CSE 484 / CSE M 584: Computer Security and Privacy

Authentication and Passwords

Spring 2017

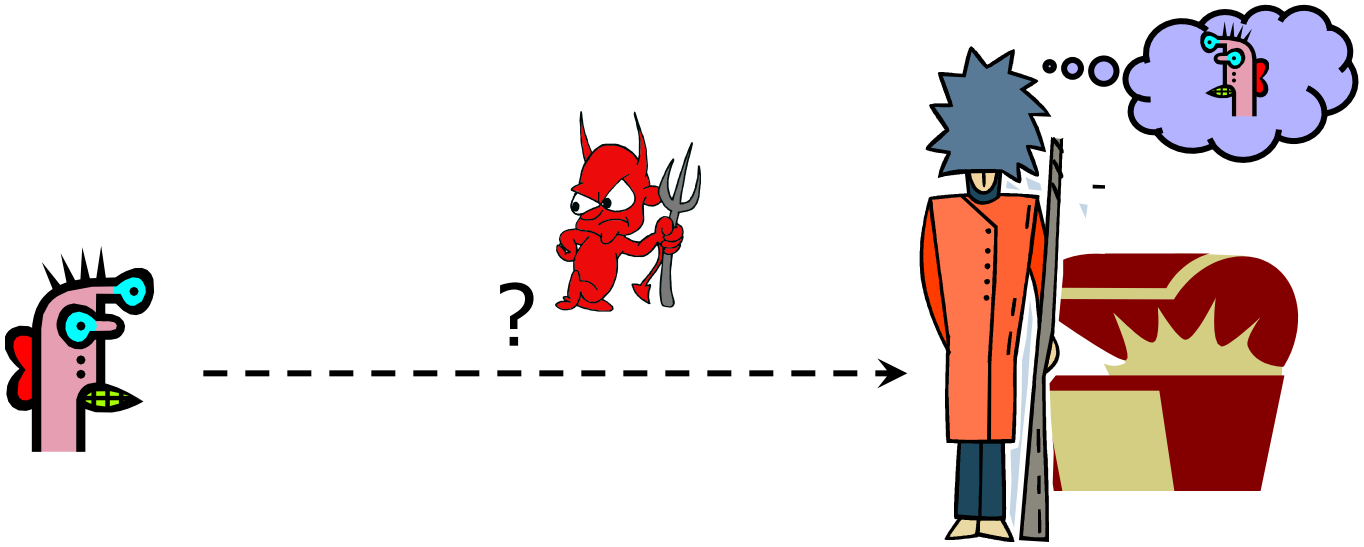
Shrirang (Shri) Mare
shri@cs.washington.edu

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

Outline

- Authentication
- Different ways to authenticate
- Passwords
- Biometrics

Basic Problem



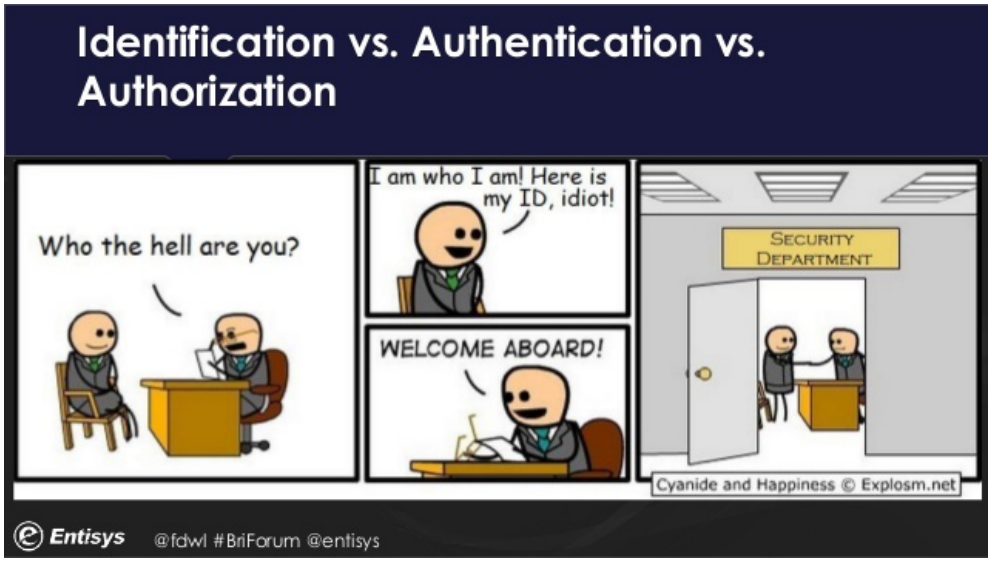
How do you prove to someone that you are who you claim to be?

Any system with access control must solve this problem.

Related terms

- Identification
- Authentication
- Authorization

Q: Can you authenticate someone without identification?



Many Ways to Prove Who You Are

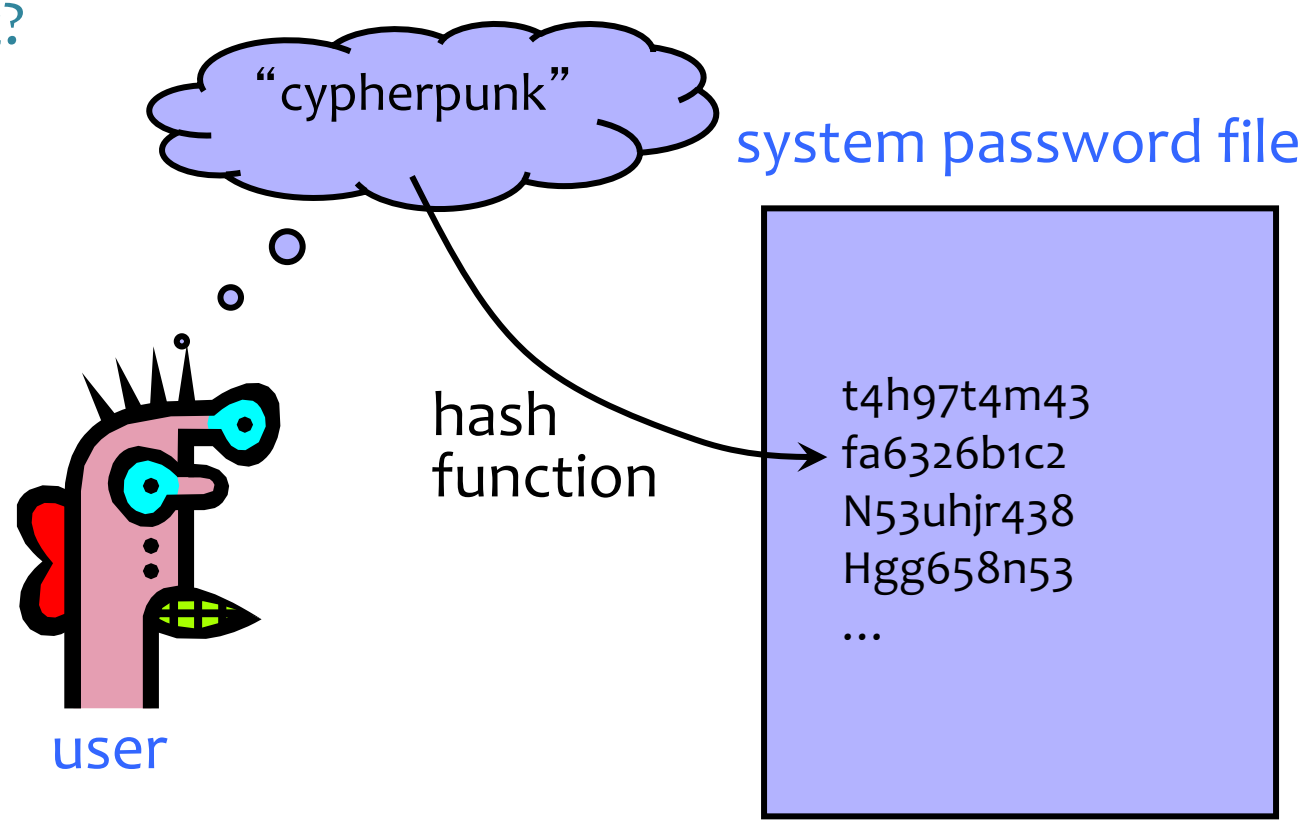
- Three main factors:
  1. What you know
     - Passwords
     - Answers to questions that only you know
  2. What you are
     - Biometrics
  3. What you have
     - Secure tokens, mobile devices
- Other factors:
  - Where you are
    - IP address, geolocation
  - Somebody you know
    - Leveraging your social network

Passwords and Computer Security

- In 2012, 76% of network intrusions exploited weak or stolen credentials (username/password)
  - Source: Verizon Data Breach Investigations Report
- First step after any successful intrusion: install sniffer or keylogger to steal more passwords
- Second step: run cracking tools on password files
  - Cracking needed because modern systems usually do not store passwords in the clear (how are they stored?)
- In Mitnick's "Art of Intrusion" 8 out of 9 exploits involve password stealing and/or cracking

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
  - "Slow" to compute

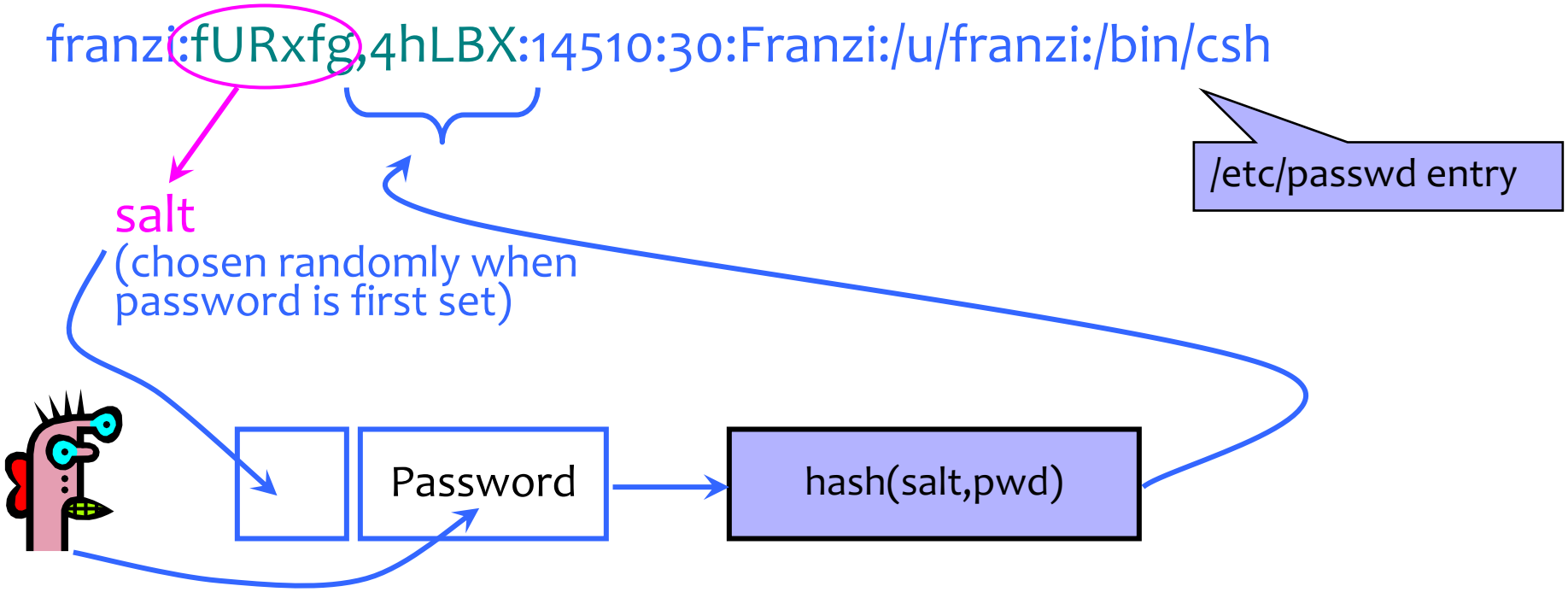
UNIX Password System

- 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 ($\sim 2^{52}$)
  - Humans like to use dictionary words, human and pet names ≈ 1 million common passwords

Dictionary Attack

- Dictionary attack is possible because many passwords come from a small dictionary
  - Attacker can pre-compute H(word) for every word in the dictionary – this only needs to be done once!
    - This is an offline attack
    - Once password file is obtained, cracking is instantaneous
  - Sophisticated password guessing tools are available
    - Take into account freq. of letters, password patterns, etc.
- In UNIX, /etc/passwd is world-readable
  - Contains user IDs and group IDs which are used by many system programs

Salt



- Users with the same password have different entries in the password file
- Offline dictionary attack becomes much harder

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)

Shadow Password

Hashed password is no longer stored in a world-readable file

Hashed passwords are stored in /etc/shadow file which is only readable by system administrator (root)

Other Password Security Risks

- Keystroke loggers
  - Hardware
  - Software (spyware)
- Shoulder surfing
- Same password at multiple sites
- Broken implementations
  - TENEX timing attack

Other Password Security Risks

- Social engineering

Other Issues

- Usability
  - Hard-to-remember passwords?
  - Carry a physical object all the time?
- Denial of service
  - Stolen wallet
  - Attacker tries to authenticate as you, account locked after three failures
  - "Suspicious" credit card usage

Default Passwords

- Pennsylvania ice cream shop phone scam
  - Voicemail PIN defaults to last 4 digits of phone number; criminals change message to "I accept collect call", make $8600 on a 35-hour call to Saudi Arabia
- Examples from Mitnick's "Art of Intrusion"
  - U.S. District Courthouse server: "public" / "public"
  - NY Times employee database: pwd = last 4 SSN digits
  - "Dixie ban"": break into router (pwd="administrator"), then into IBM AS/400 server (pwd="administrator"), install keylogger to snarf other passwords
    - "99% of people there used 'password123' as their password"

Weak Passwords

- RockYou hack

  - "Social gaming" company
  - Database with 32 million user passwords from partner social networks
  - Passwords stored in the clear
  - December 2009: entire database hacked using an SQL injection attack and posted on the Internet

Weak Passwords

- RockYou hack

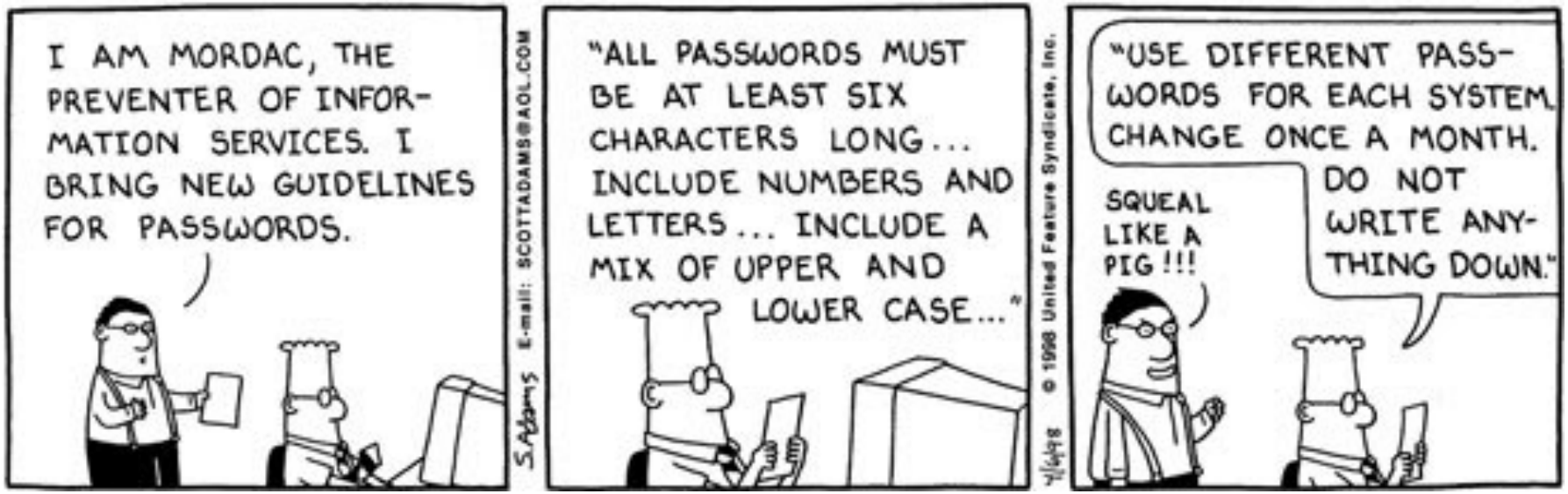
rockyou™

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Password Usability



[Inglesant and Sasse, "The True Cost of Unusable Password Policies"]

Password Policies

- Overly restrictive password policies…
  - 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords…
- … result in frustrated users and less security
  - Burdens of devising, learning, forgetting passwords
  - Users construct passwords insecurely, write them down
    - Can't use their favorite password construction techniques (small changes to old passwords, etc.)
    - "An item on my desk, then add a number to it"
  - Heavy password re-use across systems

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

Recovering Passwords

Palin E-Mail Hacker Says It Was Easy

By Kim Zetter ✉ September 18, 2008 | 10:05 am | Categories: Elections, Hacks and Cracks

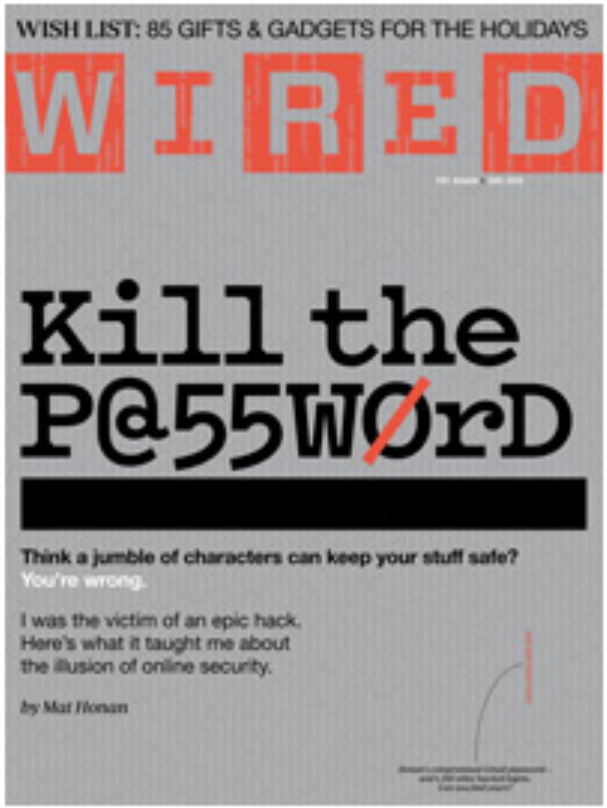
A p
obt
priv
sup
rev
too
Re

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)



"This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all. They really just wanted my Twitter handle: @mat."

"Mugged in London" Scam

James Fallows in Nov 11 issue of The Atlantic:

From: Deb Fallows <debfallows@gmail.com>

Date: Wed, Apr 13, 2011 at 8:45 AM

Subject: Problem

To:

now this might come as a suprise to you,but I made a quick trip to Madrid in Spain and was mugged.My bag,valuables,credit cards and passport all gone.The embassy has cooperated by issuing a temporary passport.I need funds to settle outstanding hotel bills,ticket and other expenses.

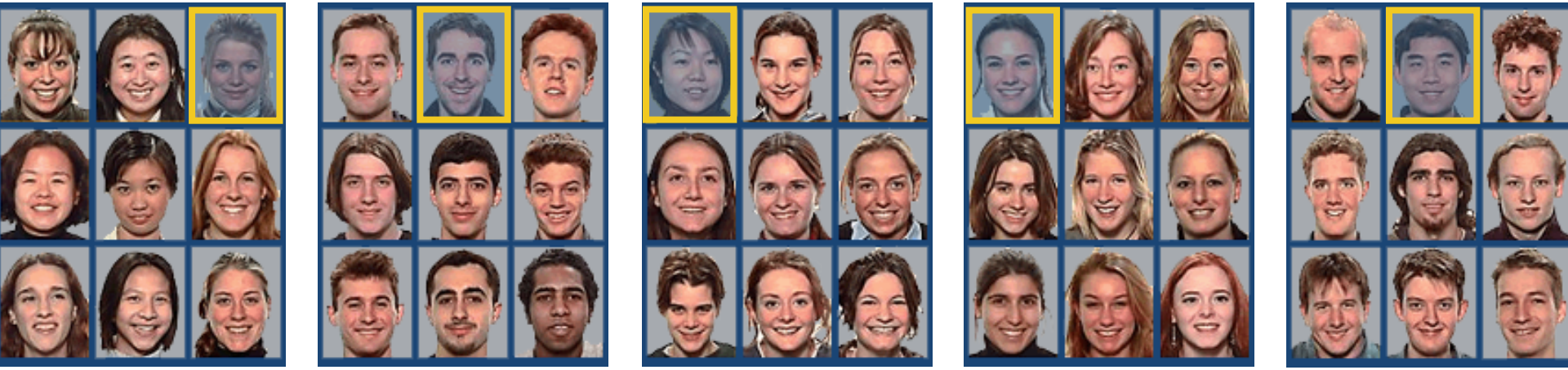
"When she looked at her Inbox, and her Archives, and even the Trash and Spam folders in her account, she found—absolutely nothing."

Improving(?) Passwords

- Graphical passwords
  - Goal: easier to remember? no need to write down?
- Password managers
  - Examples: LastPass, KeePass, built into browsers
  - Can have security vulnerabilities…
- Two-factor authentication
  - Leverage phone (or other device) for authentication
- Add biometrics
  - For example, keystroke dynamics or voiceprint

Graphical Passwords

- Many variants… one example: Passfaces
  - Assumption: easy to recall faces



  - Problem: to make passwords easy to remember, users choose predictable faces

Graphical Passwords

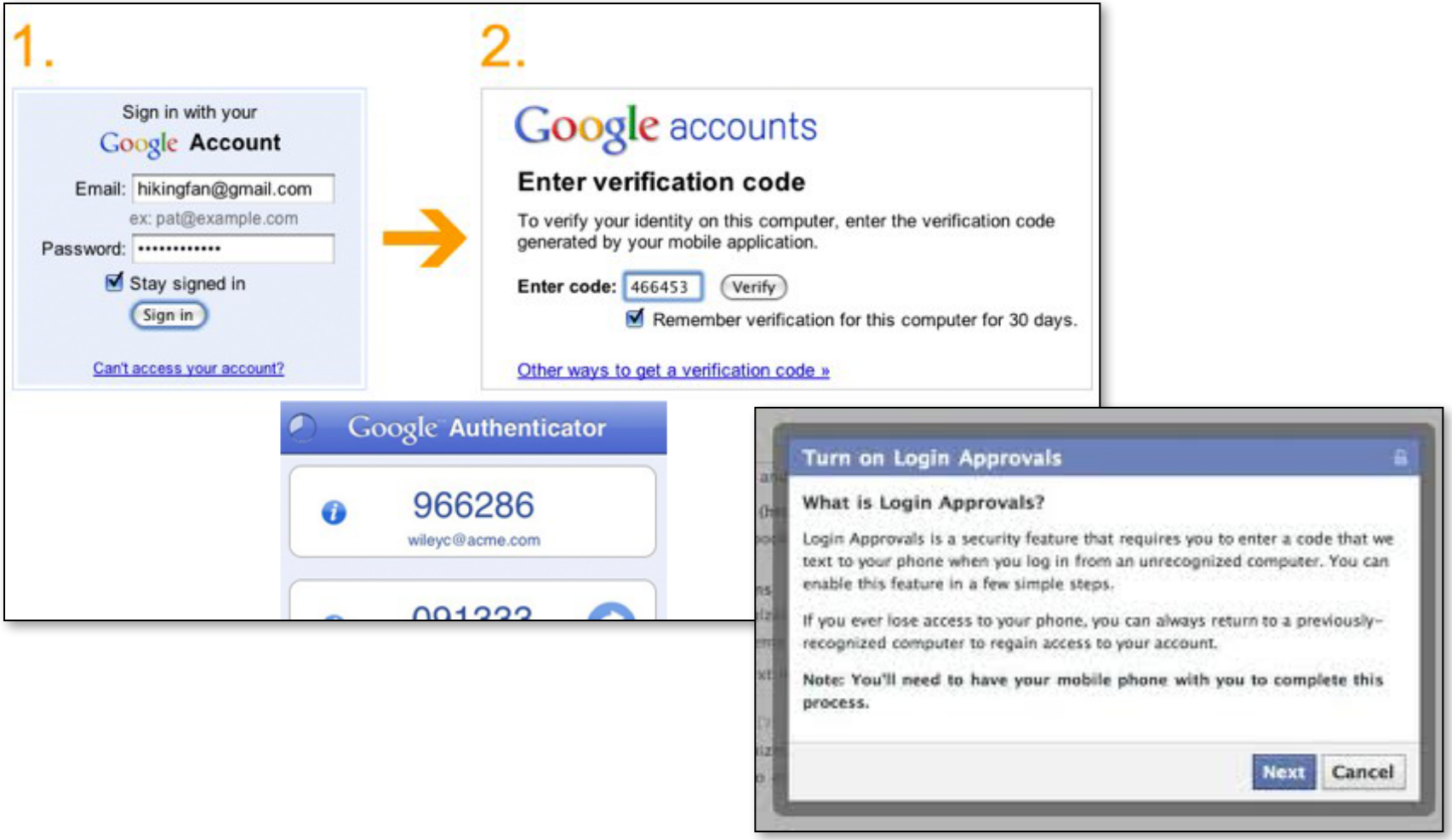
- Another variant: draw on the image (Windows 8)

- Problem: users choose predictable points/lines

Unlock Patterns

- Problems:
  - Predictable patterns (sound familiar by now??)
  - Smear patterns
  - Side channels: apps can use accelerometer and gyroscope to extract pattern!

Multi-Factor Authentication



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

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

Risks with 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.

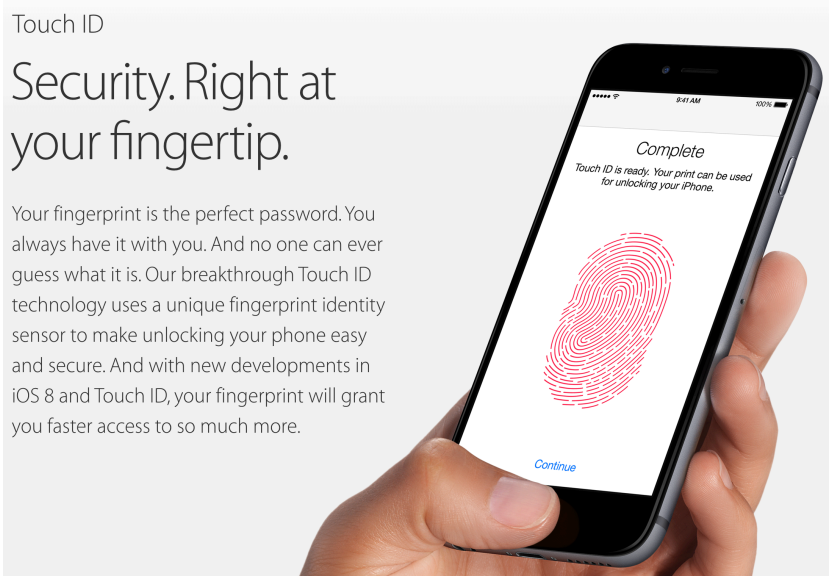
SEE ALSO:
Malaysia to act
pirates
16 Mar 05 | As

RELATED INTER
Malaysian police
The BBC is not r
for the content o
internet sites

TOP ASIA-PACIF
STORIES
Australians warn
cuts
Taiwan campus

Attacking Biometrics

- An adversary might try to steal biometric info
  - Malicious fingerprint reader
    - Consider when biometric is used to derive a cryptographic key
  - Residual fingerprint on a glass
- Ex: Apple's TouchID

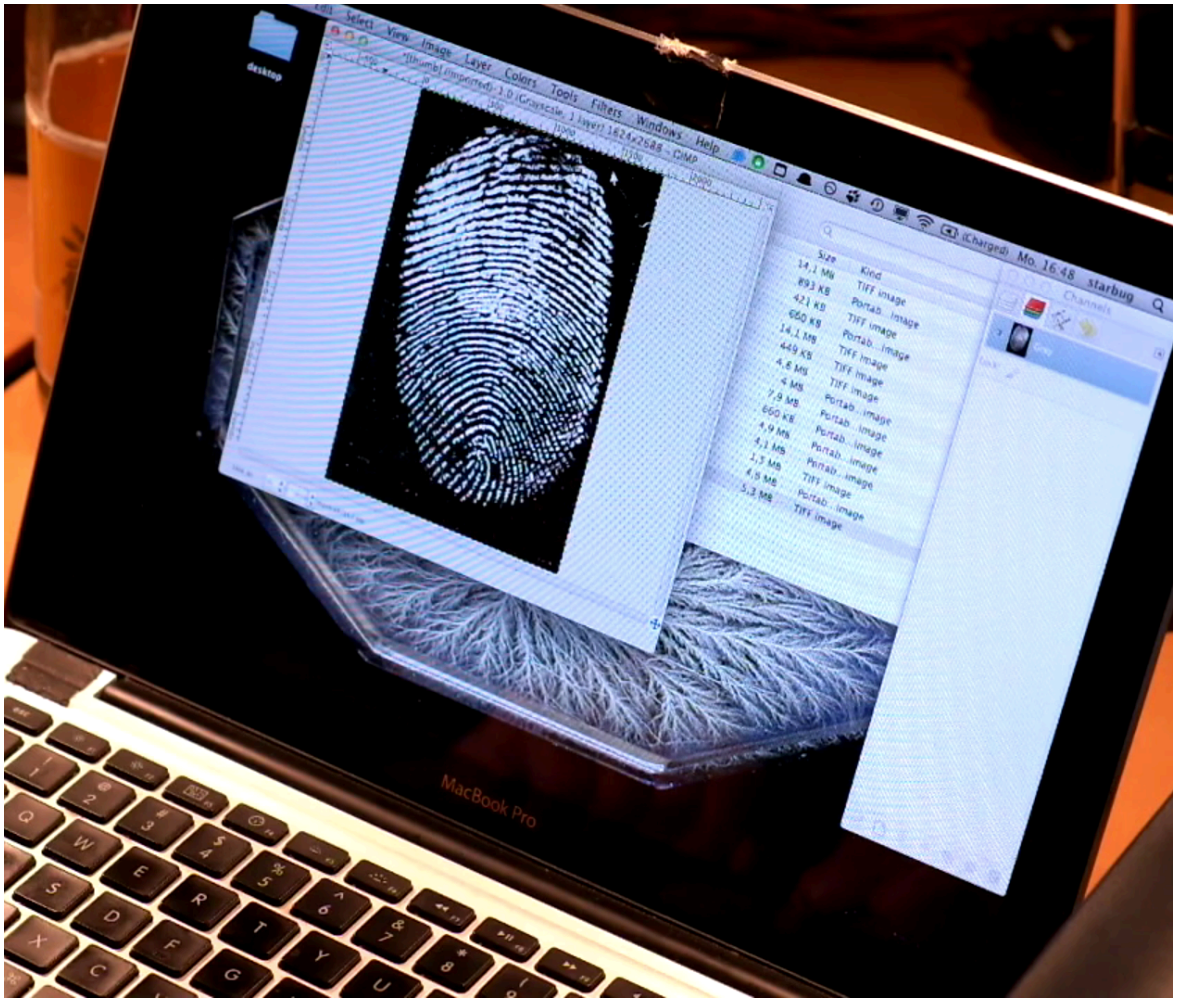


[Starbug -- http://istouchidhackedyet.com/]

Attacking Biometrics

[Starbug -- http://istouchidhackedyet.com/]

Attacking Biometrics



[Starbug -- http://istouchidhackedyet.com/]

Attacking Biometrics

[Starbug -- http://istouchidhackedyet.com/]

Attacking Biometrics