

CSE 484 (Winter 2011)

User 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 ...

Goals for Today

- ◆ Continue user authentication
- ◆ Lab 3 out soon (tentative out on Wednesday)
- ◆ Thank you for your feedback to CELT!
- ◆ TA office hours will move to labs in basement starting on Friday (after the lab 3 is announced)

Recovery Passwords

◆ <http://www.wired.com/threatlevel/2008/09/palin-e-mail-ha/>

Palin E-Mail Hacker Says It Was Easy

By [Kim Zetter](#)  September 18, 2008 | 10:05 am | Categories: [Elections](#), [Hacks and Cracks](#)

A person claiming to be the [hacker who](#)

obtained
private
supposed
revealed
took to
Republican

after the password recovery was reenabled, it took seriously 45 mins on wikipedia and google to find the info, Birthday? 15 seconds on wikipedia, zip code? well she had always been from wasilla, and it only has 2 zip codes (thanks online postal service!)

the second was somewhat harder, the question was "where did you meet your spouse?" did some research, and apparently she had eloped with mister palin after college, if you'll look on some of the screenshots that I took and other fellow anon have so graciously put on photobucket you will see the google search for "palin eloped" or some such in one of the tabs.

I found out later though more research that they met at high school, so I did variations of that, high, high school, eventually hit on "Wasilla high" I promptly changed the password to popcorn and took a cold shower...

Password Reuse

- ◆ <http://www.lightbluetouchpaper.org/2011/02/09/measuring-password-re-use-empirically/>



Measuring password re-use empirically

📅 February 9th, 2011 at 19:11 UTC by *Joseph Bonneau*

In the aftermath of Anonymous' [revenge hacking](#) of [HBGary](#) over the weekend, some enterprising hackers [used one of the stolen credentials](#) and some social engineering to gain root access at [rootkit.com](#), which has been down for a few days since. There isn't much novel about the hack but the dump of rootkit.com's SQL databases provides another password dataset for research, though an order of magnitude smaller than [the Gawker dataset](#) with just 81,000 hashed passwords.

More interestingly, due to the close proximity of the hacks, we can compare the passwords associated with email addresses registered at both Gawker and rootkit.com. This gives an interesting data point on the [widely known](#) problem

“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

◆ Password managers

◆ Two-factor authentication

- Leverages user’s phone (or other device) for authentication

Two-Factor Authentication (Last Week)

Google Introduces Two-Factor Authentication Option

Users can now generate a second, one-time password for Gmail and other accounts using a mobile phone

Feb 11, 2011 | 04:09 PM | [0 Comments](#)

By Tim Wilson
Darkreading

In an effort to help users increase the security of Gmail and other accounts, Google today introduced an option to add a second factor of authentication.

"As we announced to our Google Apps customers a few months ago, we've developed an advanced opt-in security feature called 2-step verification that makes your Google Account significantly more secure by helping to verify that you're the real owner of your account," Google says. "Now it's time to offer the same advanced protection to all of our users."

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

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.

Assumption: Easy to recall faces



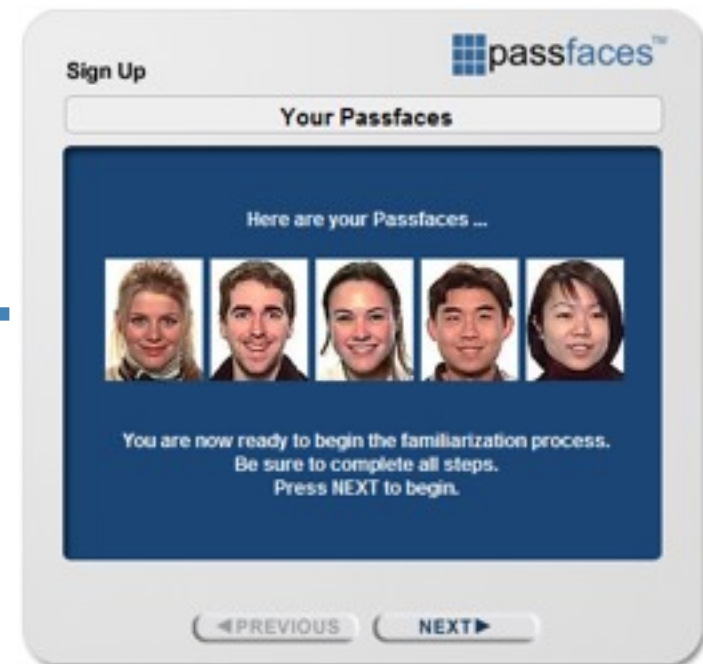
Slides from Kate Everitt

How Passfaces Works

Library of Faces



User Interface

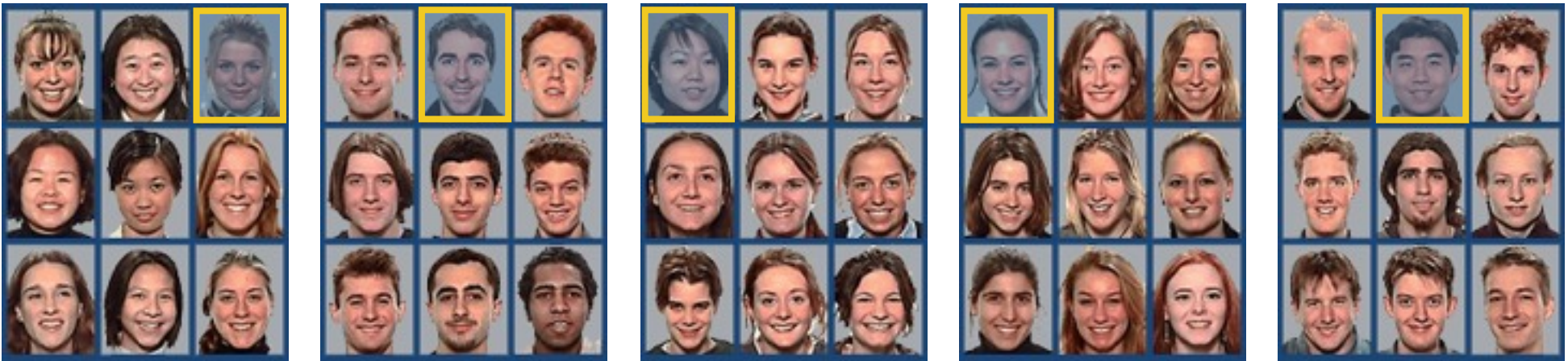


Users Are Assigned a Set of 5* Passfaces

* Typical implementation – 3 to 7 possible as standard

How Passfaces Works

- 5 Passfaces are Associated with 40 associated decoys
- Passfaces are presented in five 3 by 3 matrices each having 1 Passface and 8 decoys





The Only Fully Scalable Means to Replace or Reinforce Passwords



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

1	2	3																																																												
<table border="1"><tr><td>A</td><td></td><td></td><td></td></tr><tr><td></td><td>A</td><td></td><td></td></tr><tr><td></td><td></td><td>A</td><td></td></tr><tr><td></td><td>A</td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>A</td></tr></table>	A					A					A			A						A	<table border="1"><tr><td>B</td><td>B</td><td>B</td><td></td></tr><tr><td></td><td>B</td><td>B</td><td>B</td></tr><tr><td>B</td><td></td><td>B</td><td>B</td></tr><tr><td>B</td><td>B</td><td></td><td>B</td></tr><tr><td>B</td><td></td><td>B</td><td>B</td></tr></table>	B	B	B			B	B	B	B		B	B	B	B		B	B		B	B	<table border="1"><tr><td>B</td><td>B</td><td>B</td><td>A</td></tr><tr><td>A</td><td>B</td><td>B</td><td>B</td></tr><tr><td>B</td><td>A</td><td>B</td><td>B</td></tr><tr><td>B</td><td>B</td><td>A</td><td>B</td></tr><tr><td>B</td><td>A</td><td>B</td><td>B</td></tr></table>	B	B	B	A	A	B	B	B	B	A	B	B	B	B	A	B	B	A	B	B
A																																																														
	A																																																													
		A																																																												
	A																																																													
			A																																																											
B	B	B																																																												
	B	B	B																																																											
B		B	B																																																											
B	B		B																																																											
B		B	B																																																											
B	B	B	A																																																											
A	B	B	B																																																											
B	A	B	B																																																											
B	B	A	B																																																											
B	A	B	B																																																											
4	5																																																													
<table border="1"><tr><td>A</td><td>B</td><td>C</td><td>D</td></tr><tr><td>C</td><td>B</td><td>A</td><td>D</td></tr><tr><td>B</td><td>D</td><td>C</td><td>A</td></tr><tr><td>D</td><td>A</td><td>B</td><td>C</td></tr><tr><td>A</td><td>B</td><td>C</td><td>D</td></tr></table>	A	B	C	D	C	B	A	D	B	D	C	A	D	A	B	C	A	B	C	D	<table border="1"><tr><td>A</td><td>A</td><td>A</td><td>A</td></tr><tr><td>B</td><td>B</td><td>B</td><td>B</td></tr><tr><td>C</td><td>C</td><td>C</td><td>C</td></tr><tr><td>D</td><td>D</td><td>D</td><td>D</td></tr><tr><td>A</td><td>B</td><td>C</td><td>D</td></tr></table>	A	A	A	A	B	B	B	B	C	C	C	C	D	D	D	D	A	B	C	D																					
A	B	C	D																																																											
C	B	A	D																																																											
B	D	C	A																																																											
D	A	B	C																																																											
A	B	C	D																																																											
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

Variants...

- ◆ Plus click-based graphical passwords, drawing-based passwords, ...

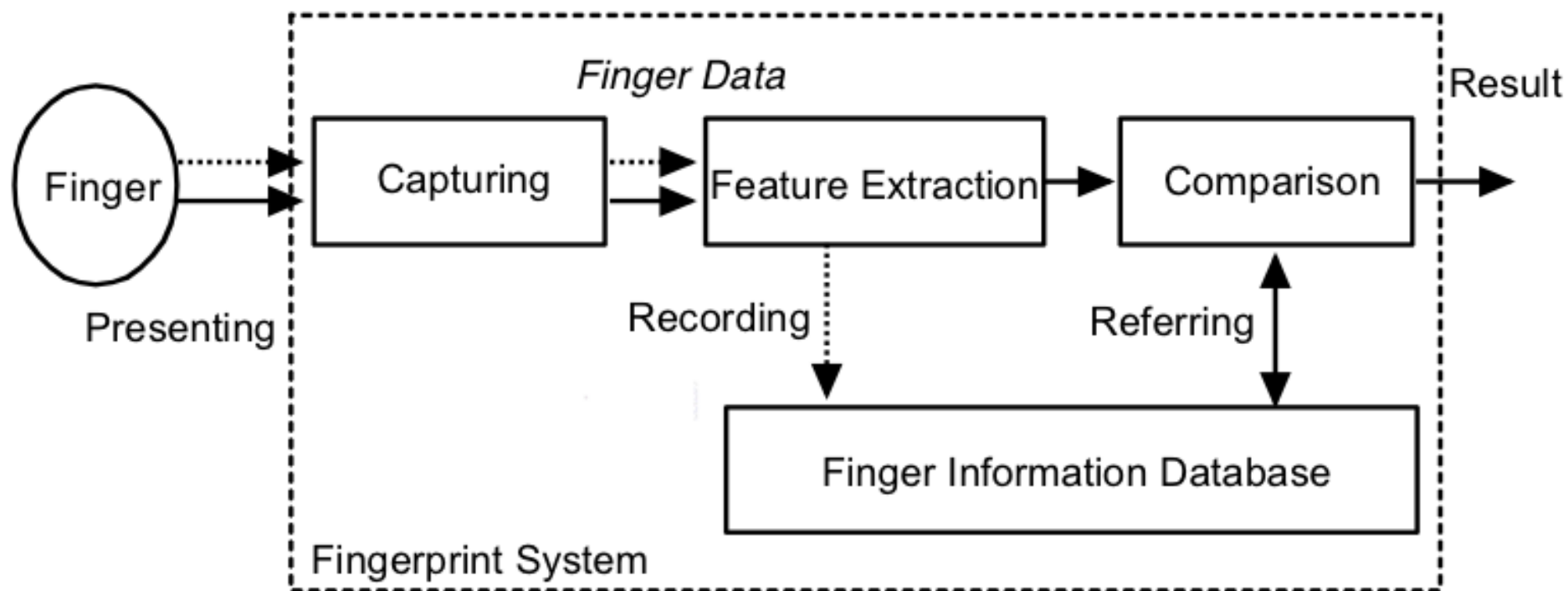
Uses of graphical passwords?

- ◆ 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 [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

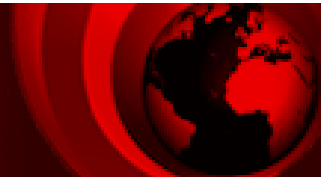
Issues with Biometrics

- ◆ 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

BBC
NEWS

 **OPEN** **The News in 2 minutes**



News services
Your news when
you want it

**News Front
Page**



Africa

Americas

Asia-Pacific

Europe

Middle East

South Asia

UK

Business

Health

Science/Nature

Technology

Entertainment

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

 [E-mail this to a friend](#)

 [Printable version](#)

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 against pirates](#)
16 Mar 05 | [Asia](#)

RELATED INTEREST

- ▶ [Malaysian police](#)
The BBC is not responsible for the content of internet sites

TOP ASIA-PACIFIC STORIES

- ▶ [Australians warn of cuts](#)
- ▶ [Taiwan campus](#)

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.

Voluntary: Making a Finger

[Matsumoto]



Pour the liquid into the mold.



Put it into a refrigerator to cool.

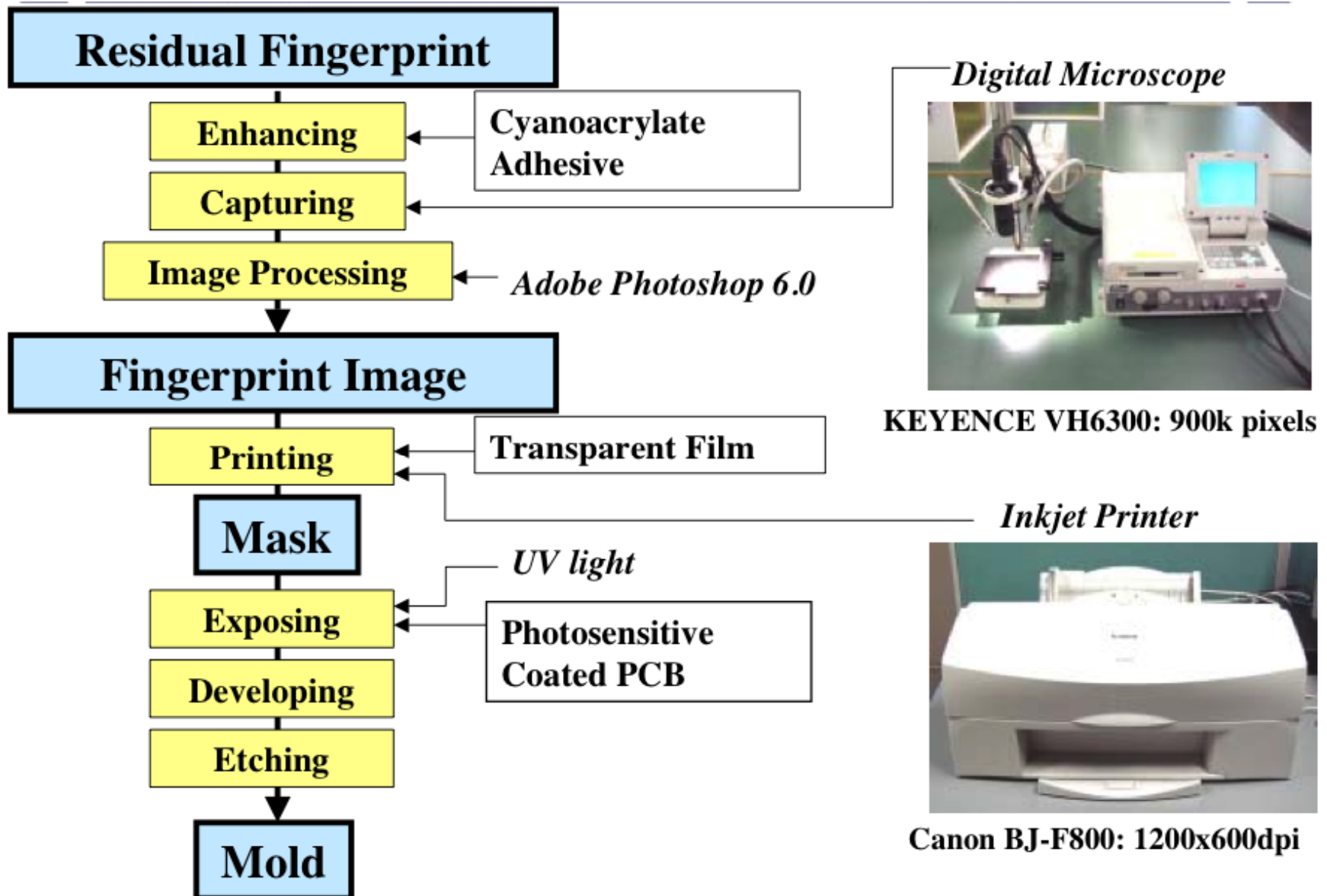


The gummy finger

It takes around 10 minutes.

Involuntary

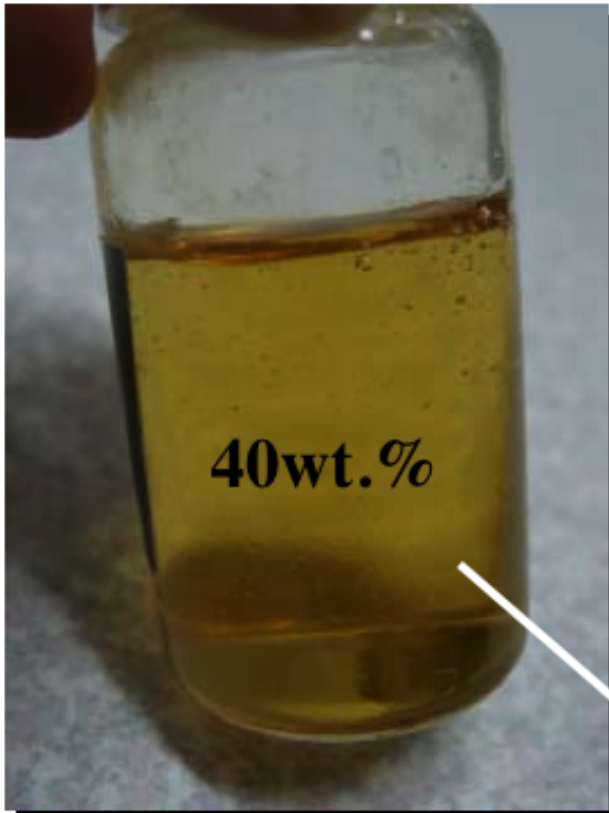
[Matsumoto]



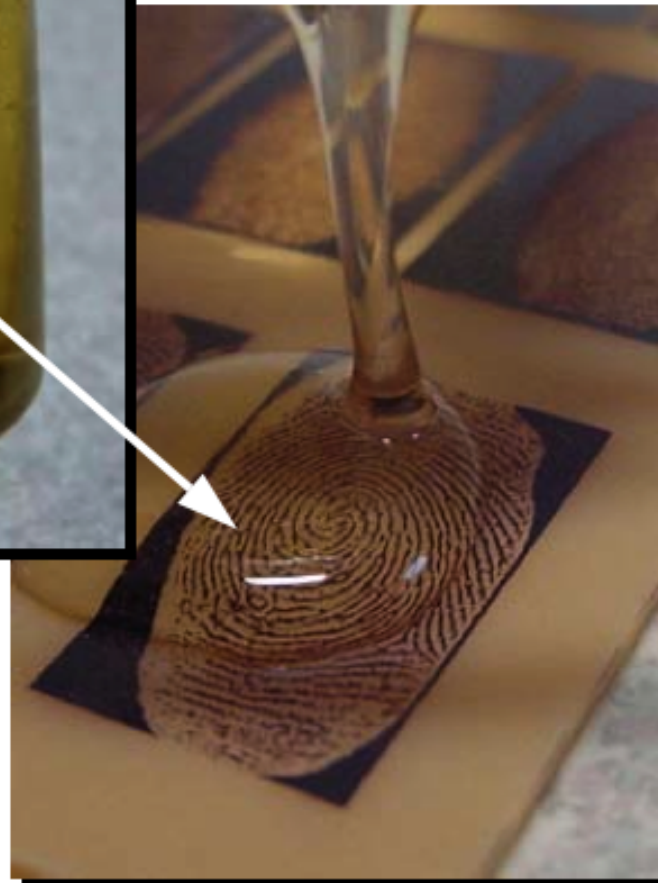
Involuntary

[Matsumoto]

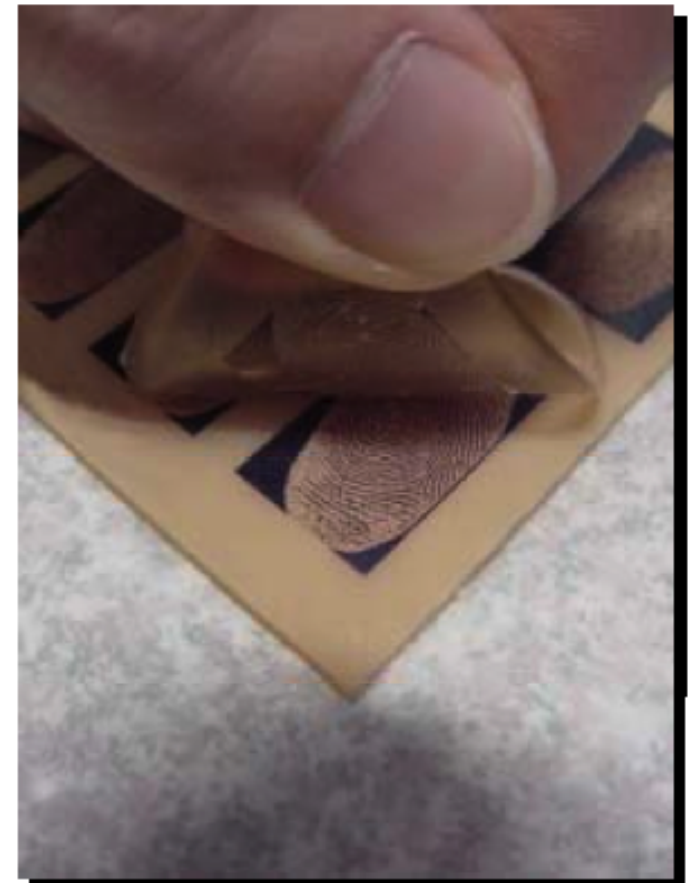
Gelatin Liquid



**Drip the liquid
onto the mold.**

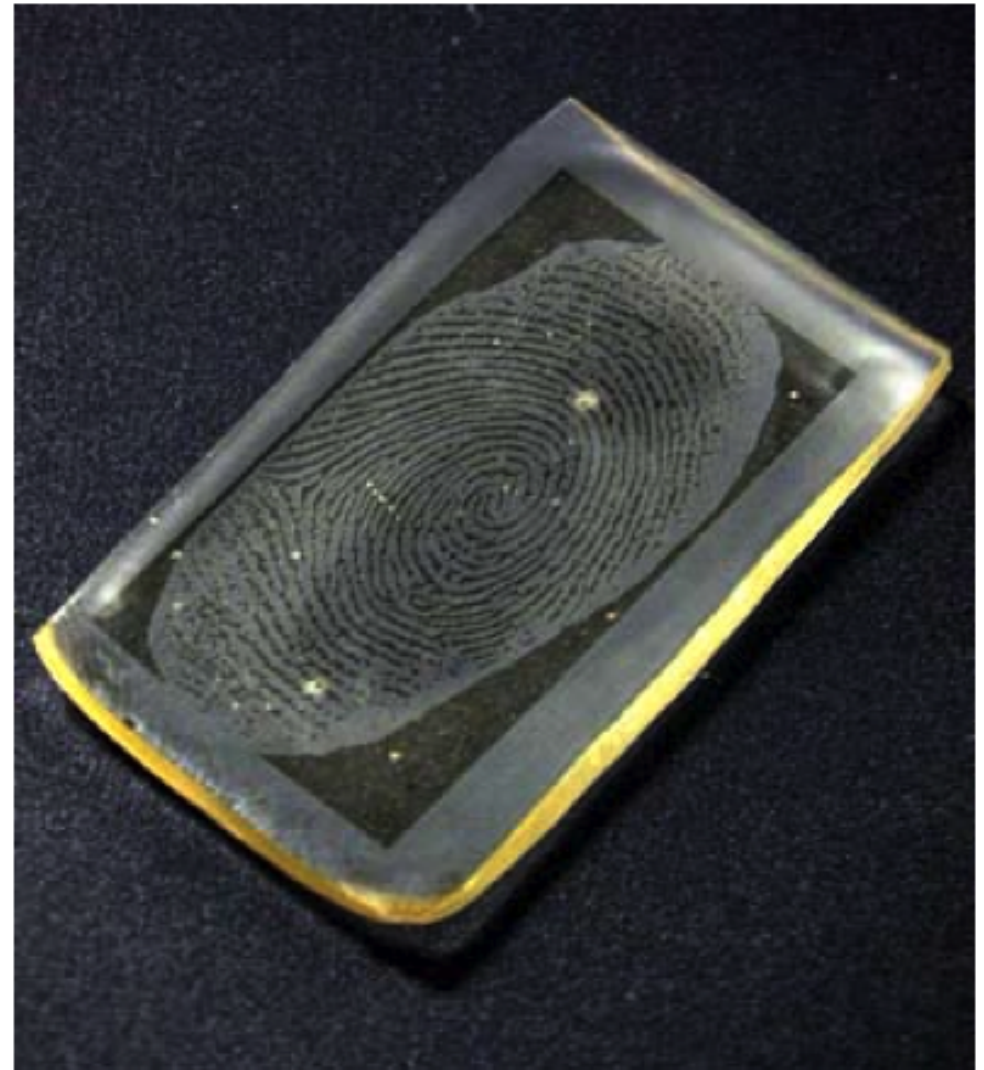


**Put this mold into
a refrigerator to cool,
and then peel carefully.**



Involuntary

[Matsumoto]



Authentication by Handwriting

[Ballard, Monrose, Lopresti]

- ◆ Maybe a computer could also forge some biometrics

graphic language target	crisis management target	solo concert target
graphic language human forgery	crisis management human forgery	solo concert human forgery
graphic language generative forgery	crisis management generative forgery	solo concert generative forgery

Generated by computer algorithm trained on handwriting samples

Password Managers

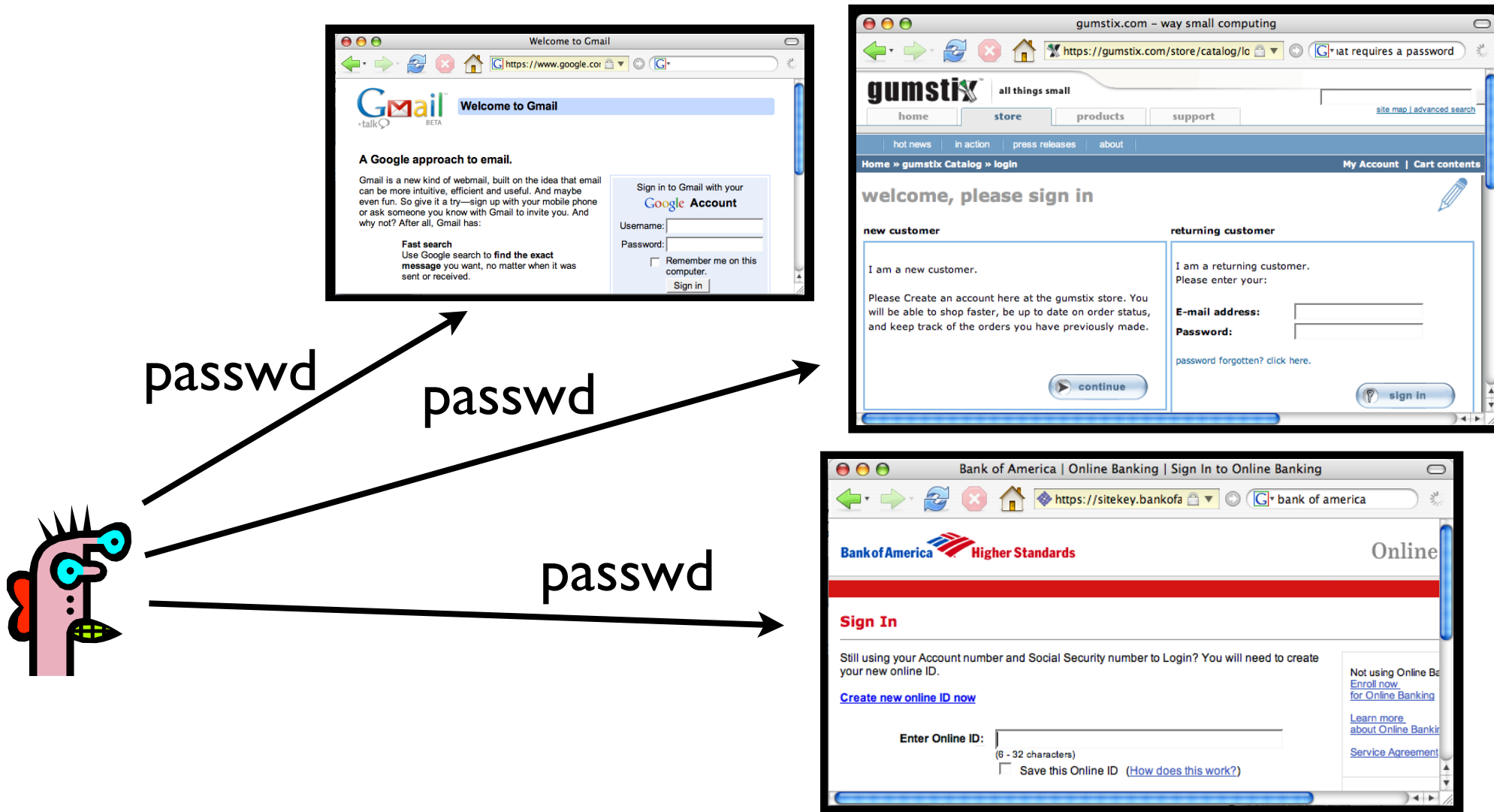
- Idea: Software application that will store and manage passwords for you.
- You remember one password.
- Each website sees a different password.
- Examples: [PwHash](#) (Usenix Security 2005) and [Password Multiplier](#) (WWW 2005).

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



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



@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd, domain)

Prevent phishing attacks

Password Multiplier



Active with Alt-P or double-click

sitePwd = Hash(username, pwd, domain)

Both solutions target simplicity and transparency.

Usenix 2006: Usability testing

HCI is important!

- 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 work stresses
need to observe real users

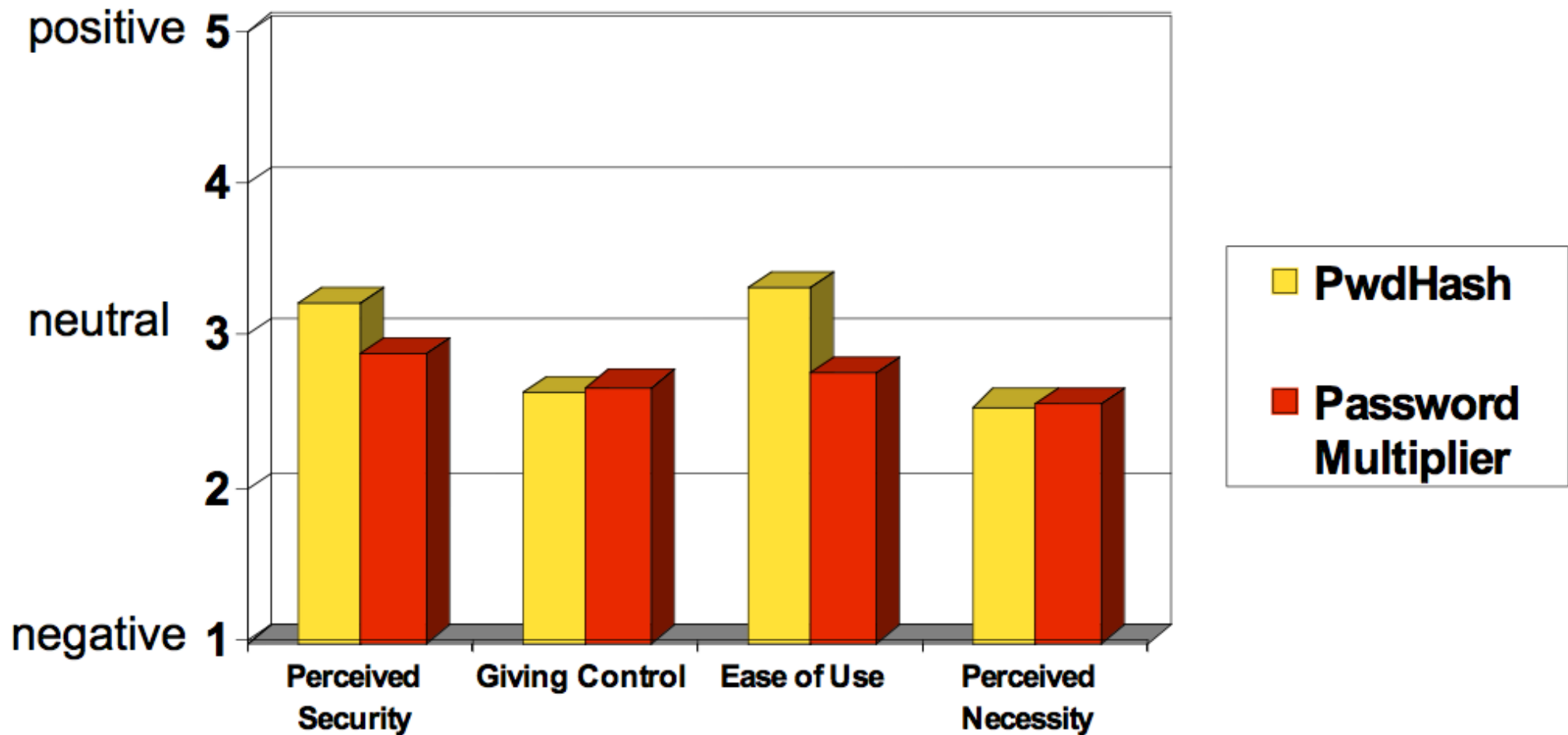
Study details

- 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)

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%

Questionnaire responses



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.

HCI is important!

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.