Announcements
- First assignment (article summary) length (300 words) - 10 points
  Interest - up to 10 points
  Grammar - 25 points
  Thesis - 25 points
  Facts to support your position, taken from article (30 points) - at least 4 facts
- Lab next week (Thursday in class)
Authentication (Access control)

4 Basic strategies

1) Something you know → passwords!
2) Something you possess
3) Something you are
4) Something you do

Which of these is the most common?
Passwords

Common Attacks:

- network sniffing
- brute force (dictionary attack)
- getting file w/ password
- physical access
- social engineering
Defenses against password attacks

- Up to 5 login attempts
- Automatic logout
- Password policies (user education)
- Reactive password checking (try to hack passwords)
- Separate passwords from user IDs
- Hashed passwords
- Salting the hash
- Resetting passwords
- Intentionally slow down authentication
Hashed Passwords

In general, only hashed versions of passwords are saved.

Why?

Password files were irresistible.

One extra layer of protection

In addition, there is generally a "random" piece of information. This is used in the hashing in addition to the password.

Why? Makes sure repeat passwords hash to different values.

Usually this creation time of account.

\[ h(\text{password} + \text{salt}) \]
Unix Implementation

- User password of 8 digits
  → 56-bit value
  ⇒ now much larger
- 12-bit salt value, usually based on account creation time

- Hash function (based on DES—more later)
  is run ~25 times.

- Resulting 64-bit value is converted to 14 character sequence

Sound impressive?
In 2003, a supercomputer managed over 50 million password guesses in 80 minutes.

(Back then, a regular machine could have done the same in about 1 month.)

(faster now)

Stronger variants essentially use stronger but slower hash algorithms.

(One even just runs a dummy for loop!)
Single Most Important Defense

user education

Choose Secure pass words!!

Use “random” phrases, or take first letter of each word.

Incorporate a letter @2 from website.
Password Checkers

Algorithms that allow or reject passwords based on how likely they are to be cracked.

1. Rule enforcement:

- check 6-8 letters or digits
- not your name, "password",
- or dictionary word
- at least 1 number...
Consider current letter, probability that next letter is any other letter.
Bloom filter
Token-Based Authentication
(something you possess)

- ATM cards
- key fobs with “random” generator
- RFID
- key card

- steal
- social engineering
- keeping card after leaving
- packet sniffing
- forge (cloning)
Biometric Authentication

Something you are or do

Hard to steal

Expensive

People change

Difficult to make effective

At heart these are algorithms possible to fool them.
A Note about Remote Authentication

Goal: Give eavesdroppers as little information as possible.

Sample (and simple) protocol:

1) User transmits identity

2) Host sends a nonce (random #), r, plus 2 functions h( ) + f( )

3) User sends: f(r, h(password))

Defends against: