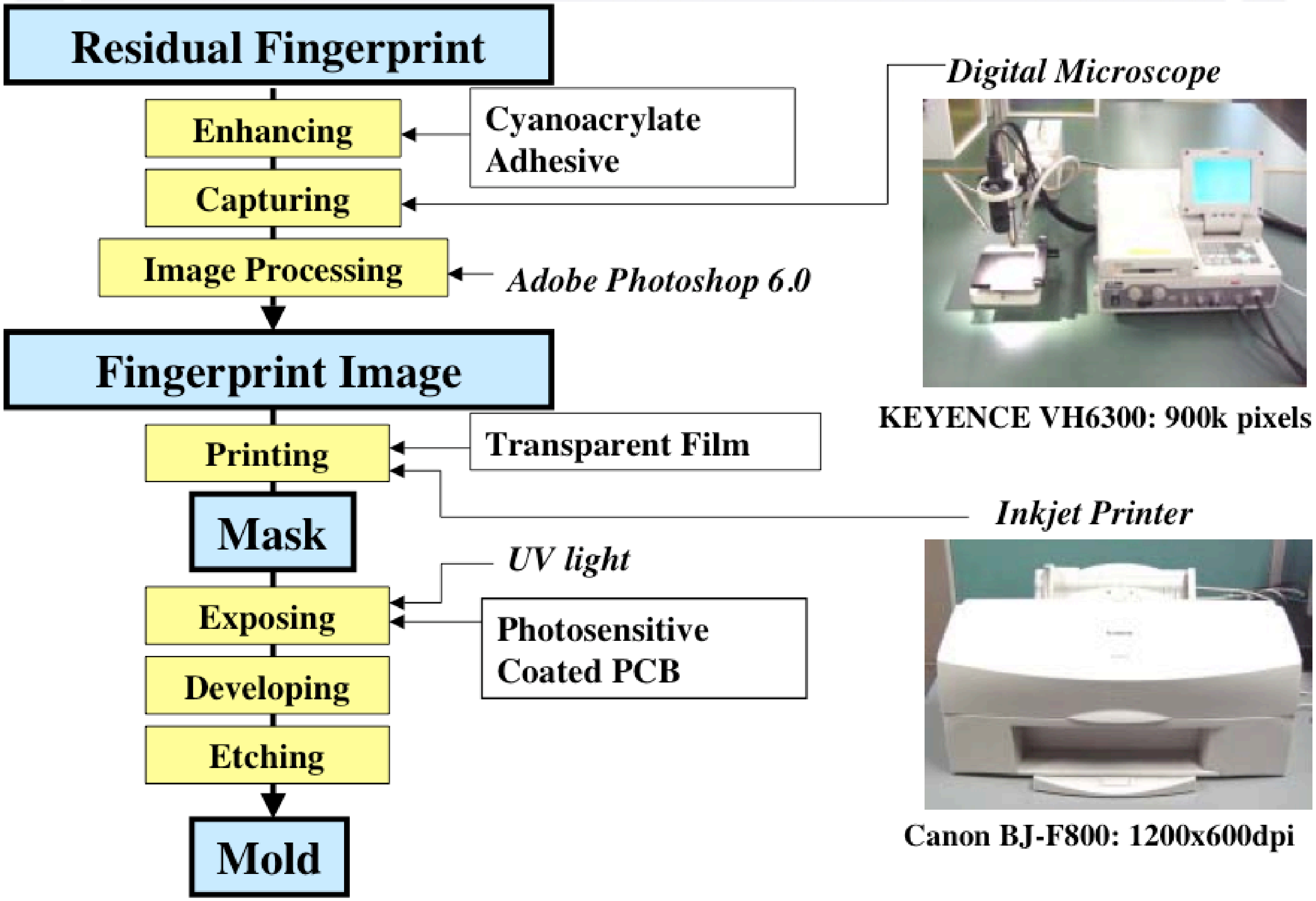
It takes around 10 minutes.

The gummy finger

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

- Printing ← Transparent Film, Inkjet Printer

Mask

- Exposing ← *UV light*, Photosensitive Coated PCB
- Developing
- Etching

Mold

Digital Microscope

KEYENCE VH6300: 900k pixels

Inkjet Printer

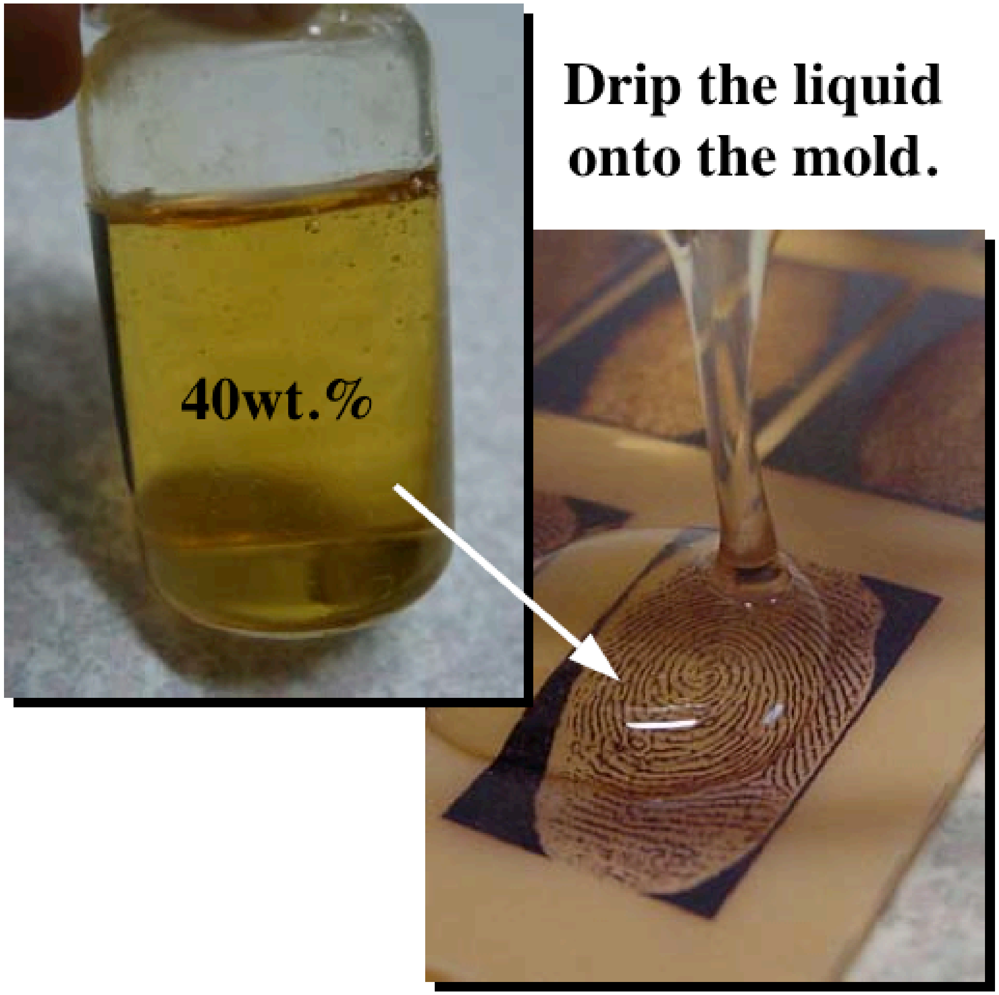
Canon BJ-F800: 1200x600dpi

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

Involuntary

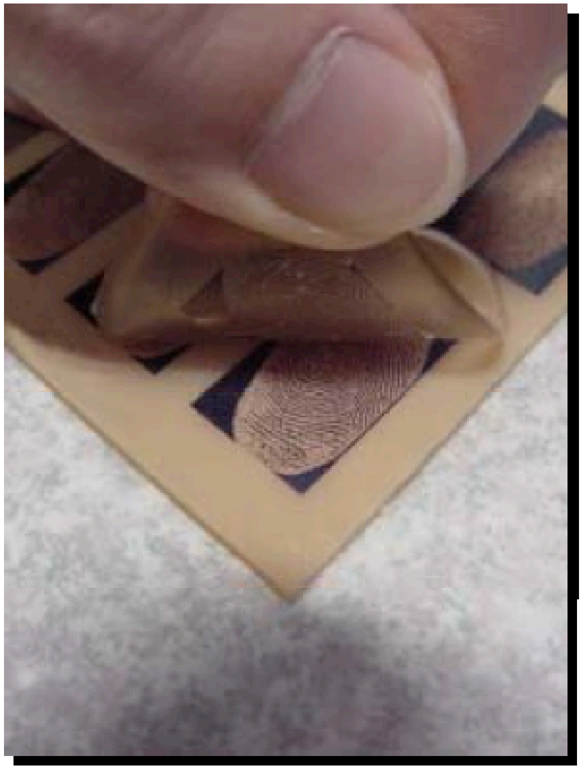
[Matsumoto]

Gelatin Liquid



Drip the liquid onto the mold.

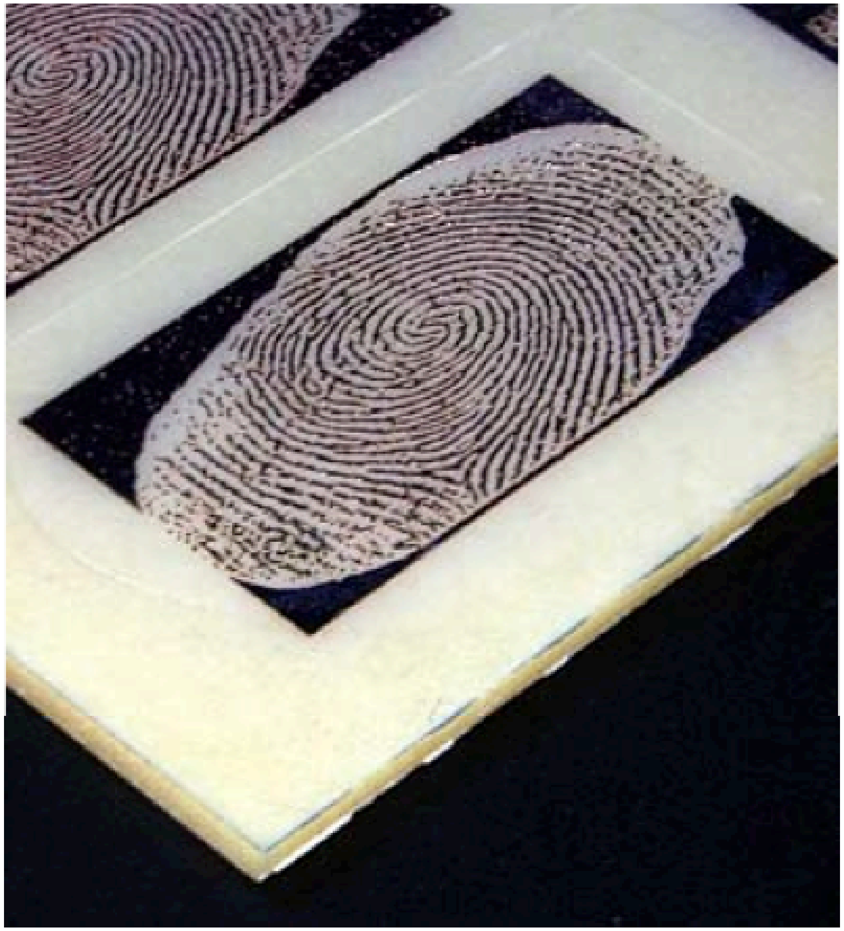
Put this mold into a refrigerator to cool, and then peel carefully.

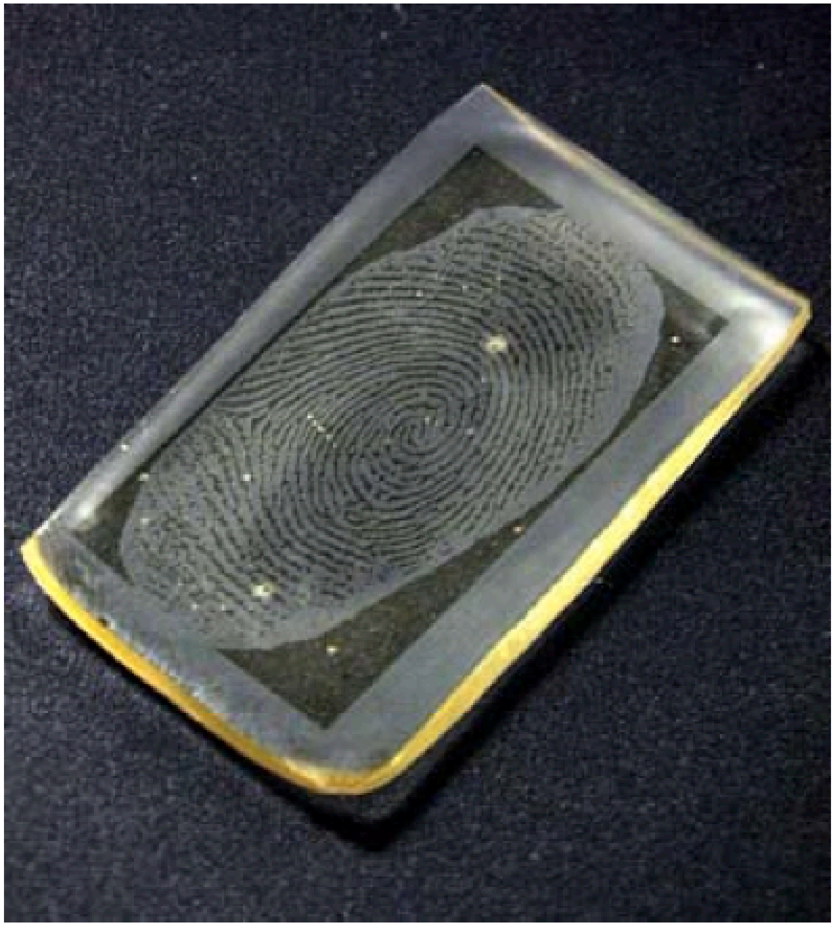


http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Involuntary

[Matsumoto]



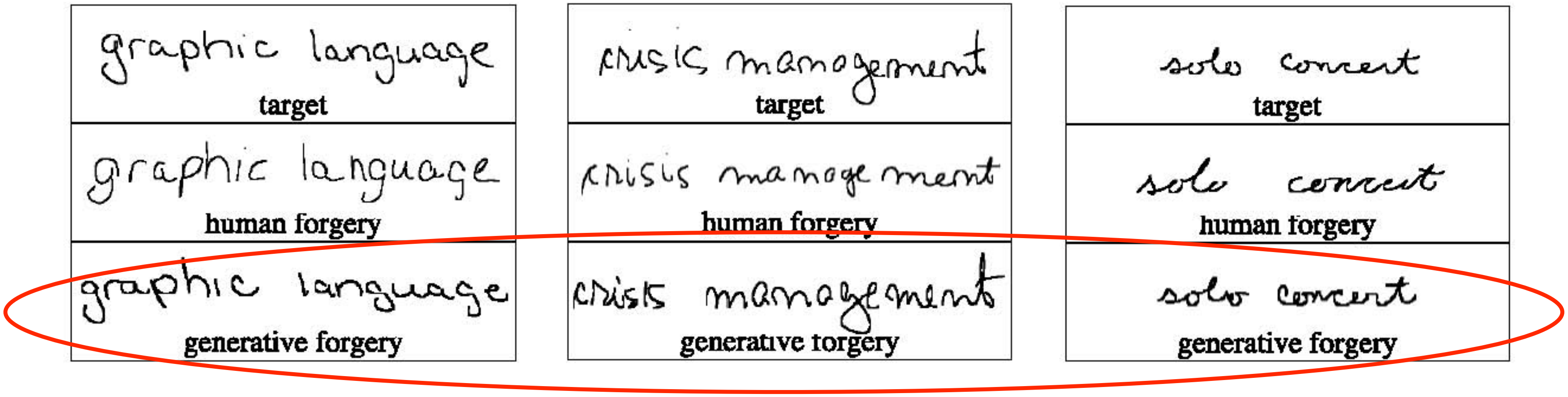


http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Authentication by Handwriting

[Ballard, Monrose, Lopresti]

- Maybe a computer could also forge some biometrics



Generated by computer algorithm trained on handwriting samples

Password Managers

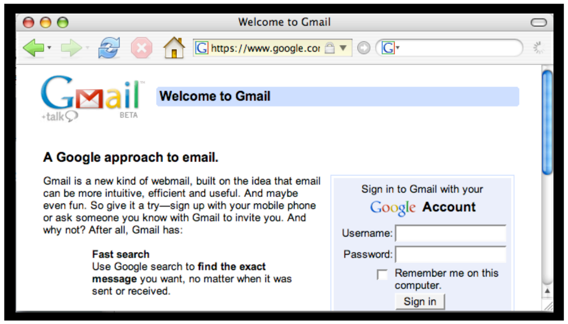
- Idea: Software application that will store and manage passwords for you.
  - You remember one password.
  - Each website sees a different password.
- Examples: PwdHash (Usenix Security 2005) and Password Multiplier (WWW 2005).

Key ideas

- User remembers a single 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

The problem

Alice needs passwords for all the websites that she visits



Welcome to Gmail

https://www.google.com

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:

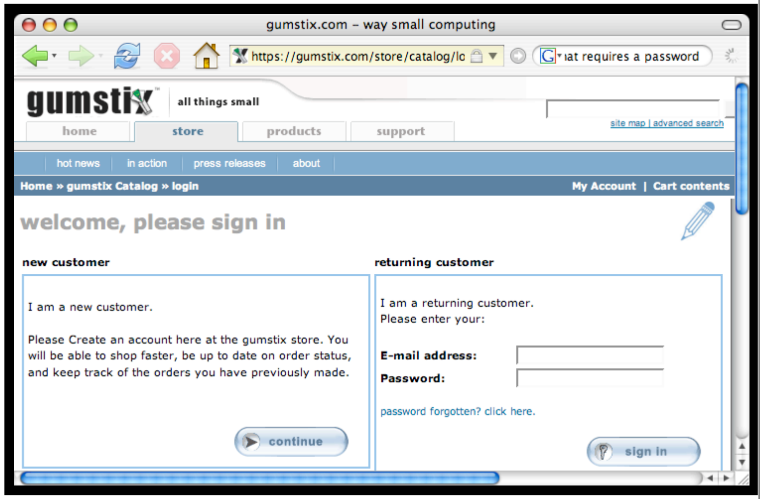
Fast search
Use Google search to **find the exact message** you want, no matter when it was sent or received.

Sign in to Gmail with your Google **Account**

Username:

Password:

□ Remember me on this computer.



gumstix.com – way small computing

https://gumstix.com/store/catalog/lo

ıat requires a password

Home » gumstix Catalog » login

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.

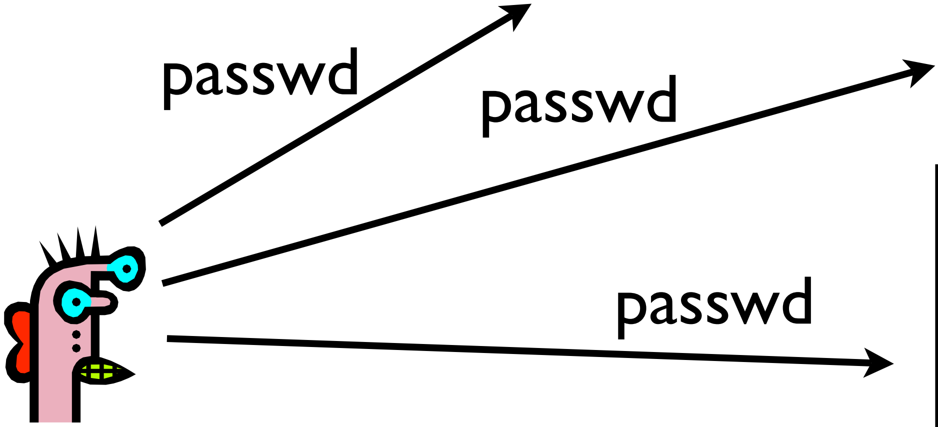
returning customer

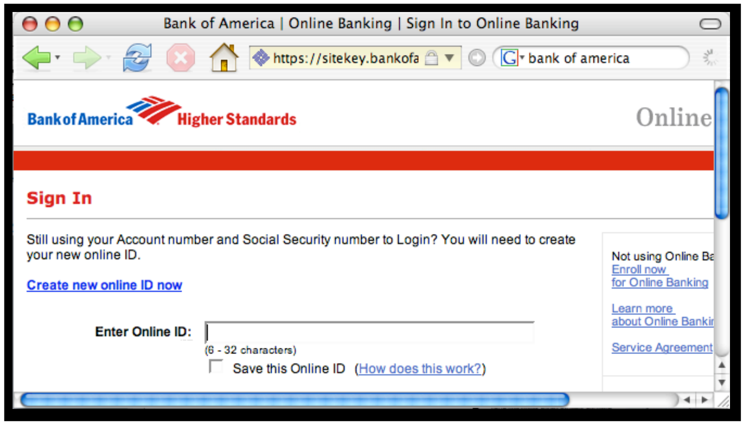
I am a returning customer.
Please enter your:

E-mail address:

Password:

password forgotten? click here.





Bank of America | Online Banking | Sign In to Online Banking

https://sitekey.bankofa

bank of america

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

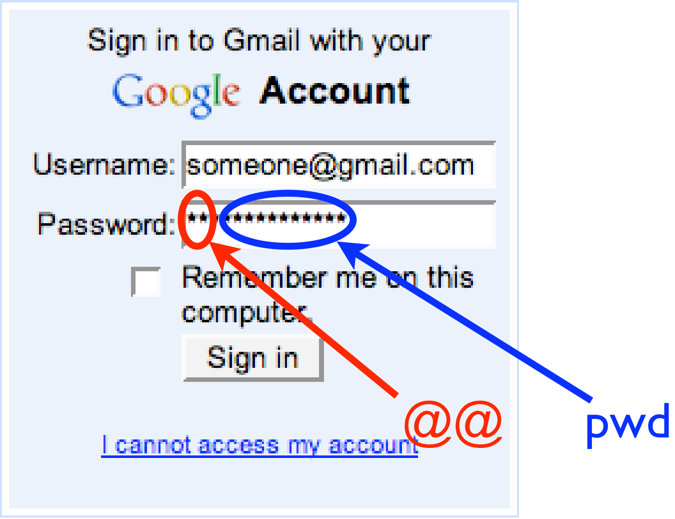
Possible solutions

- 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.

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)

PwdHash



Sign in to Gmail with your Google Account

Username: someone@gmail.com

Password: **************

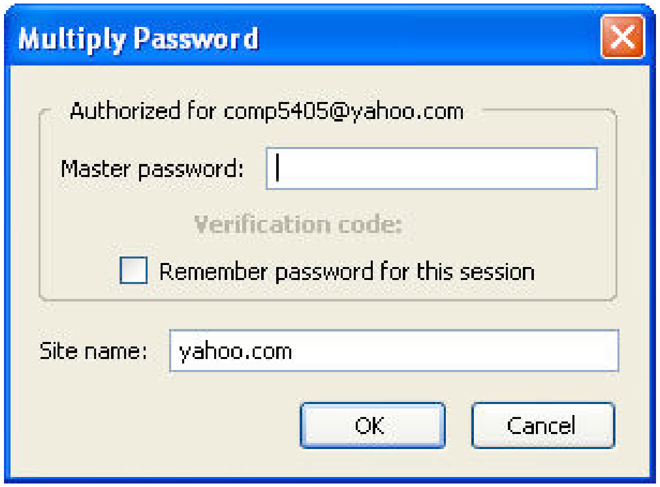
□ Remember me on this computer.

@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd,domain)

Prevent phishing attacks

Password Multiplier



Multiply Password

Authorized for comp5405@yahoo.com

Master password:

Verification code:

□ Remember password for this session

Site name: yahoo.com

Active with Alt-P or double-click

sitePwd = Hash(usrname, pwd, domain)

Both solutions target simplicity and transparency.

Usenix 2006:
Usabilty testing

- Are these programs usable? If not, what are the problems?
- Two main approaches for evaluating usability:
  - Usability inspection (no users)
    - Cognitive walk throughs
    - Heuristic evaluation
  - User study
    - Controlled experiments
    - Real usage

This paper stresses
need to observe real users

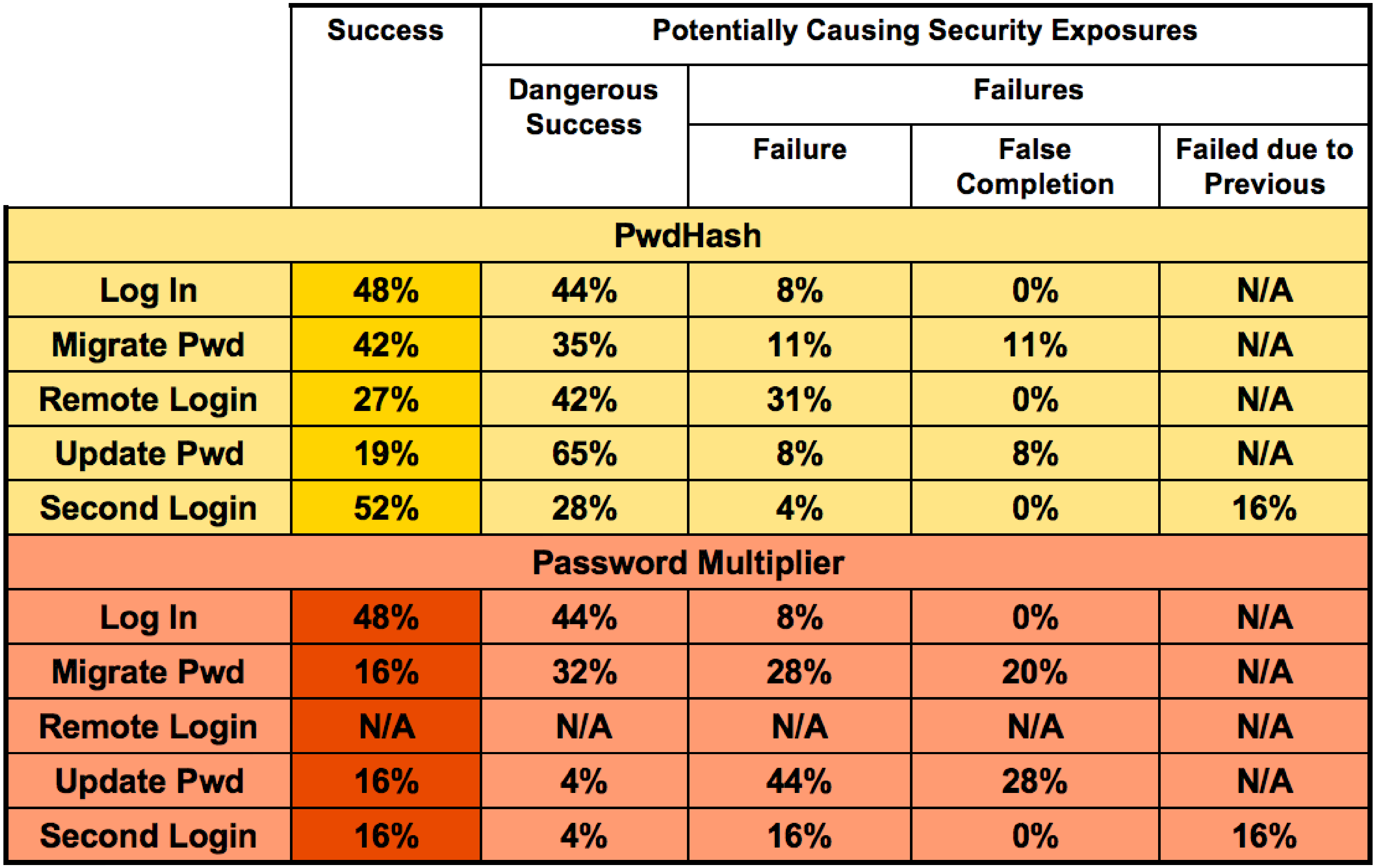
[Chiasson, van Oorschot, Biddle]

Study details

- 26 participants, across various backgrounds (4 technical)
- Five assigned tasks per plugin
- Data collection
    - Observational data (recording task outcomes, difficulties, misconceptions)
    - Questionnaire data (initial attitudes, opinions after tasks, post questionnaires)

[Chiasson, van Oorschot, Biddle]

Task completion results

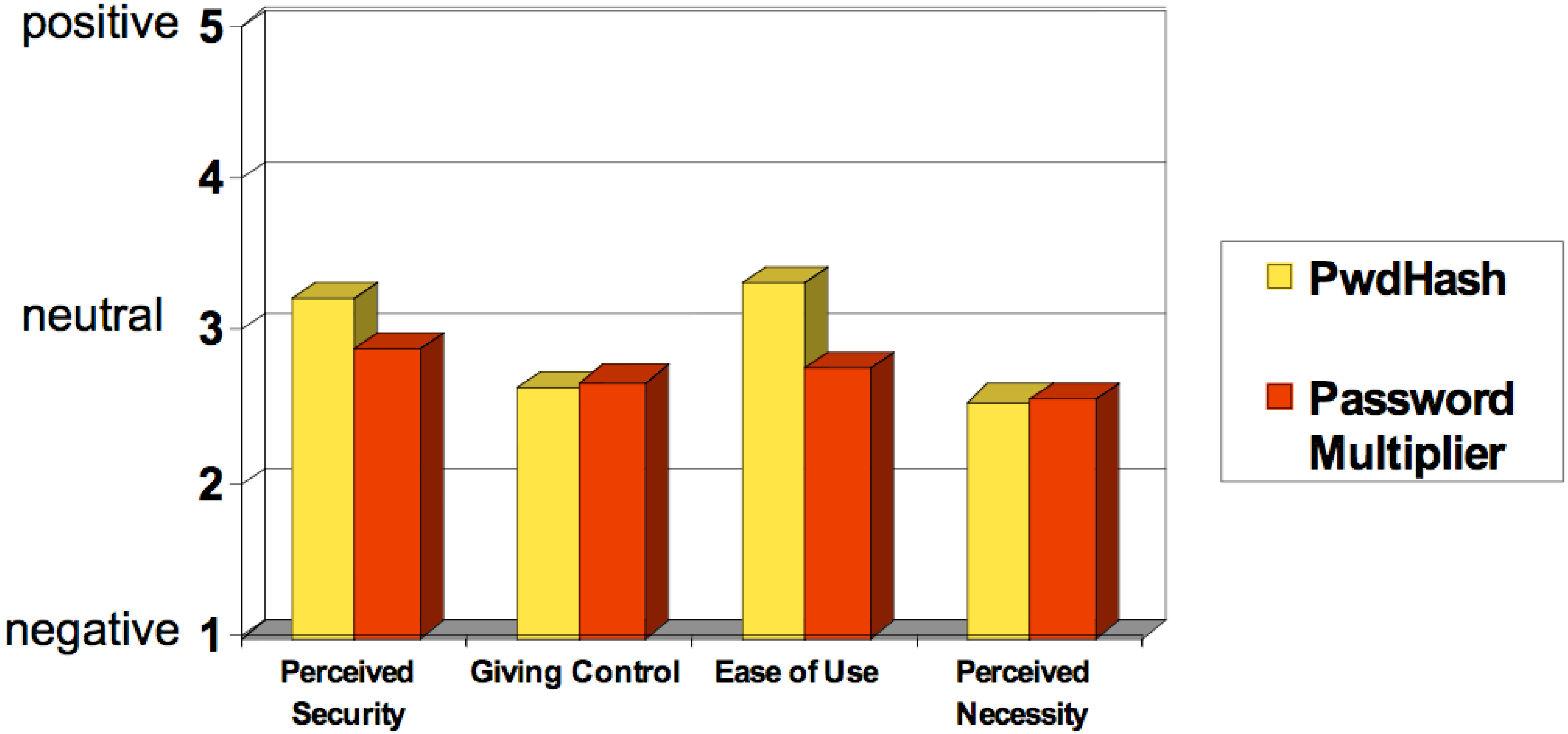


	Success	Potentially Causing Security Exposures			
		Dangerous Success	Failures		
			Failure	False Completion	Failed due to Previous
PwdHash					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	42%	35%	11%	11%	N/A
Remote Login	27%	42%	31%	0%	N/A
Update Pwd	19%	65%	8%	8%	N/A
Second Login	52%	28%	4%	0%	16%
Password Multiplier					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	16%	32%	28%	20%	N/A
Remote Login	N/A	N/A	N/A	N/A	N/A
Update Pwd	16%	4%	44%	28%	N/A
Second Login	16%	4%	16%	0%	16%

http://www.scs.carleton.ca/~schiasso/Chiasson_UsenixSecurity2006_PwdManagers.ppt

[Chiasson, van Oorschot, Biddle]

Questionnaire responses



http://www.scs.carleton.ca/~schiasso/Chiasson_UsenixSecurity2006_PwdManagers.ppt

Problem: Transparency

- Unclear to users whether actions successful or not.
  - Should be obvious when plugin activated.
  - Should be obvious when password protected.
- Users feel that they should be able to know their own password.

Problem: Mental model

Users seemed to have misaligned mental models

- Not understand that one needs to put "@@" before *each* password to be protected.
- Think different passwords generated for each session.
- Think successful when were not.
- Not know to click in field before Alt-P.
- PwdHash: Think passwords unique to them.

When “nothing works”

- Tendency to try all passwords
  - A poor security choice.
  - May make the use of PwdHash or Password Multiplier *worse* than not using any password manager.
- Usability problem leads to security vulnerabilities.