CSE 484 / CSE M 584 (Winter 2013)

Authentication

Tadayoshi Kohno

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

Goals for Today

- Authentication
- Lab 2 due Wednesday
- Tentative plan:
  - Hw3 out this Thursday (tentative!)
  - Lab3 out on Monday
- Reminder: Transparencies are online

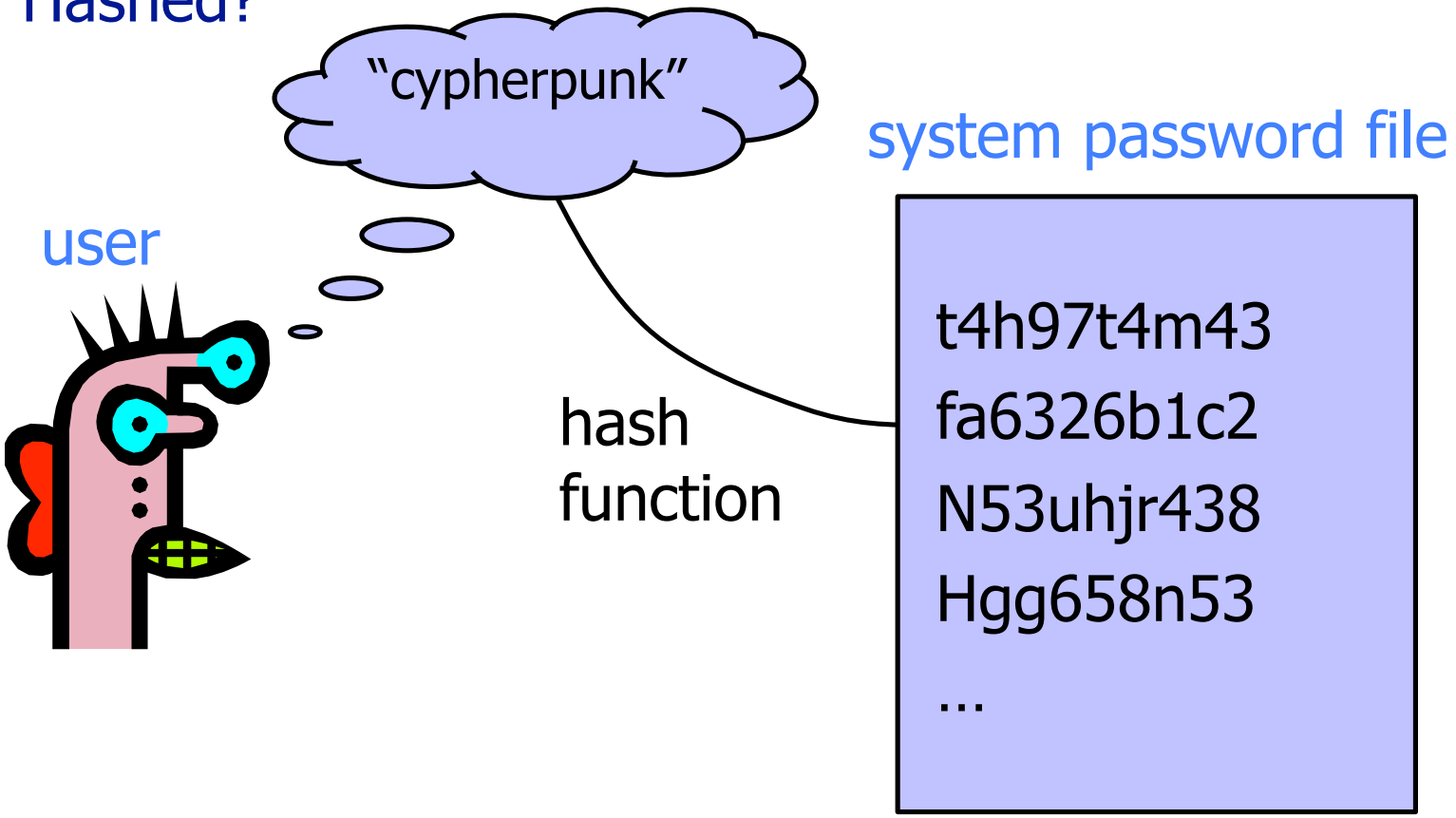
Server Authentication

- Q1: 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?



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.")
- Modern Unix systems, option between:
  - MD5
  - SHA-256
  - SHA-512
  - Blowfish (sometimes)

UNIX Password System

- Approach: Hash passwords
- 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

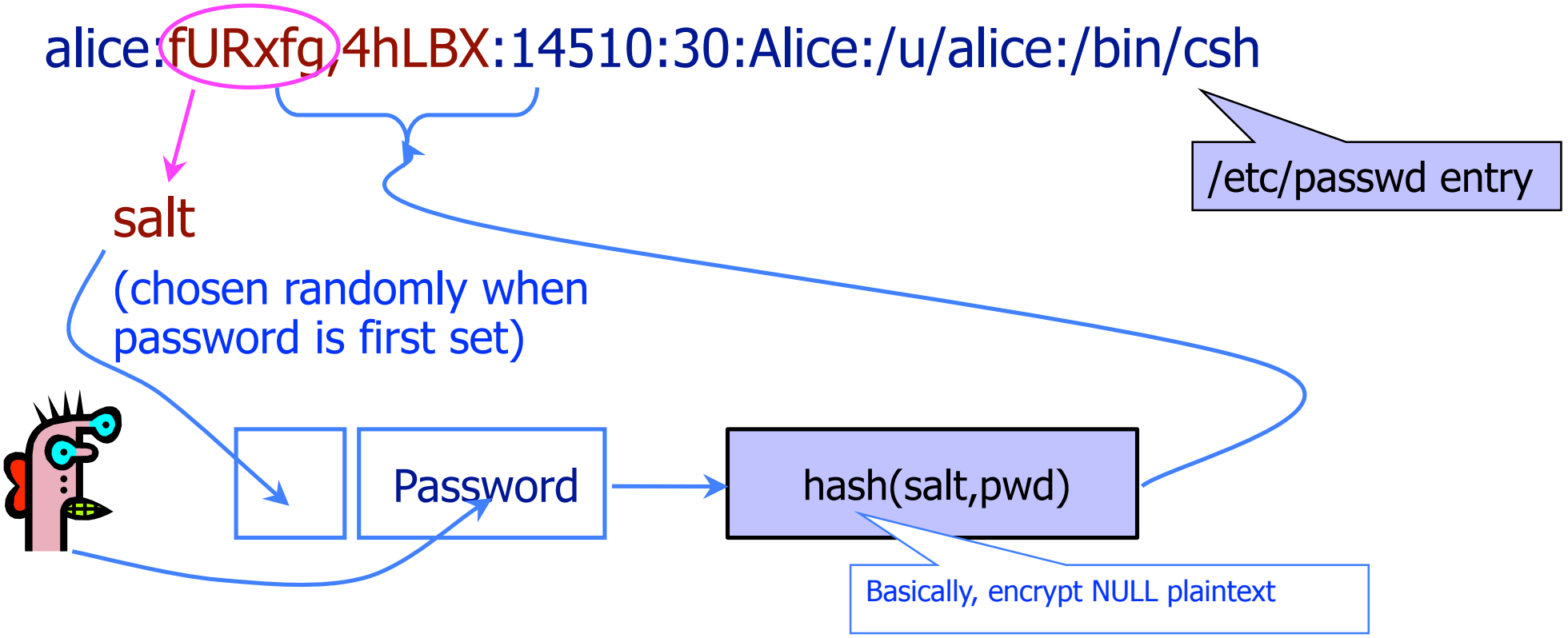
Dictionary Attack

- Password file /etc/passwd
  - World readable on some systems (especially older ones)
  - Could be accessed by attacker who compromises system
- 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!

Dictionary Attack

- Password file /etc/passwd
  - World readable on some systems (especially older ones)
  - Could be accessed by attacker who compromises system
- 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!!

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 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…

Wired cover story (Dec 2012)

Also in this issue

Kill the Password: Why a String of Characters Can't Protect Us Anymore

Password Reuse

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

Light Blue Touchpaper

Security Research, Computer Laboratory, University of Cambric

HOME | ABOUT | ARCHIVES | AUTHORS

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

Question?

- Q1: How do you handle passwords today?
- Q2: How would you like to handle passwords in the future?
  - Q2.1: What new things would you need to be created in order for you to do that?

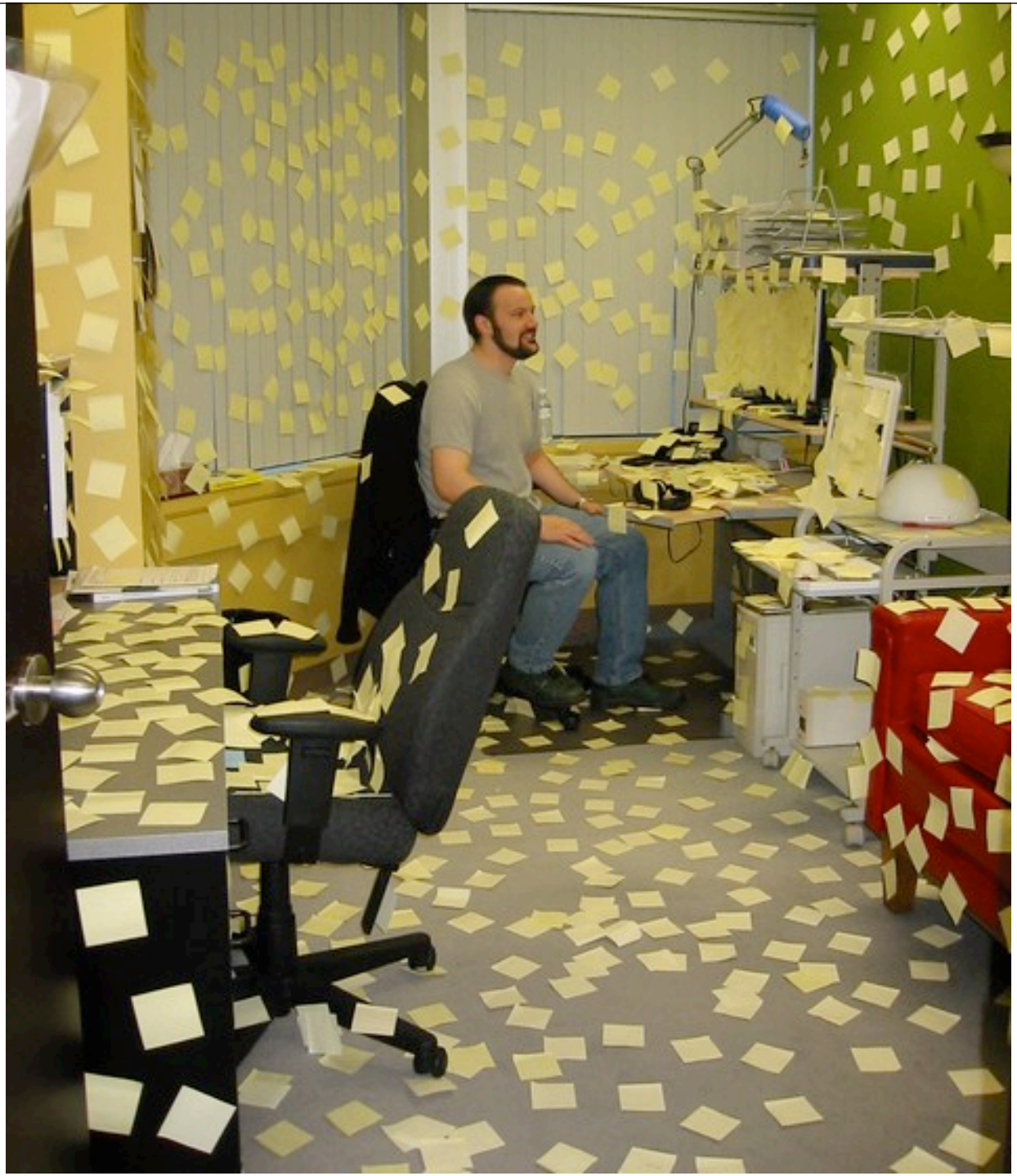


Image from http://www.interactivetools.com/staff/dave/damons_office/

Classroom Survey

Who here...

- repeats 1 password across many sites?
- uses 1 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?

"Improving" Passwords

- Add biometrics
  - For example, keystroke dynamics or voiceprint
  - Revocation is often a problem with biometrics
- Graphical passwords
  - Goal: easier to remember? no need to write down?
- Password managers
- Two-factor authentication
  - Leverages user's phone (or other device) for authentication

Two-Factor Authentication

Google Introduces Two-Factor Authentication Option

Users car … for Gmail

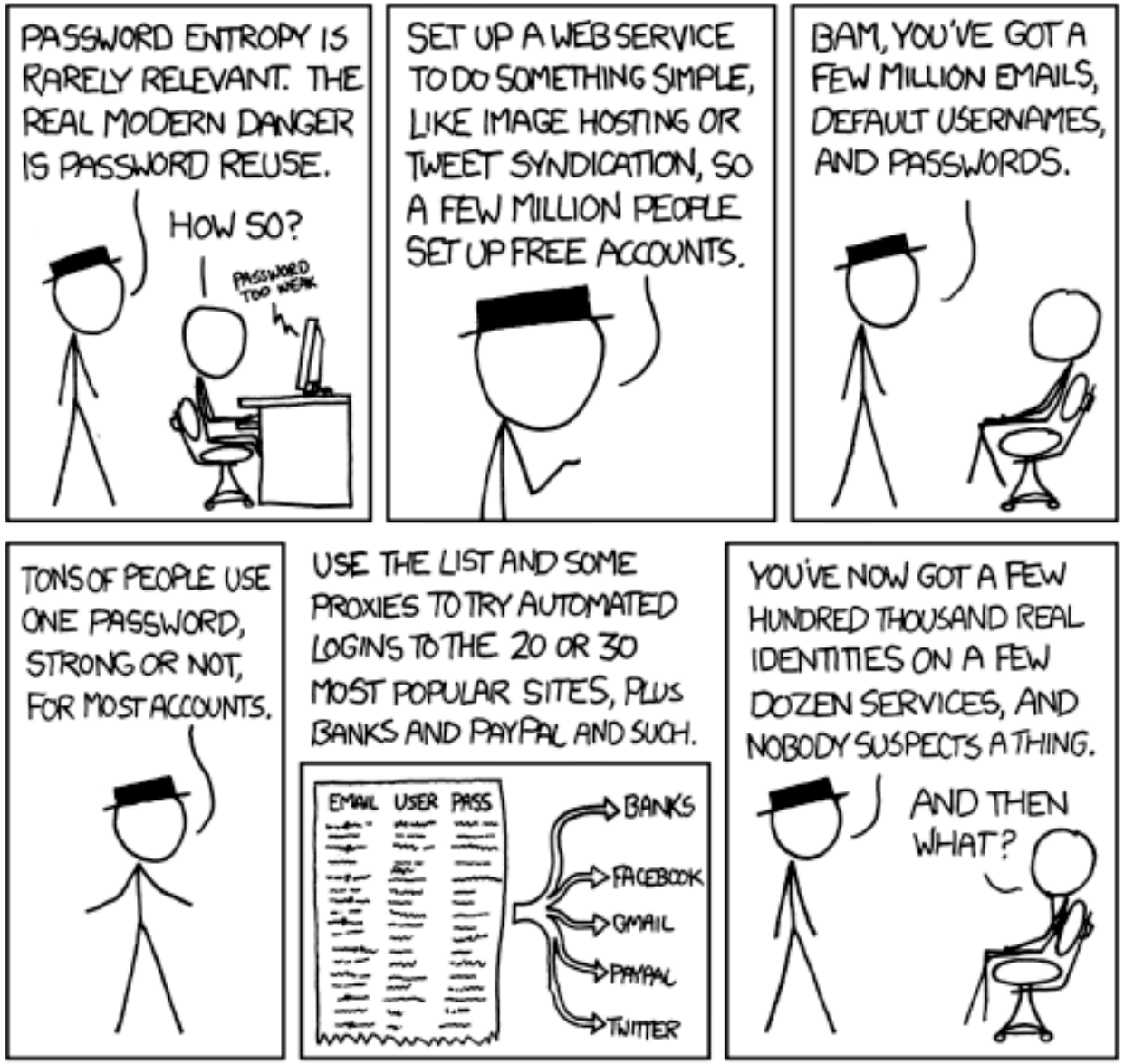
Feb 11, 2011

By Tim Wilso
Darkreading

In an effort t… accounts, G… authenticatio…

"As we anno… we've develo… verification t… helping to ve… "Now it's tim…

Password Reuse



UNCOMMON (NON-GIBBERISH) BASE WORD

ORDER UNKNOWN

Tr0ub4dor&3

CAPS?

COMMON SUBSTITUTIONS

NUMERAL

PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

~28 BITS OF ENTROPY

2^{28} = 3 DAYS AT 1000 GUESSES/SEC

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:

EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:

HARD

correct horse battery staple

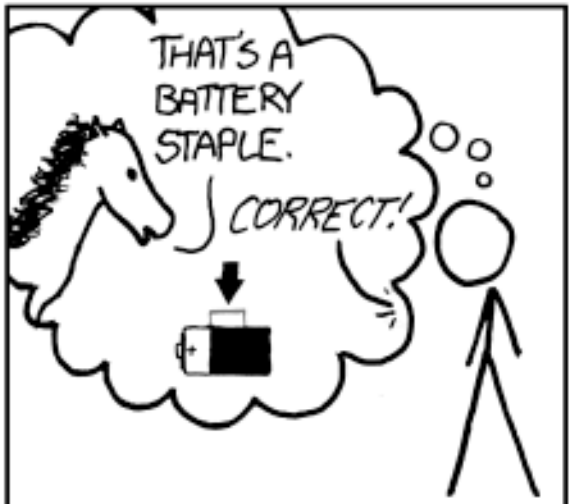
FOUR RANDOM COMMON WORDS

~44 BITS OF ENTROPY

2^{44} = 550 YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS:

HARD



DIFFICULTY TO REMEMBER:

YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Paper Published at SOUPS 2012:

Correct horse battery staple: Exploring the usability of system-assigned passphrases

Richard Shay, Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek,
Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University Pittsburgh, PA
{rshay,pgage,sarangak,mmazurek,bur,tvidas,lbauer,nicolasc,lorrie}@cmu.edu

ABSTRACT

Users tend to create passwords that are easy to guess, while system-assigned passwords tend to be hard to remember. Passphrases, space-delimited sets of natural language words, have been suggested as both secure and usable for decades. In a 1,476-participant online study, we explored the usability of 3- and 4-word system-assigned passphrases in comparison to system-assigned passwords composed of 5 to 6 random characters, and 8-character system-assigned pronounceable passwords. Contrary to expectations, system-assigned passphrases performed similarly to system-assigned passwords of similar entropy across the usability metrics we examined. Passphrases and passwords were forgotten at similar rates, led to similar levels of user difficulty and annoyance, and were both written down by a majority of participants. However, passphrases took significantly longer for participants to enter, and appear to require error-correction to counteract entry mistakes. Passphrase usability did not seem to increase when we shrunk the dictionary from which words were chosen, reduced the number of words in a passphrase, or allowed users to change the order of words.

in an effort to prevent users from choosing passwords that are too easily guessed [10]. Unfortunately, strict password-composition policies sometimes lead to user frustration without substantial security benefit [1, 23]. Also, even under a strict policy, users may fulfill policy requirements in predictable ways [54], such as basing their passwords on older passwords, names, or words [51, 60], or reusing passwords across domains [17].

One approach to making passwords more secure is to remove user choice and have the authentication system generate passwords randomly. Such *system-assigned* passwords can be guaranteed to be sufficiently difficult to guess, although they have been perceived as difficult to remember and type [37].

A *passphrase* is a password composed of a sequence of words. Passphrases are typically much longer than ordinary passwords, and proponents argue that they are more secure and easier to remember. One NIST publication states that "any long password that can be remembered must necessarily be a 'pass-phrase' composed of dictionary words" [10]. The use of passphrases has recently garnered appreciable attention [40, 49], and some institutions have adopted passphrases as a password policy (e.g., [58]). Despite this

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 (even if above true)
  - Need infrastructure for displaying and storing images
  - Shoulder surfing

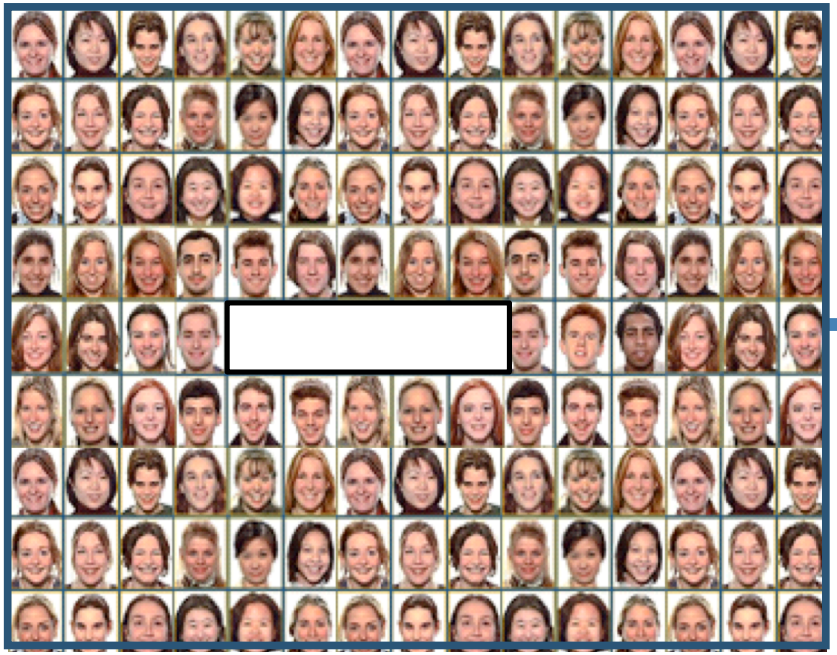
Graphical Password Systems

- *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

How Passfaces Works

Library of Faces



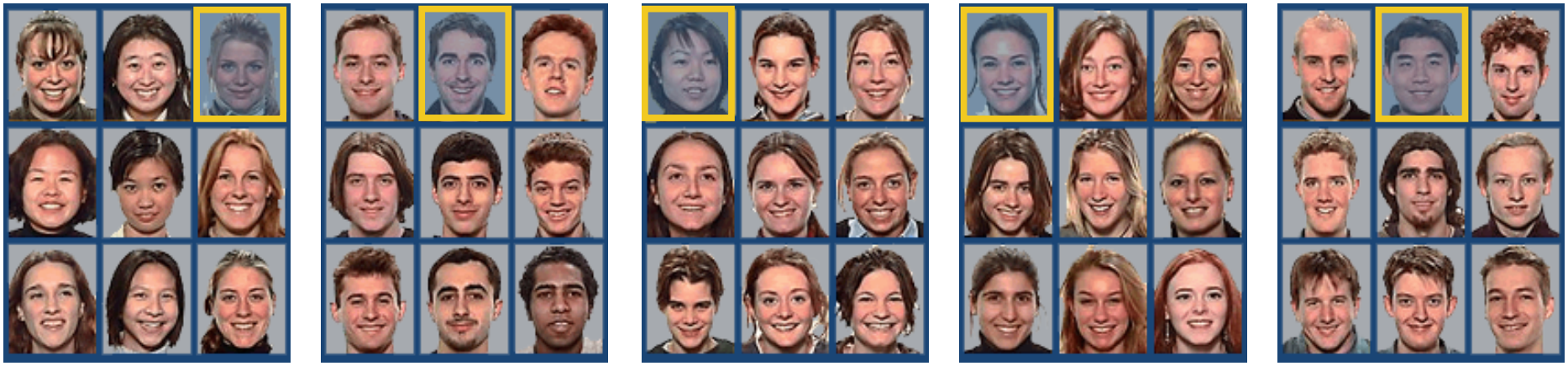
User Interface

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

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

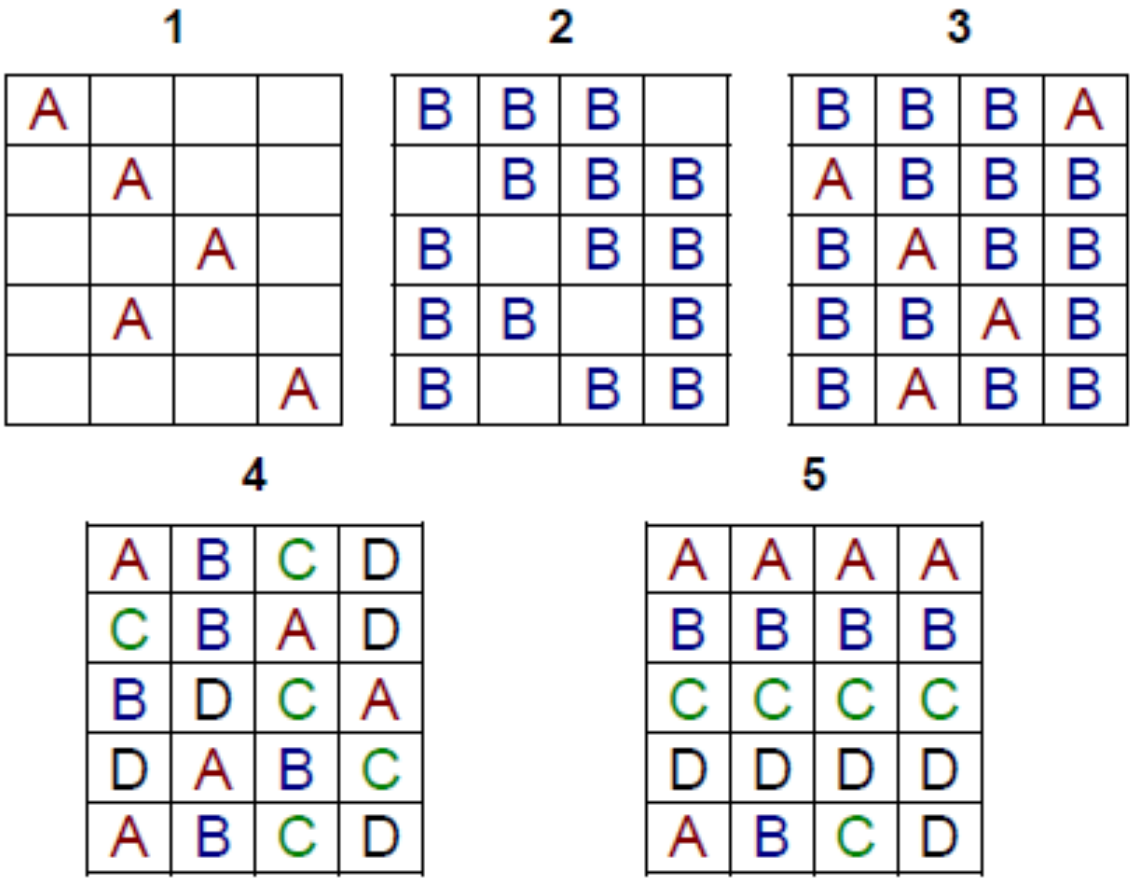
- Experimental study of 154 computer science students at Johns Hopkins and Carnegie Mellon
- Conclusions:
  - "… faces chosen by users are highly affected by the race of the user… the gender and attractiveness of the faces bias password choice… In the case of male users, we found this bias so severe 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

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

Variants...

- Recall that there also exist: click-based graphical passwords, drawing-based passwords, ...

Uses of graphical passwords?

- For what applications might graphical passwords be particularly useful?

Multi-Factor Authentication

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

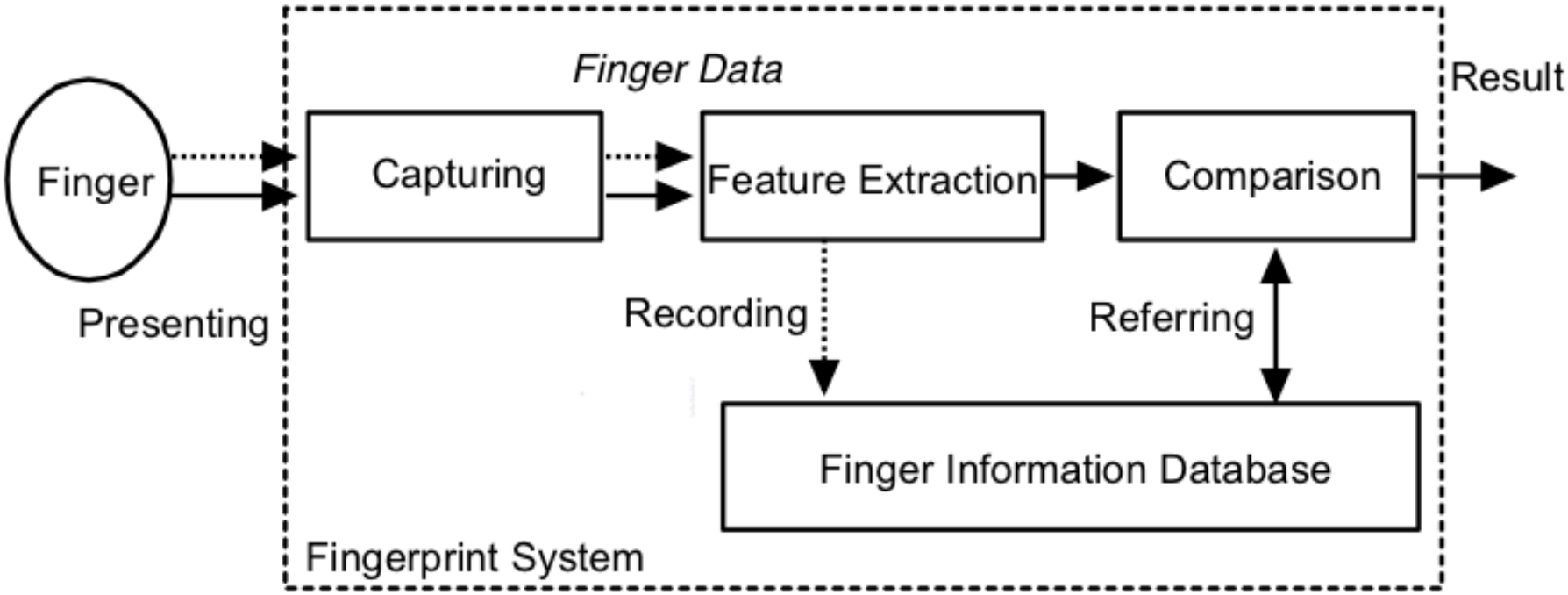
For better security, require **two or more factors:**

- 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

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?
- 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 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 pirates
16 Mar 05 | As

RELATED INTER
- Malaysian police

The BBC is not r for the content o internet sites

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

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