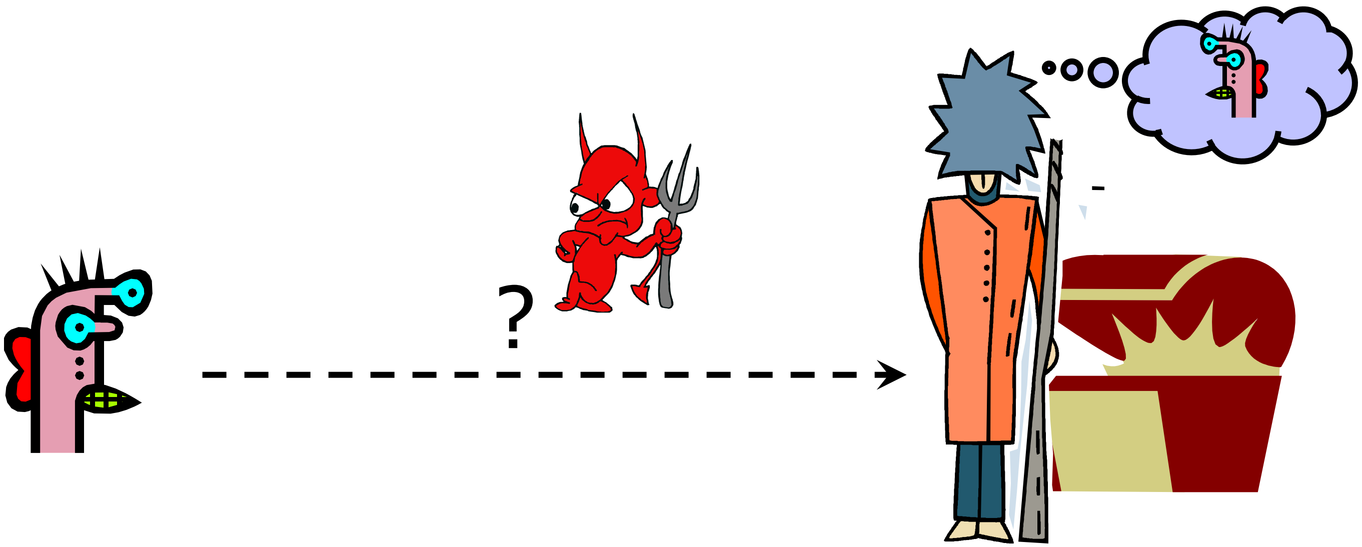
usfCS
UNIVERSITY of SAN FRANCISCO
department of computer science

Passwords

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

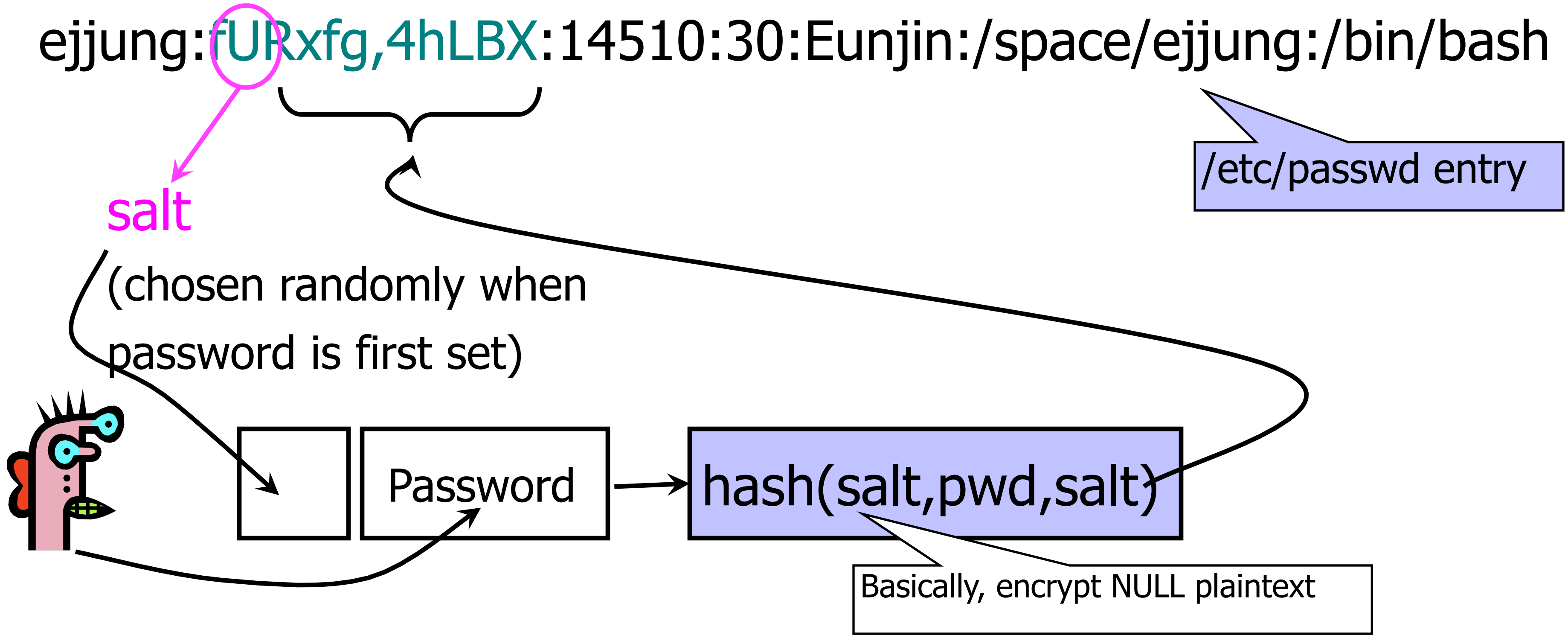
- User has a secret password.
  System checks it to authenticate the user.
- How is the password communicated?
  - Eavesdropping risk
- How is the password stored?
  - In the clear? Encrypted? Hashed?
- How does the system check the password?
- How easy is it to guess the password?
  - Easy-to-remember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

UNIVERSITY of SAN FRANCISCO
department of computer science

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



ejjung:fURxfg,4hLBX:14510:30:Eunjin:/space/ejjung:/bin/bash

/etc/passwd entry

salt

(chosen randomly when password is first set)

Basically, encrypt NULL plaintext

- Users with the same password have <u>different</u> 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

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

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