CSE 484 / CSE M 584 (Autumn 2011)

User Authentication

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, 11/07

- Homework #2
  - Due Wednesday @5pm
- Lab #2
  - Due week from Friday
  - Mail cse484-tas to get your group set up
- Office hours before HW #2 is due
  - Today and Wednesday in CSE 210 after class

Server Authentication

- Q: How should we store passwords on a server?

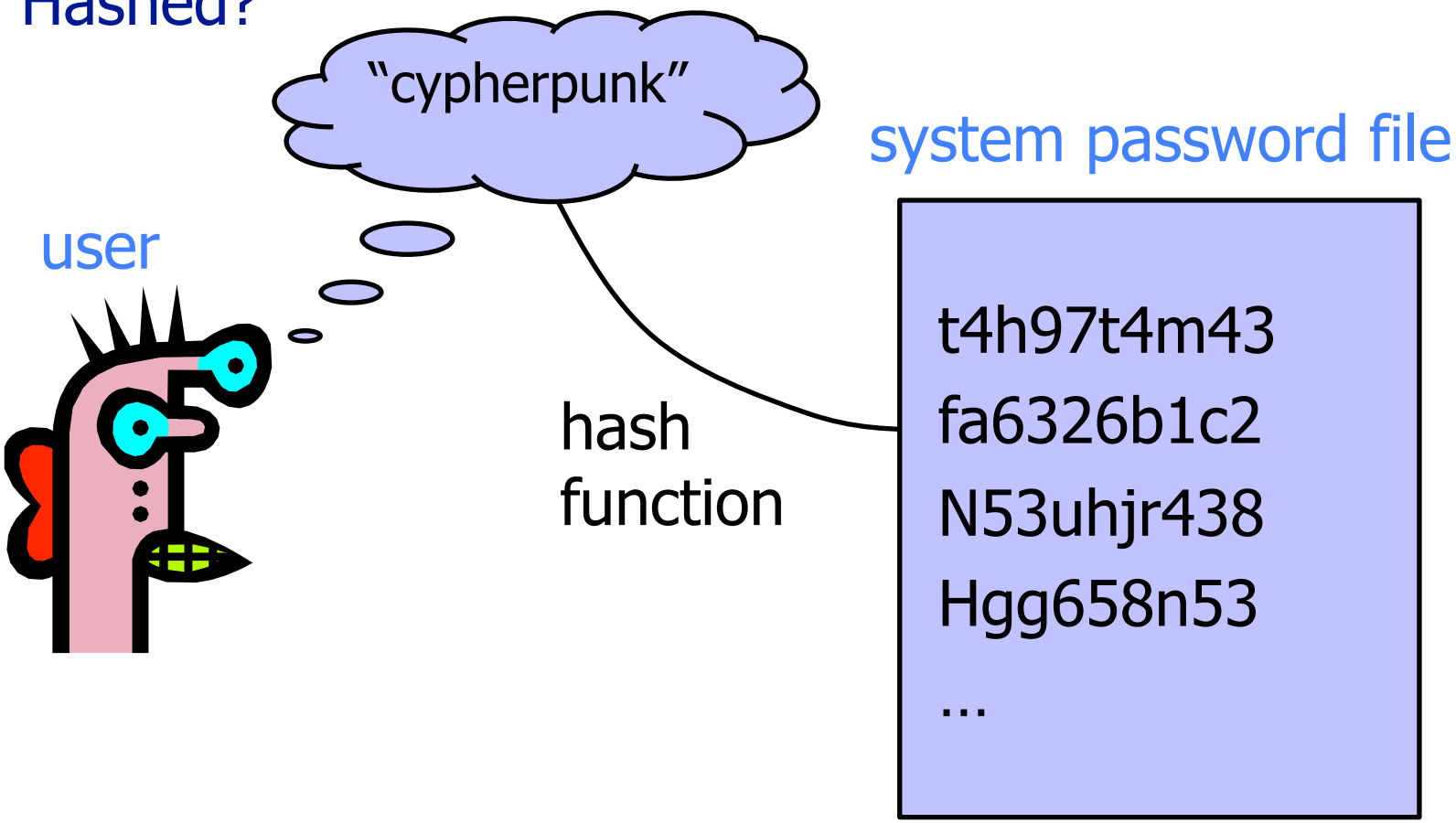
- Q2: What threats are you worried about?

UNIX-Style Passwords

- How should we store passwords on a server?
  - In cleartext?
  - Encrypted?
  - Hashed?

UNIX-Style Passwords

- How should we store passwords on a server?
  - In cleartext?
  - Encrypted?
  - Hashed?



Password Hashing

- Instead of user password, store H(password)
- When user enters password, compute its hash and compare with entry in password file
  - System does not store actual passwords!
  - System itself can't easily go from hash to password
    - Which would be possible if the passwords were encrypted
- Hash function H must have some properties
  - One-way: given H(password), hard to find password
    - No known algorithm better than trial and error
    - The attacker doesn't need to find **the** password, just **a** password that hashes to the stored value
  - "Slow" to compute

(Early) UNIX Password System

- Uses DES encryption as if it were a hash function
  - Encrypt NULL string using password as the key
    - Truncates passwords to 8 characters!
  - Artificial slowdown: run DES 25 times
    - Why 25 times? Slowdowns like these are important in practice!
  - ("Don't use DES like this at home.")
  - Can instruct modern UNIXes to use cryptographic hash function

(Early) UNIX Password System

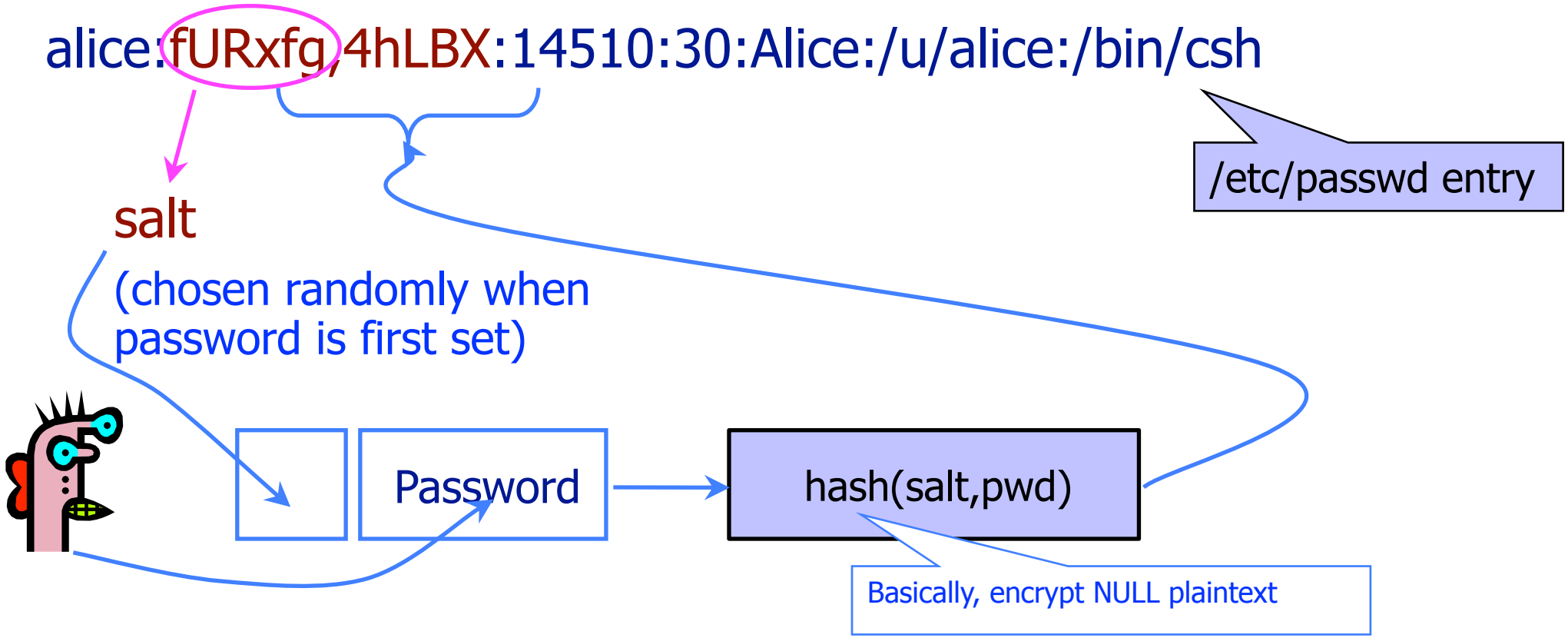
- Uses DES encryption as if it were a hash function
  - Encrypt NULL string using password as the key
    - Truncates passwords to 8 characters!
  - Artificial slowdown: run DES 25 times
    - Why 25 times? Slowdowns like these are important in practice!
  - ("Don't use DES like this at home.")
  - Can instruct modern UNIXes to use cryptographic hash function
- Problem: passwords are not truly random
  - With 52 upper- and lower-case letters, 10 digits and 32 punctuation symbols, there are $94^8 \approx$ 6 quadrillion possible 8-character passwords (around 2^{52})
  - Humans like to use dictionary words, human and pet names $\approx$ 1 million common passwords

Dictionary Attack

- Password file /etc/passwd is world-readable
  - Contains user IDs and group IDs which are used by many system programs
- Dictionary attack is possible because many passwords come from a small dictionary
  - Attacker can compute H(word) for every word in the dictionary and see if the result is in the password file
  - With 1,000,000-word dictionary and assuming 10 guesses per second, brute-force online attack takes 50,000 seconds (14 hours) on average
    - This is very conservative. Offline attack is much faster!
  - As described (H(word)), could just create dictionary of "word to H(word)" mapping once -- for all users!!

DEMO

Salt



- Users with the same password have <u>different</u> entries in the password file
- Online dictionary attack is still possible! (Precomputed dictionaries possible too -- but significantly more expensive.)

Advantages of Salting

- Without salt, attacker can pre-compute hashes of all dictionary words once for all password entries
  - Same hash function on all UNIX machines
  - Identical passwords hash to identical values; one table of hash values can be used for all password files
- With salt, attacker must compute hashes of all dictionary words once for each password entry
  - With 12-bit random salt, same password can hash to 2^{12} different hash values
  - Attacker must try all dictionary words for each salt value in the password file
- Pepper: Secret salt (not stored in password file)

Other Password Issues

- Keystroke loggers
  - Hardware
  - Software / Spyware
- Shoulder surfing
- Online vs offline attacks
  - Online: slower, easier to respond
- Multi-site authentication
  - Share passwords?


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!!!

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 access to Alaska Gov. Sarah Palin's private Yahoo e-mail on Tuesday has posted a supposed first-person account of the hack, revealing the relatively simple steps he says he took to crack the private e-mail of the Republican vice-presidential candidate.

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 obtaine private suppos revealir took to Republi

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 youll look on some of the screenshits 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

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.

Slides from Kate Everitt





Slides from Kate Everitt

Slides from Kate Everitt

Assumption: Easy to recall faces

Slides from Kate Everitt

How Passfaces Works

Library of Faces

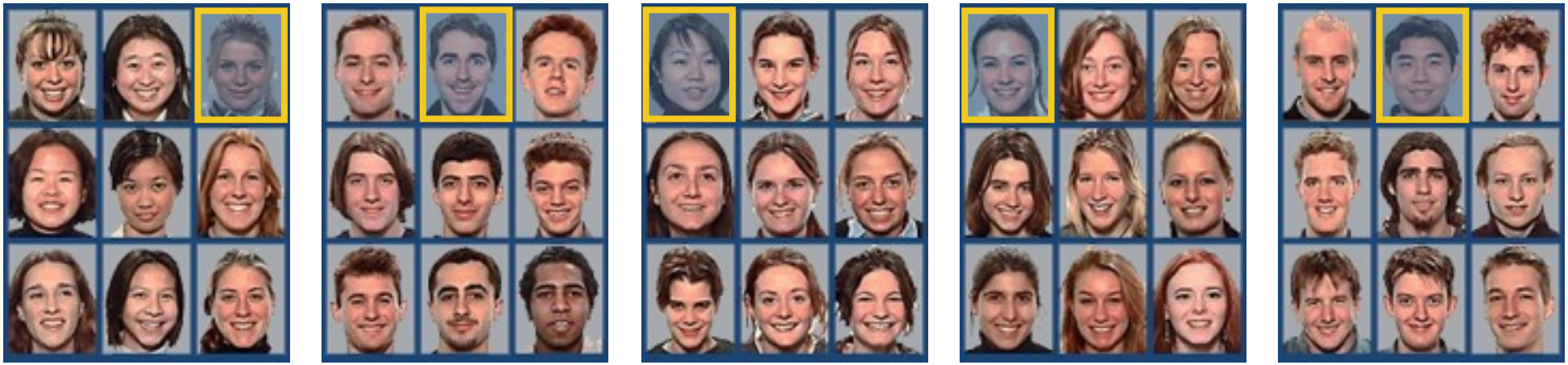
User Interface

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



passfaces™

STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords

passfaces™

STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords

passfaces™

STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords

passfaces™

STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords

passfaces™

STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords

passfaces™

STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords

passfaces™

STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords

Demo

passfaces™

You Have Successfully Logged on Using Passfaces

CONGRATULATIONS! You have successfully logged on using Passfaces, the ONLY Fully Scalable means to Replace or Reinforce Passwords. For more information on Passfaces, call 410.224.4848 or e-mail us at sales@passfaces.com

OK

passfaces™

STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords

Demo

passfaces™

You Have Successfully Logged on Using Passfaces

CONGRATULATIONS! You have successfully logged on using Passfaces, the ONLY Fully Scalable means to Replace or Reinforce Passwords. For more information on Passfaces, call 410.224.4848 or e-mail us at sales@passfaces.com

OK

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"

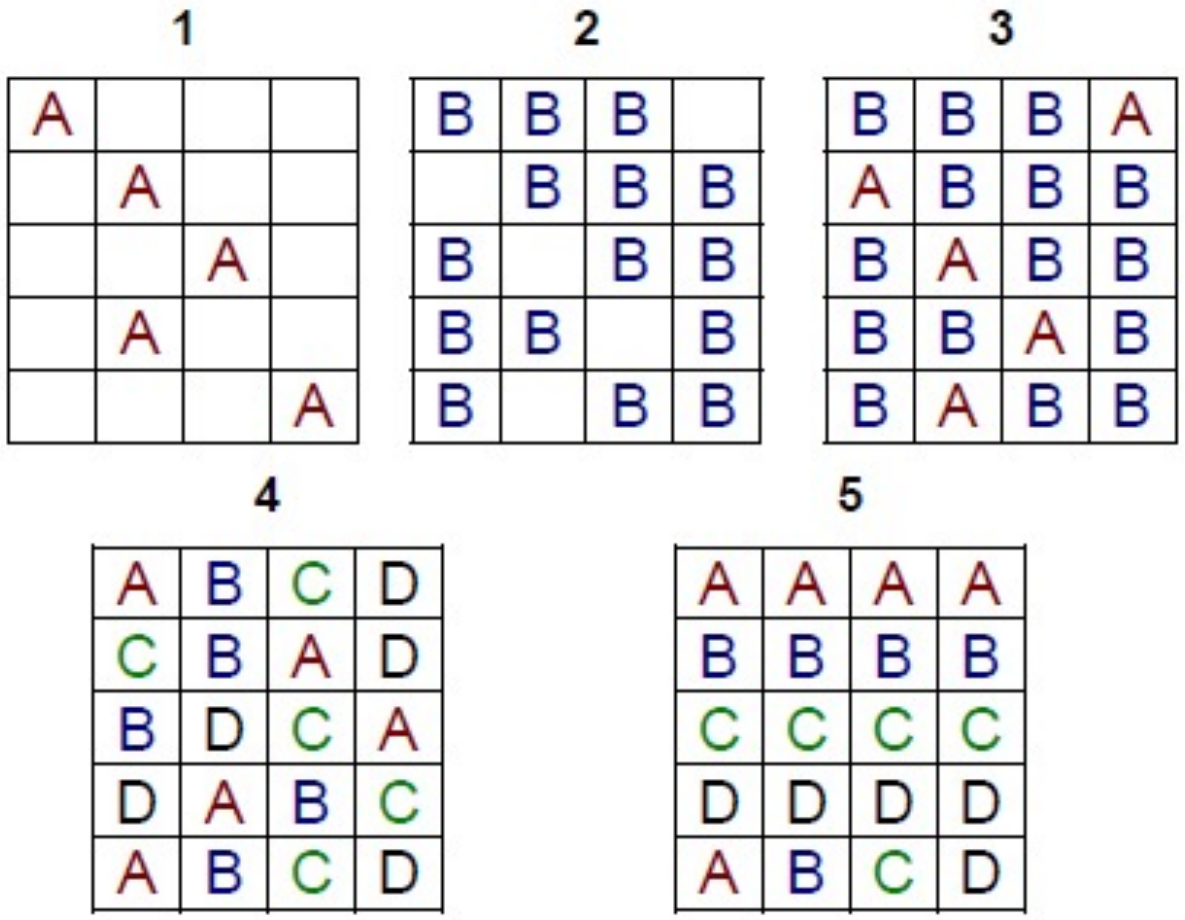
- Recommendation: system picks passfaces
- But is that still memorable? What issues could arise?

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

Study Conditions



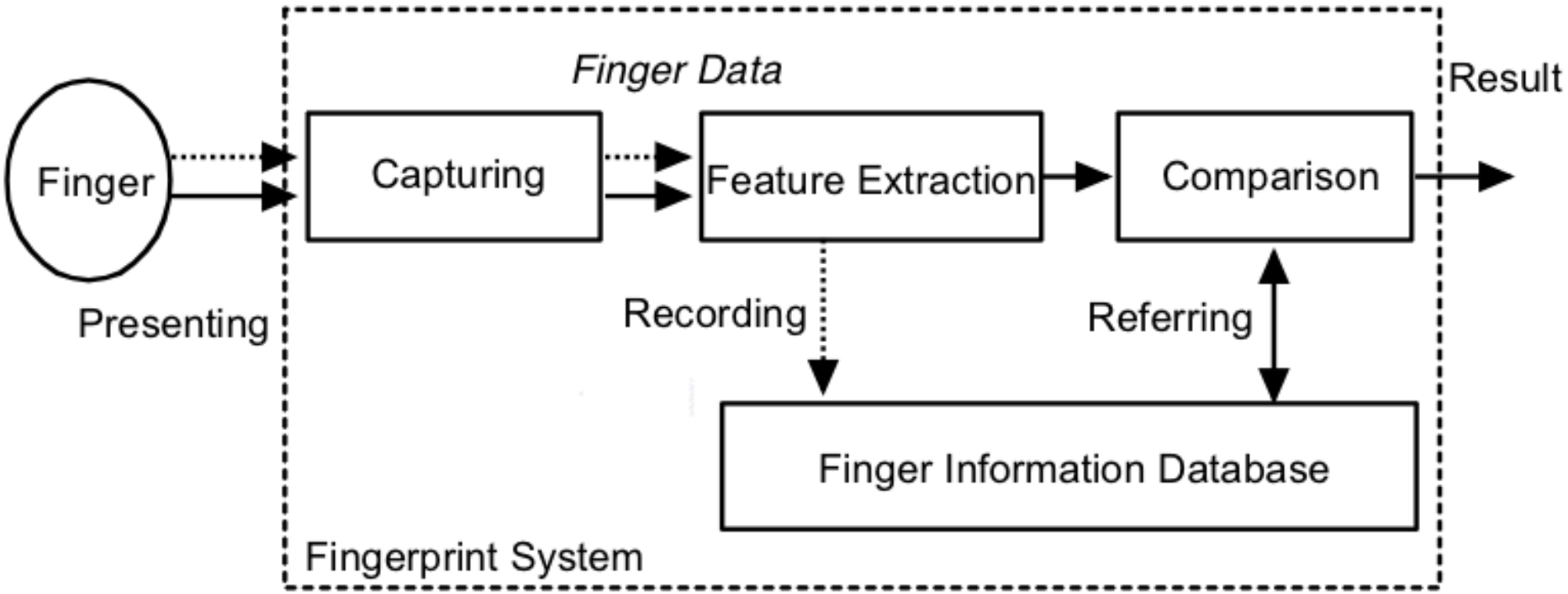
Frequency, interference, and training do play a role in memorability

Slides from Kate Everitt

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