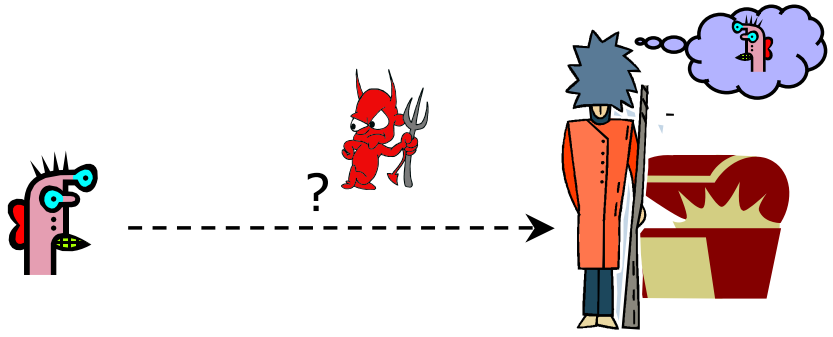
usfCS
UNIVERSITY of SAN FRANCISCO
department of computer science

Passwords

Vitaly Shmatikov
modified by EJ Jung

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

Many Ways to Prove Who You Are

- What you know
  - Passwords
  - Secret key
- Where you are
  - IP address
- What you are
  - Biometrics
- What you have
  - Secure tokens

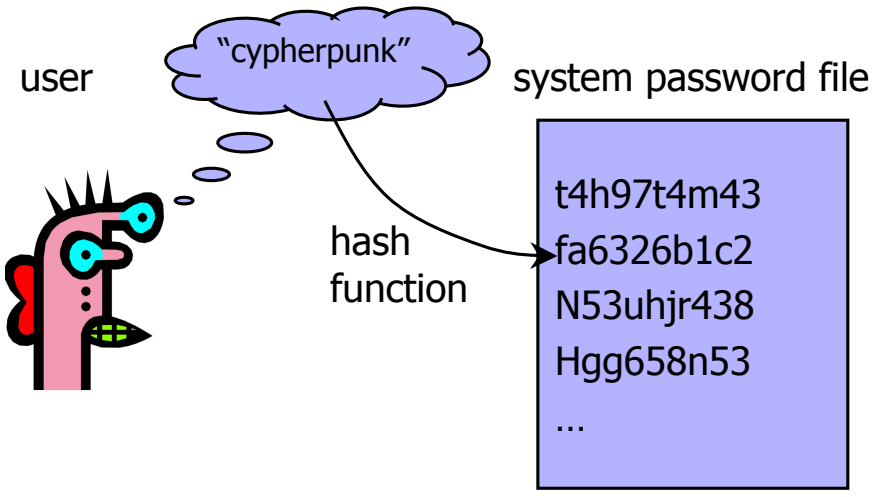
Other Aspects

- 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
- Social engineering

Password-Based Authentication

- User has a secret password.
  System checks it to authenticate the user.
- How is the password communicated?
  - Eavesdropping risk
- How is the password stored?
  - In the clear? Encrypted? Hashed?
- How does the system check the password?
- How easy is it to guess the password?
  - Easy-to-remember passwords tend to be easy to guess
  - Password file is difficult to keep secret

UNIX-Style Passwords



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!
- Hash function H must have some properties
  - One-way: given H(password), hard to find password
    - No known algorithm better than trial and error
  - Collision-resistant: given H(password1), hard to find password2 such that H(password1)=H(password2)
    - It should even be hard to find any pair p1,p2 s.t. H(p1)=H(p2)

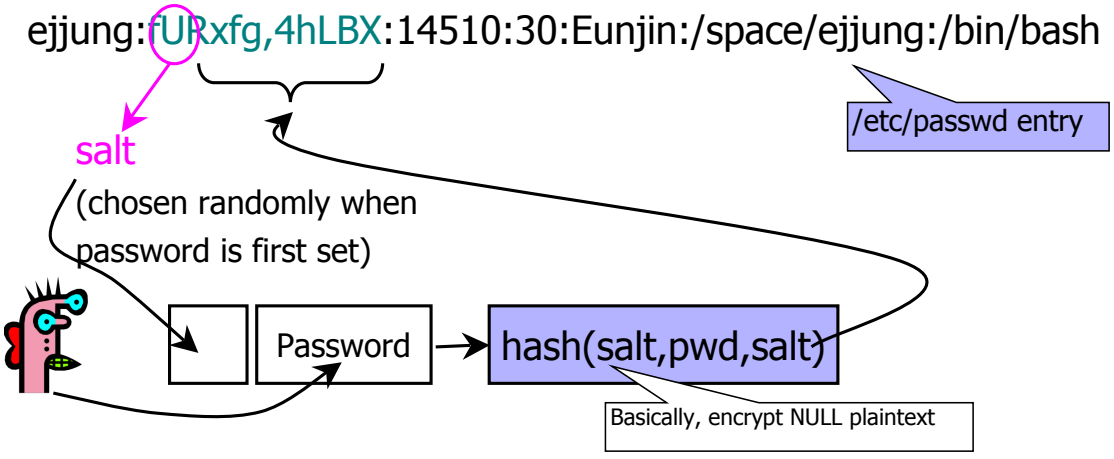
UNIX Password System

- 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
  - Can instruct modern UNIXes to use MD5 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
  - Humans like to use dictionary words, human and pet names ≈ 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!

Salt



- Users with the same password have different entries in the password file
- Dictionary attack is still possible!

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

Shadow Passwords

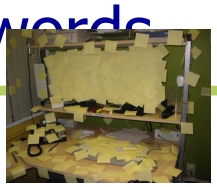
ejjung:x:14510:30:Eunjin:/space/ejjung:/bin/bashsh

Hashed password is not stored in a world-readable file

/etc/passwd entry

- Store hashed passwords in /etc/shadow file which is only readable by system administrator (root)
- Add expiration dates for passwords
- Early Shadow implementations on Linux called the login program which had a buffer overflow!

How People Use Passwords



- Write them down
- Use a single password at multiple sites
  - Do you use the same password for Amazon and your bank account? UT Direct? Do you remember them all?
- Make passwords easy to remember
  - "password", "Longhorns", "Kevin123"
- Some services use "secret questions" to reset passwords
  - "What is your favorite pet's name?"
  - Paris Hilton's T-Mobile cellphone hack

Memorability vs. Security

[Ross Anderson]

- One bank's idea for making PINs "memorable"
  - If PIN is 2256, write your favorite word in the grid

1	2	3	4	5	6	7	8	9	0
	b								
	l								
				u					
					e				

Do you see a problem?

  - Fill the rest with random letters
- Now, instead of 9999 possibilities for PIN, attacker just has to guess a short English word

Social Engineering

- Univ. of Sydney study (1996)
  - 336 CS students emailed asking for their passwords
    - Pretext: "validate" password database after suspected break-in
  - 138 returned their passwords; 30 returned invalid passwords; 200 reset passwords (not disjoint)
- Treasury Dept. report (2005)
  - Auditors pose as IT personnel attempting to correct a "network problem"
  - 35 (of 100) IRS managers and employees provide their usernames and change passwords to a known value
- Other examples: Mitnick's "Art of Deception"

Strengthening 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
- Rely on the difficulty of computer vision
  - Face recognition is easy for humans, hard for machines
  - Present user with a sequence of faces, he must pick the right face several times in a row to log in

Graphical Passwords

- Images are easy for humans to remember
  - Especially if you invent a memorable story to go along with the images
- Dictionary attacks on graphical passwords are believed to be difficult
  - Images are very "random" (is this true?)
- Still not a perfect solution
  - Need infrastructure for displaying and storing images
  - Shoulder surfing

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"*

What About Other Images?

Invent a story for an image or a sequence of images

"We went for a walk in the park yesterday"

Fish-woman-girl-corn

Need to remember the order!

User Experiences

- 50% unable to invent a story, so try to pick four pleasing pictures and memorize their order
  - "I had no problem remembering the four pictures, but I could not remember the original order"
  - "… but the third try I found a sequence that I could remember. fish-woman-girl-corn, I would screw up the fish and corn order 50% of the time, but I knew they were the pictures"
- Picture selection biases
  - Males select nature and sports more than females
  - Females select food images more often

Shoulder Surfing

- Graphical password schemes are perceived to be more vulnerable to "shoulder surfing"
- Experimental study with graduate students at the University of Maryland Baltimore County
  - 4 types of passwords: Passfaces with mouse, Passfaces with keyboard, dictionary text password, non-dictionary text password (random words and numbers)
- Result: non-dictionary text password most vulnerable to shoulder surfing
  - Why do you think this is the case?

Biometric Authentication

- Nothing to remember
- Passive
  - Nothing to type, no devices to carry around
- Can't share (usually)
- Can be fairly unique
  - … If measurements are sufficiently accurate

Problems with Biometrics

- Identification vs. authentication
  - Identification = associating an identity with an event or a piece of data
    - Example: fingerprint at a crime scene
  - Authentication = verifying a claimed identity
    - Example: fingerprint scanner to enter a building
- How hard are biometric readings to forge?
  - Difficulty of forgery is routinely overestimated
  - Analysis often doesn't take into account the possibility of computer-generated forgery
- Revocation is difficult or impossible

Biometric Error Rates (Benign)

- "Fraud rate" vs. "insult rate"
  - Fraud = system accepts a forgery (false accept)
  - Insult = system rejects valid user (false reject)
- Increasing acceptance threshold increases fraud rate, decreases insult rate
  - Pick a threshold so that fraud rate = insult rate
- For biometrics, U.K. banks set target fraud rate of 1%, insult rate of 0.01% [Ross Anderson]
  - Common signature recognition systems achieve equal error rates around 1% - not good enough!

Other Biometrics (1)

- 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 (2)

- 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)
- Voice, ear shape, vein pattern, face temperature

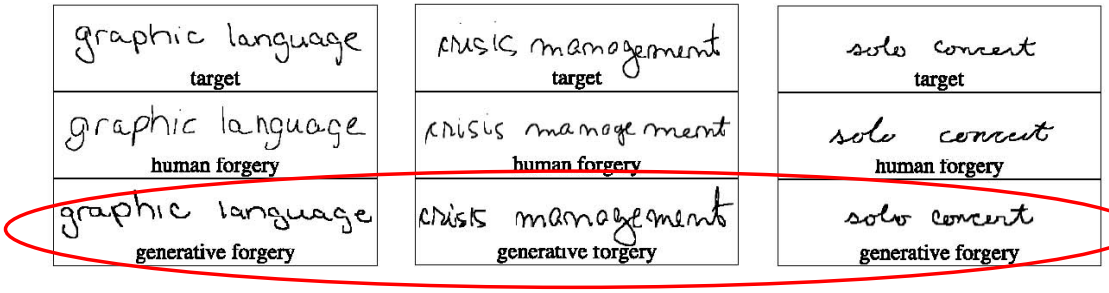
Risks of Biometrics

- 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

Bypassing Biometrics

Forging Handwriting

[Ballard, Monrose, Lopresti]



Generated by computer algorithm trained on handwriting samples

Cloning a Finger

[Matsumoto]

Making an Artificial Finger from a Residual Fingerprint

Materials

A photosensitive coated Printed Circuit Board (PCB)
"10K" by Sanhayato Co., Ltd .

320JPY/sheet

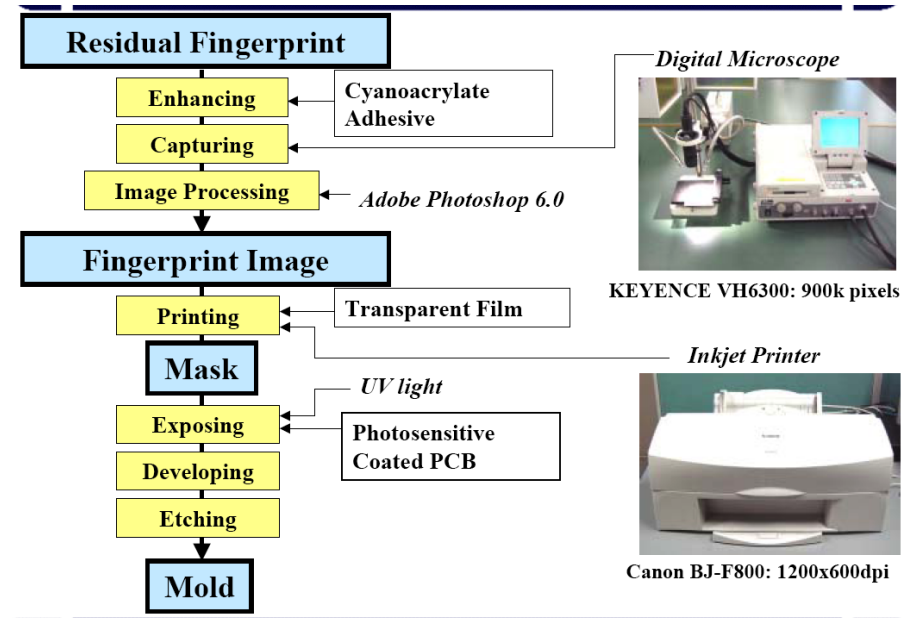
Solid gelatin sheet
"GELATINE LEAF "
by MARUHA CORP

200JPY/30grams

Yokohama Nat. Univ. Matsumoto Laboratory

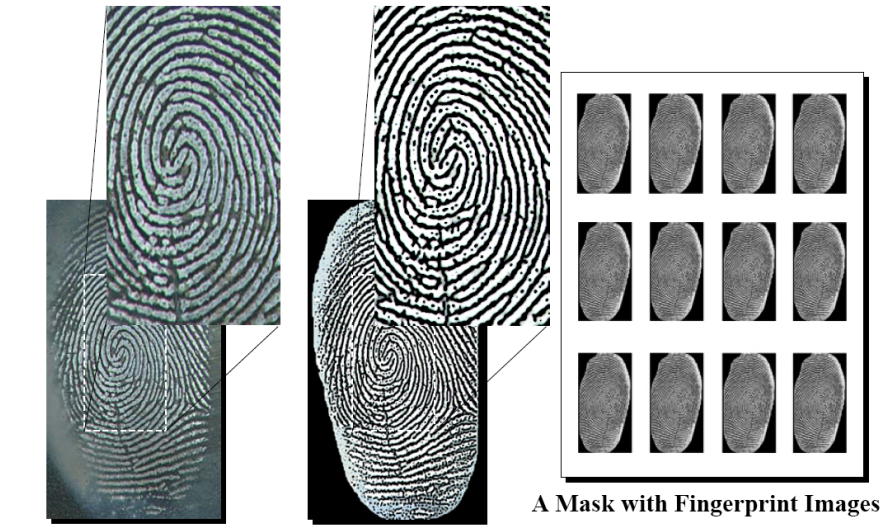
Cloning Process

[Matsumoto]



Fingerprint Image

[Matsumoto]

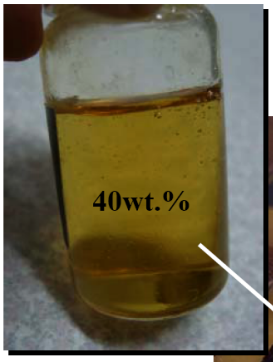


An Enhanced Fingerprint A Fingerprint Image A Mask with Fingerprint Images

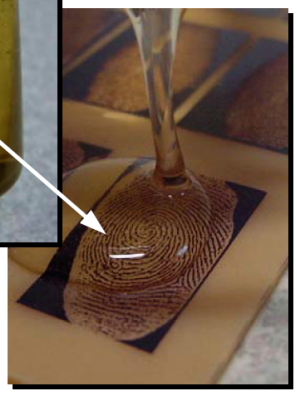
Molding

[Matsumoto]

Gelatin Liquid



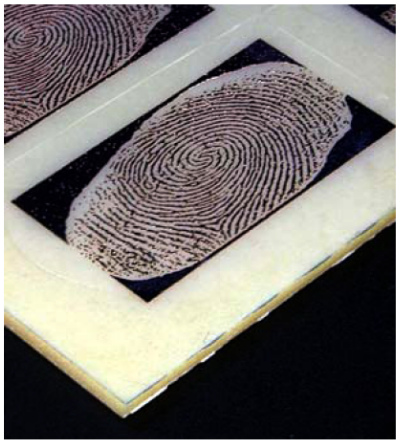
Drip the liquid onto the mold.



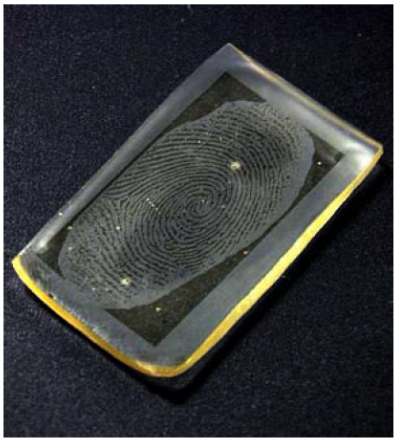
Put this mold into a refrigerator to cool, and then peel carefully.

The Mold and the Gummy Finger

[Matsumoto]



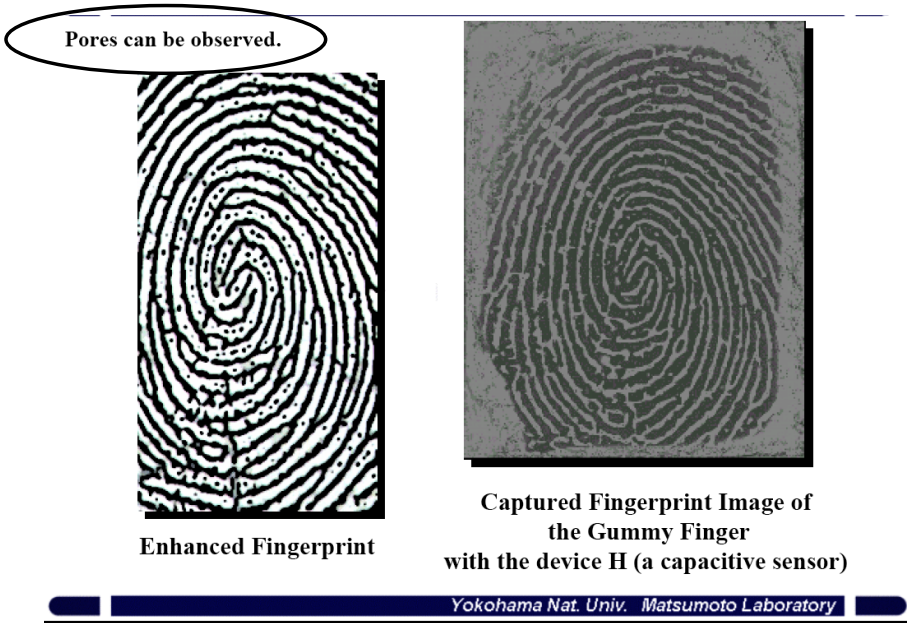
Mold: 70JPY/piece
(Ten molds can be obtained in the PCB.)



Gummy Finger: 50JPY/piece

Side By Side

[Matsumoto]



Play-Doh Fingers

[Schuckers]

- Alternative to gelatin
- Play-Doh fingers fool 90% of fingerprint scanners
  - Clarkson University study
  - See video online
    - Reference section on the course website
- Suggested perspiration measurement to test "liveness" of the finger

Passwords in the Real World

[PasswordResearch.com]

- From high school pranks…
  - Student in Tyler changes school attendance records
  - Students in California change grades
    - Different authentication for network login and grade system, but teachers were using the same password (very common)
- …to serious cash
  - English accountant uses co-workers' password to steal $17 million for gambling
- …to identity theft
  - Helpdesk employee uses passwords of a credit card database to sell credit reports to Nigerian scammers

Passwords and Computer Security

- First step after any successful intrusion: install sniffer or keylogger to steal more passwords
- Second step: run cracking tools on password files
  - Usually on other hijacked computers
- In Mitnick's "Art of Intrusion", 8 out of 9 exploits involve password stealing and/or cracking
  - Excite@Home: usernames and passwords stored in the clear in troubleshooting tickets
  - "Dixie bank" hack: use default router password to change firewall rules to enable incoming connections

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 bank": 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"

Single Sign-On

- Idea: authenticate once, use everywhere
- Examples:
  - Microsoft .NET passport
  - Kerberos
  - Liberty Alliance
- Related systems:
  - Google Checkout
  - Password managers