

# **Chapter 3**

## **User Authentication—Passwords, Biometrics and Alternatives**

### **Group C**

Purnima Miazy ID: 18701001

Jannatul Ferdous Talukdar ID: 18701004

Nabila Ayman ID: 18701017

Mosharat Jahan ID: 18701040

Ishra Naznin ID: 18701069

Afia Tasnim ID: 18701072

Nishat Sultana ID: 18701074

## 3.1 Password Authentication



- ▶ Storing hashes vs cleartext.
- ▶ Pre-computed dictionary attack.
- ▶ Targeted vs Trawling scope.
- ▶ Approaches to defeat password authentication
- ▶ Password composition policies and strength
- ▶ Pros and cons of passwords

## 3.2 Password-guessing strategies and defenses



- ▶ Password- guessing attacks fall into two categories
  1. Online Password- Guessing Attacks
  2. Offline Password- Guessing Attacks
- ▶ Online Password- Guessing Attacks
  1. Mounted against a publically reachable password-protected server.
- ▶ Offline Password- Guessing Attacks
  1. Involves recovering passwords from an already obtained password hashfile
  2. Can be slowed down using
    - ▶ ITERATED HASHING (PASSWORD STRETCHING)
    - ▶ PASSWORD SALTING
    - ▶ PEPPER (SECRET SALT)

## 3.2 Password-guessing strategies and defenses



- ▶ System-assigned passwords and brute-force guessing.
- ▶ Probability of guessing success:  $q = GT/R$
- ▶ Lower bound on length.  $n = \lg(R)/\lg(b)$  where  $R = GT/q$ .
- ▶ User passwords and skewed distributions.
- ▶ Password denylists and proactive password cracking.
- ▶ Login passwords vs. passkeys.

## 3.3 Account Recovery and Secret Questions



Some of the password reset methods are:

- ▶ **Recovery passwords and recovery links:** Using a recovery email address.
- ▶ **Loss of primary email password:** Pre-register to an independent device or channel, most commonly by a phone number.
- ▶ **Questions based recovery:** A method to address forgotten passwords is secret questions(challenge questions).

**Usability aspects:**Using questions to cue information from user's long-term memory.

**Security aspects:**Trying to salvage security by requiring answers to more questions reduces efficiency.

## 3.4 One-time password generators



A security issue with ordinary passwords is their static nature. If captured by a passive attacker, simple replay of the password defeats security. A possible solution is One Time Password(OTP) —passwords valid for one use only.

1. **OTP's received by mobile** - Mobile phones may be used as an independent channel for one-time codes via “text” or SMS (Short Message Service).
2. **Passcode generators** - The device holds a user-specific secret, and computes a passcode output with properties similar to OTPs, which is usable for a specific time. The OTP is typically used as a “second factor” alongside a static password.

## 3.4 One-time password generators



3. **Hardware tokens** - Passcode generators and mobile phones used for user authentication are instances of a class of method includes hardware tokens such as 'smart cards'.
4. User authentication categories -
  - ▶ **what you know** : PIN,password
  - ▶ **what you have** : Chip card
  - ▶ **what you are** : fingerprints
5. **Multiple factor** - More than one methods used in parallel both must succeed for user authentication.

## 3.5 Biometric authentication



### 1. Biometric authentication

- ▶ Security is generally less than expected.
- ▶ Physical biometrics->“what you are” category .
- ▶ Behavioral biometrics -> “what you do” category.
- ▶ Not secret

### 2. Failure to enroll/failure to capture

### 3. Disadvantages(Biometrics)

- ▶ Require custom client-side hardware
- ▶ Biometrics are non-secrets
- ▶ Security of biometrics is often over-stated

### 4. Biometric process:Enrollment and verification

### 5. False rejects, false accepts

### 6. False accept/reject rates



## 3.5 Biometric authentication



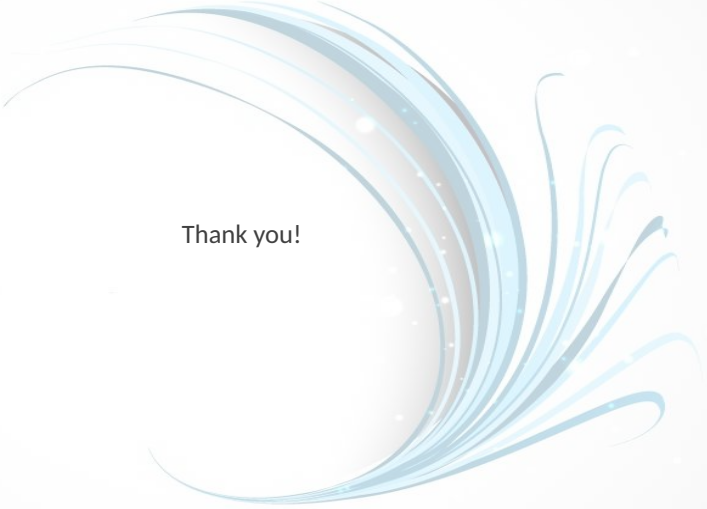
### EVALUATING BIOMETRICS USING STANDARD CRITERIA

- ▶ Universality
- ▶ Distinguishability
- ▶ Invariance: Stable over time??
- ▶ Ease-of-sampling: Sample obtained measured?
- ▶ Accuracy
- ▶ Cost: time (sampling; processing), storage, hardware/software costs
- ▶ User acceptance : Users willingly to use?

### Attacks on biometric authentication

#### Biometrics

Authentication(Sample matched against user template) VS. Identification (one-to-many test)( Against criminal database) (Match crowd faces).



Thank you!