# Dictionary Attack 2

- Suppose attacker has a dictionary containing *N common passwords, say,*

$$d_0, d_1, d_2, \ldots, d_{N-1}$$

- Then he/she could pre-compute the hash of each password in the dictionary,

$$y_0 = H(d_0), \; y_1 = H(d_1), \ldots, \; y_{N-1} = H(d_{N-1})$$

- Suppose Trudy gets access to password file containing hashed passwords
  1. She only needs to compare hashes to her pre-computed dictionary
  2. After one-time work of computing hashes in dictionary, actual attack is trivial
- Can we prevent this forward search attack? Or at least make it more difficult?

# Salt (1)

- We can prevent forward search attack by appending a non-secret random value, known as a **salt**, to each password before hashing.
- A password salt is analogous to the initialization vector, or IV, in, say, cipher block chaining (CBC) mode encryption. Whereas an IV is a non-secret value that causes identical plaintext blocks to encrypt to different ciphertext values, a salt is a non-secret value that causes identical password to hash to different values.
- Let $p$ be a newly entered password. We generate a random salt value $s$ and compute $y = H(p, s)$ and store the pair $(s, y)$ in the password file.
- Note that the salt $s$ is no more secret than the hash value.
- Now to verify an entered password $x$ , we retrieve $(s, y)$ from the password file, compute $H(x, s)$ , and compare this result with the stored value $y$ .

# Salt (2)

- Note that salted password verification is just as easy as it was in the unsalted case. But attacker's job has become much more difficult.
- Suppose Alice's password is hashed with salt value $s_a$ and Bob's password is hashed with salt value $s_b$.
- Then, to test Alice's password using her dictionary of common passwords, attacker must compute the hash of each word in his/her dictionary with salt value $s_a$,
- but to attack Bob's password, attacker must re-compute the hashes using salt value $s_b$.
- For a password file with $N$ users, attacker's work has just increased by a factor of $N$. Consequently, a pre-computed file of hashed passwords is no longer useful for attacker.

# Some Other Password Issues

- Today, most users need multiple passwords, but users can't (or won't) remember a large number of passwords. This results in a significant amount of password reuse, and any password is only as secure as the least secure place it's used.
- Social engineering is also a major concern with passwords. For example, if someone calls you, claiming to be a system administrator who needs your password to correct a problem with your account, would you give away your password?
- Keystroke logging software and similar Spyware are also serious threats to password-based security
- There are many available and popular password cracking tools. These tools come with preconfigured dictionaries, and it is easy to produce customized dictionaries

# Something You Are: Biometrics

- There are many different types of biometrics including:
  1. fingerprints,
  2. iris scan,
  3. hand geometry,
  4. biometrics based on speech recognition,
  5. gait (walking) recognition,
  6. and digital doggie (odor recognition).

# Why Biometrics?

- ✓ In the information security arena, biometrics are seen as a more secure alternative to passwords.
- ✓ For biometrics to be a practical replacement for passwords, cheap and reliable systems are needed.
- ✓ Today, usable biometric systems exist, including laptops using thumbprint authentication, palm print systems for secure entry into restricted facilities, the use of fingerprints to unlock car doors, and so on.
- ✓ But given the potential of biometrics and the well-known weaknesses of password-based authentication, biometrics are not really that popular yet

# Ideal Biometric Requirements

1. **Universal** — applies to (almost) everyone
   – In reality, no biometric applies to everyone
2. **Distinguishing** — distinguish with certainty
   – In reality, cannot hope for 100% certainty
3. **Permanent** — physical characteristic being measured never changes
   – In reality, OK if it to remains valid for long time
4. **Collectable** — easy to collect required data
   – Depends on whether subjects are cooperative
5. Also, safe, user-friendly, reliable, …

# Identification vs. Authentication

- Biometrics are also applied in various identification problems
- **Identification** — Who goes there?
  - Compare **one-to-many**
  - Example: Fingerprint database
- **Authentication** — Are you who you say you are?
  - Compare **one-to-one**
  - Example: Thumbprint mouse
- Identification problem is more difficult because more "random" matches since more comparisons
- We are (mostly) interested in authentication

# Two phases of biometric system

1. **Enrollment phase**; where subjects have their biometric information gathered and entered into a database:
   - Subject's biometric info put into database
   - Must carefully measure the required info
   - OK if slow and repeated measurement needed
   - Must be very precise
   - May be a weak point in real-world use
2. **Recognition phase**; this occurs when the biometric detection system is used in practice to determine whether to authenticate the user or not:
   - Biometric detection, when used in practice
   - Must be quick and simple
   - But must be reasonably accurate

# Two Types of Biometric Errors

- There are two types of errors that can occur in biometric recognition:

1. Suppose Bob poses as Alice and the system mistakenly authenticates Bob as Alice. The rate at which such misauthentication occurs is the **fraud rate**.
2. Now suppose that Alice tries to authenticate as herself, but the system fails to authenticate her. The rate at which this type of error occurs is the **insult rate**.

- For any biometric, we can decrease the fraud or insult rate at the expense of the other.
  - For example, if we require a 99% voiceprint match, then we can obtain a low fraud rate, but the insult rate will be high, since a speaker's voice will naturally change slightly from time to time.
  - On the other hand, if we set the threshold at a 30% voiceprint match, the fraud rate will likely be high, but the system will have a low insult rate.
- The **equal error rate** is the rate for which the fraud and insult rates are the same. This is a useful measure for comparing different biometric systems.

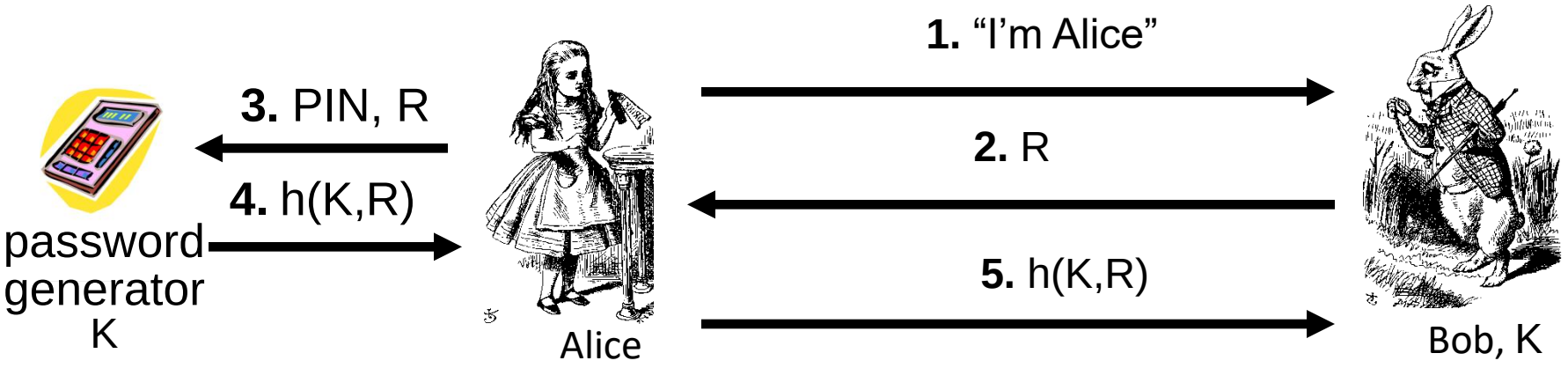
# Equal Error Rate Comparison

- Equal error rate (EER): fraud == insult rate
- **Fingerprint** biometrics used in practice have EER ranging from about $10^{-3}$ to as high as 5%
  - However, most fingerprint biometrics are relatively cheap devices that do not achieve anything near the theoretical potential for fingerprint matching
- **Hand geometry** has EER of about $10^{-3}$
- In theory, **iris scan** has EER of about $10^{-6}$ . But to achieve such spectacular results, the enrollment phase must be extremely accurate.
- Most biometrics much worse than fingerprint!
- Biometrics are useful for authentication, but for identification, are not so impressive today

# Something You Have

- Something in your possession
- Examples include following…
  1. Car key
  2. Laptop computer (or MAC address)
  3. Password generator (next)
  4. ATM card, smartcard, etc.

# Password Generator (1)




1. Alice receives random "challenge" R from Bob
2. Alice enters PIN and R in password generator
3. Password generator hashes symmetric key K with R
4. Alice sends "response" h(K,R) back to Bob
5. Bob verifies response

➢ *Note: Alice **has** password generator and **knows** PIN*

# Password Generator (2)

- For a challenge-response authentication scheme to work, Bob must be able to verify that Alice's response is correct. Thus, Bob and the password generator must both have access to the key *K, since the* password generator needs the key to compute the hash, and Bob needs the key to verify Alice's response.
- Alice accesses the key *K only indirectly—by* entering her PIN into the key generator.
- In fact, the password generator scheme above requires both "something you have" (the password generator) and "something you know" (the PIN).
- Any authentication method that requires two out of the three "somethings" is known as ***two-factor authentication.***

# Finally . . .

- *Acknowledgment*: These lecture notes are based on the textbook of Mark Stamp and ppt slides offered by him. My sincere thanks are devoted to him and to all other people who offered the material on the web.

- Students are advised to study and solve the problems and answer the questions in **Assignment-9**.