STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

SSW 322: Software Engineering Design VI

User Authentication
2020 Spring

Prof. Lu Xiao
lxiao6@stevens.edu
Office Hour: Monday/Wednesday 2 to 4 pm
https://stevens.zoom.us/j/632866976
Software Engineering
School of Systems and Enterprises

Today's Topic – Security Overview

- User Authentication
  - Principles
  - Means of authentication
  - Security issues of authentication

- Computer Security---Principles and Practice 4th Edition, William Stallings and Lawire Brown, ISBN-10 1-292-22061-9

What is User Authentication?

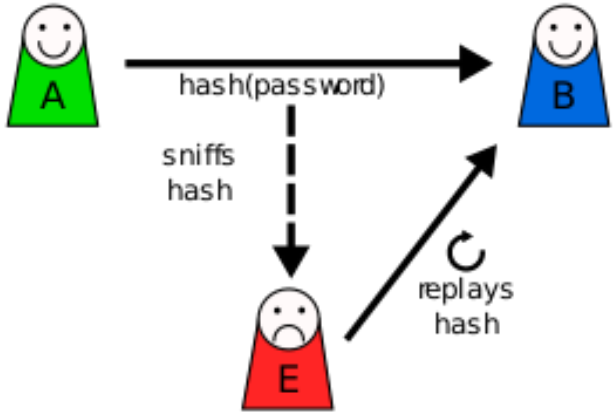
- User authentication is the fundamental building block and the primary line of defense.
  - Alice Toklas have her user identifier ABTOKLAS, stored on any server or computer system.
  - A typical authentication item associate with this ABTOKLAS is a password, which is kept as a secret (only Alice and the server knowns).
  - The combination of ABTOKLAS and the password enables Alice's access permissions and the system audit her activities.
  - ABTOKLAS is public, but password is a secret, thus no one can pretend to be Alice.

Digital User Authentication Principles

- NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, December 2016)
  1. Identify information system users, processes acting on behalf of users, or devices.
  2. Authenticate the identities of those users, processes, or devices, as prerequisite to allowing access to organizational information systems.
  3. Use multifactor authentication for local and network access to privileged accounts and for networks access to non-privileged accounts.

Digital User Authentication Principles

4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.



5. Prevent reuse of identifiers for a defined period.
6. Disable identifiers after a defined period of inactivity.
7. Enforce a minimum password complexity and change of characters when new passwords are created.

Digital User Authentication Principles

8. Prohibit password reuse for a specified number of generations.

9. Allow temporary password use for system logons with an immediate change to a permanent password.

10. Store and transmit only cryptographically-protected passwords.

11. Obscure feedback of authentication information.

e.g. Office 365 natively obscures password entry with asterisks or dots. This experience is the same across web applications and local applications installed on a device or machine.

Means of Authentication

- There are four general means of authentication
  1. Something the individual knows: e.g. password, pin, or answers to a set of pre-arranged questions
  2. Something the individual possesses: e.g. electronic keycards, and physical keys. This type of authentication is referred to as a *Token*.
  3. Something the individual is (static biometrics): e.g. fingerprint, retina, and face.
  4. Something the individual does (dynamic biometrics): e.g. voice pattern, handwriting, and typing rhythm.

Password-Based Authentication

- The system compares the password to a previously stored password for a user ID, maintained in **a system password file.**
- The password serves to authenticate the ID of the individual logging on to the system.
- The ID serves to:
  - Determine whether user is authorized
  - Determine the privileges of the user
  - Discretionary access control

The Vulnerability of Passwords

- Offline dictionary attacks
  - Determined hackers gain access to the system's password file. Attackers compare the password hashes against commonly used passwords. The attacker gain access by the ID/password combination when a match is found.
  - Countermeasures include:
    - Prevent unauthorized access to the system's password file
    - Intrusion detection to identify compromise
    - Rapid reissuance of passwords.

The Vulnerability of Passwords

- Specific account attack:
  - The attacker targets a specific account and submits password guesses until the correct password is discovered.
  - The standard countermeasure is an account lockout mechanism, which locks out access to the account after a number of failed login attempts.
- Popular password attack:
  - Use a popular password and try it against a wide range of user IDs. A user's tendency is to choose a password that is easily remembered.
  - Countermeasures includes policies to inhibit the selection of common passwords and scanning the IP addresses of authentication requests and client cookies.

The Vulnerability of Passwords

- Password guessing against single user:
  - The attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess password.
  - Countermeasures include training in and enforcement of password policies that make passwords difficult to guess. Such as secrecy, minimum length, character set, etc.
- Workstation hijacking:
  - The attacker waits until a logged-in workstation is unattended.
  - The standard countermeasure is automatically logging the workstation out after a period of inactivity. Or instruction detection schemes for detecting changes in user behavior.

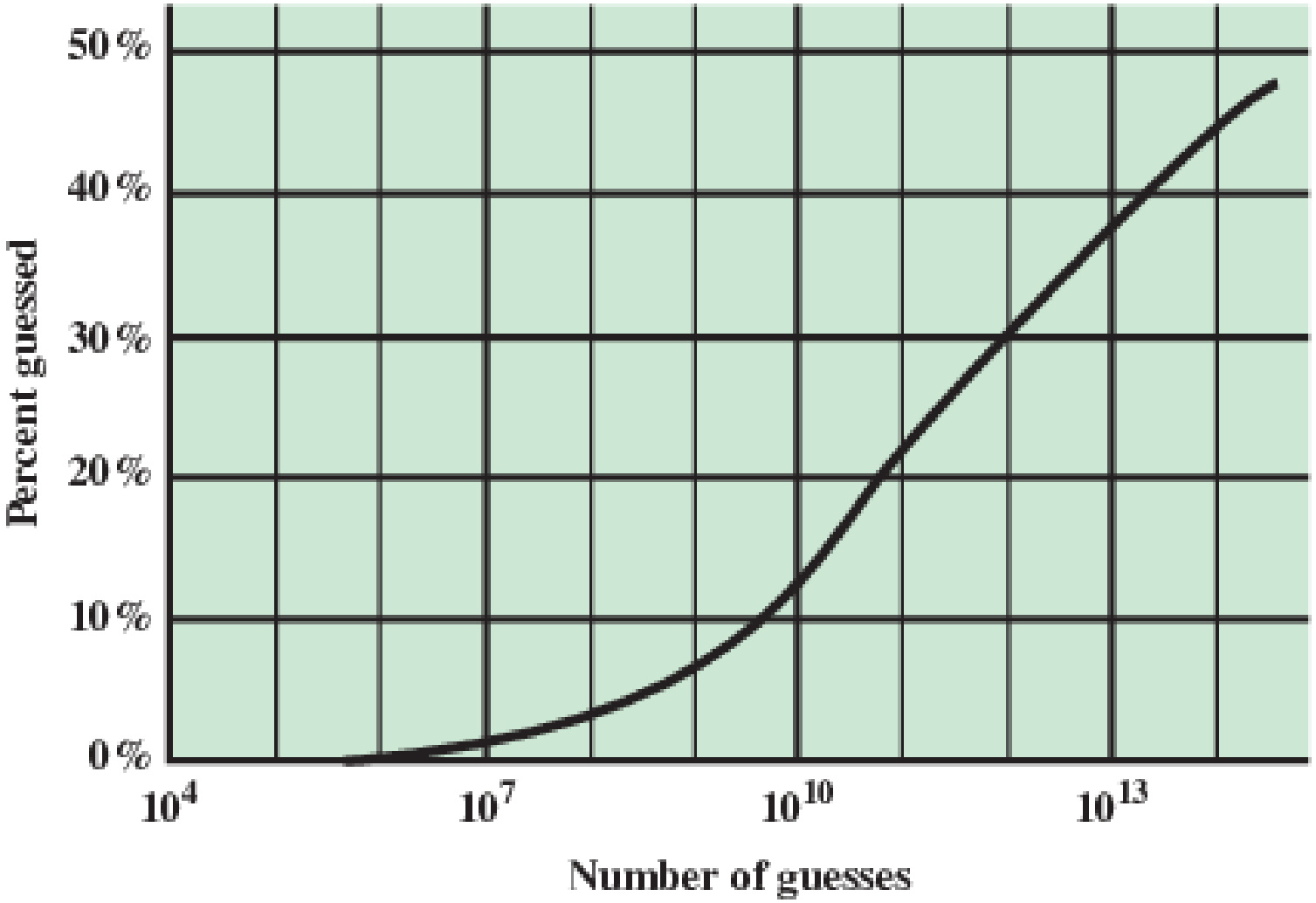
The Vulnerability of Passwords

- Exploiting user mistakes:
  - A user may unintentionally share a password by mistake. Attackers may gain access of password through social tactics.
  - Countermeasures include training, intrusion detection, and simpler passwords combined with another authentication mechanism.
- Exploiting multiple password use:
  - Different network devices share the same or a similar password for a given user.
  - Countermeasures include a policy that forbids the same or similar password on particular network devices.

The Vulnerability of Passwords

- Electronic monitoring
  - If a password is communicated across the network to log on to a system, it is vulnerable to eavesdropping. Simple encryption will not fix this problem.
  - Do not use public network to log onto critical information systems.

The Vulnerability of Passwords

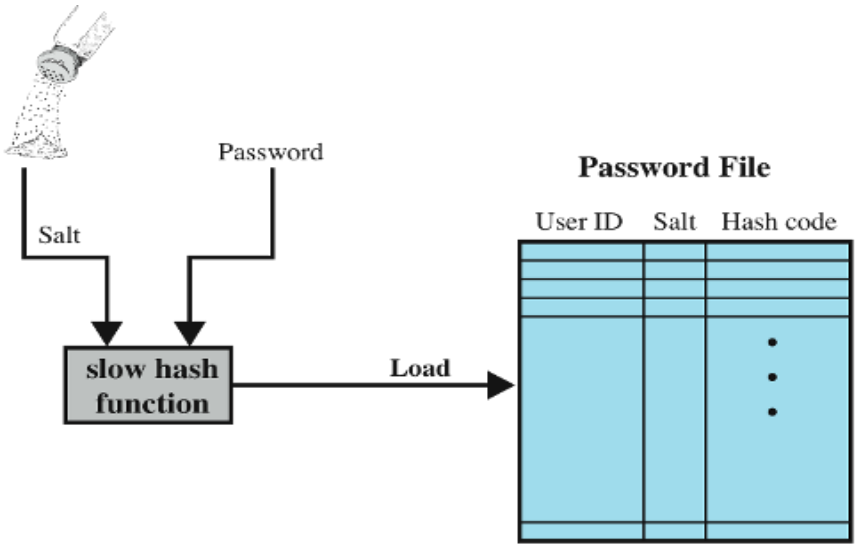


Why passwords remain popular?

- Techniques that utilize client-side hardware, such as fingerprint scanners and smart cards, require the implementation of the appropriate user authentication software to exploit this hardware on both the client and server end.
- Physical tokens, such as smart cards, are expensive and/or inconvenient to carry around.
- Automated password managers that relieve users of the burden of knowing and entering passwords have poor support for roaming and synchronizing across multiple client platforms.

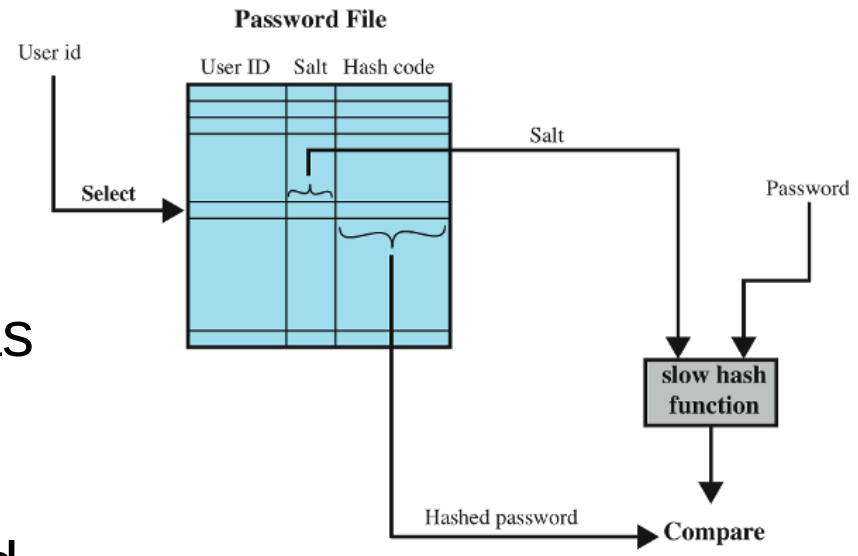
The Use of Hashed Passwords

- A widely used password security technique: hashed password + salt value.
- The password is combined with a fixed length salt value to serve as the input to a hashing algorithm to produce a fix length hash code.
- The salt value is:
  - Based on time
  - Random number
- The hash algorithm is designed to be slow in order to thwart attacks.



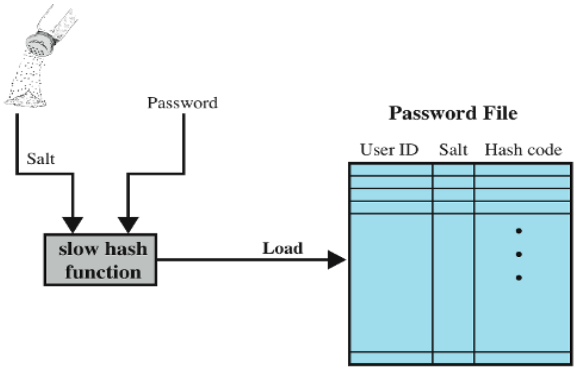
The Use of Hashed Passwords

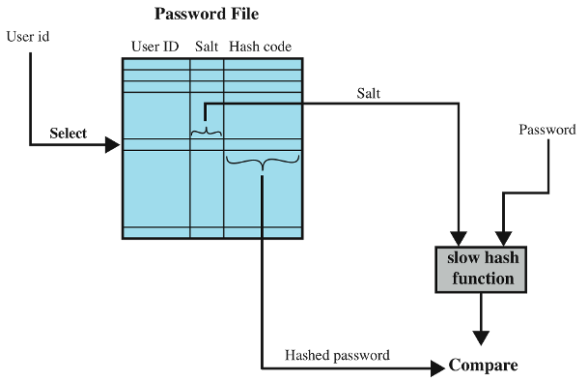
- When a user attempts to log on to a UNIX system, the user provides an ID and a password.
- The system uses the ID to obtain the salt value and the encrypted password.
- The salt value and user provided password are used as input to the encryption algorithm.
- If the value matches the stored value, the password is accepted.



The Use of Hashed Passwords

- The salt value has three purposes:
  1. Prevents duplicated passwords from being visible in the password file.
  2. Increases the difficulty of offline dictionary attacks. If a salt value is x bits, the number of possible passwords increase by a factor of 2^x.
  3. Impossible to find out whether a person has used the same passwords on different devices/systems.





Password Selection Strategies

- When not constrained, users tend to choose passwords that easy to remember, thus short or easy to guess.
  - Birthday, people's names, personal information, such as license or plate numbers.
- If users are assigned password of randomly generated 8 characters, password cracking is effectively impossible.
  - ia5pl/yCzxFh9ozB/iw0, x0PKPXVup96+M3hX/557, 5pBGtHfu43TXljrx3LhR, g1sJOj1Oo3bp3cyvLr63.
- Our goal is to eliminate guessable passwords while allowing users to select a password that is memorable. Four basic techniques are in use:
  - User education; Computer-generated passwords; Reactive password checking; Complex password policy

Password Selection Strategies

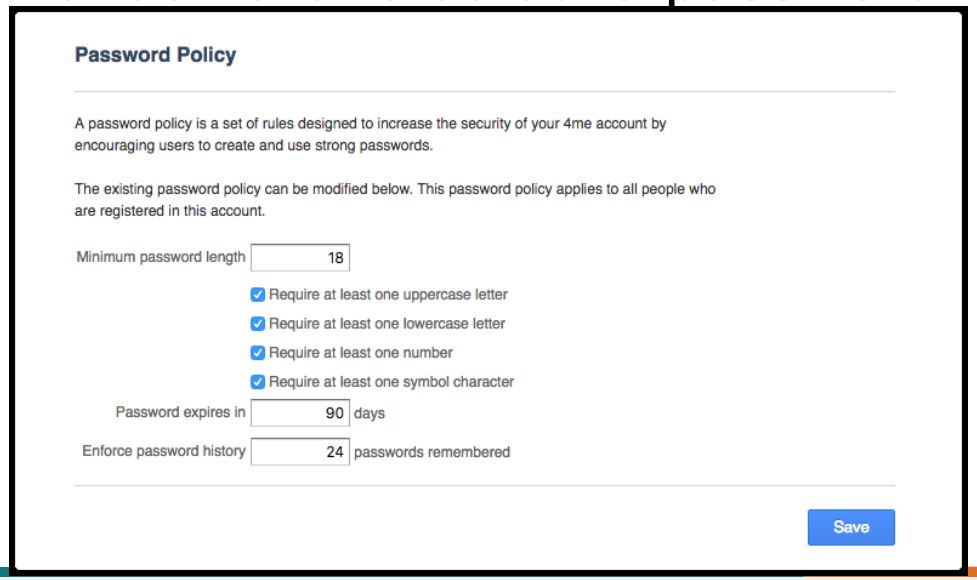
- User education:
  - Users can be told the importance of using hard-to-guess passwords
    - They may ignore the guidelines
    - They may not be a good judges of what is a strong password.
  - A good technique is to use the first letter of each word of a phrase:
    - “An apple a day keeps the doctor away”---Aaadktda
    - “My dog’s first name is Rex” ---MdfniR
    - “My sister Peg is 24 years old” --- MsPi24yo

Password Selection Strategies

- Computer-generated password
  - If the passwords are quite random, the user won't be able to remember them.
  - In general, computer-generated password schemes have a history of low acceptance.
- Reactive password checking
  - The system periodically runs its own password cracker to find guessable passwords.
  - The system cancels vulnerable passwords and notify the users.
  - However, this is resource intensive.

Password Selection Strategies

- Complex password policy:
  - A promising approach to improve password security
  - A user picks his/her own password. However, the system checks to see if the password is allowable end ,it not, rejects it.
  - If a system rejects too many passwords, users will complain its too hard to select a password.

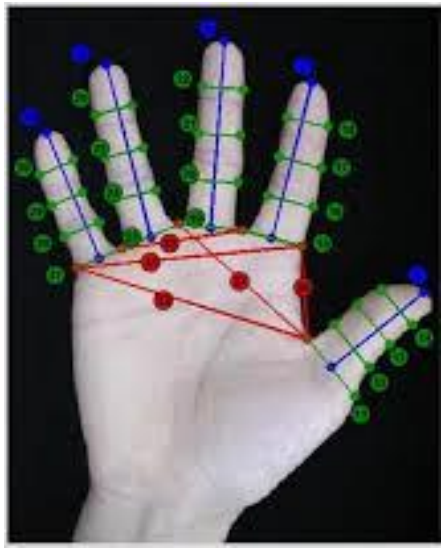


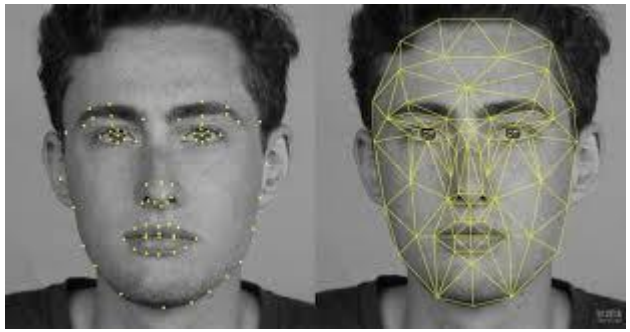
Token-based Authentication

- Objects that a user possesses for the purpose of user authentication
  - Memory cards: sore but not process data. Such as bank with magnetic strip on the back, hotel room card, etc.
  - Smart cards, such as embedded microprocessor
  - Electronic Identify Cards: the use of smart cards as a national identify card for citizens. E.g. the German eID card.

Biometric Authentication

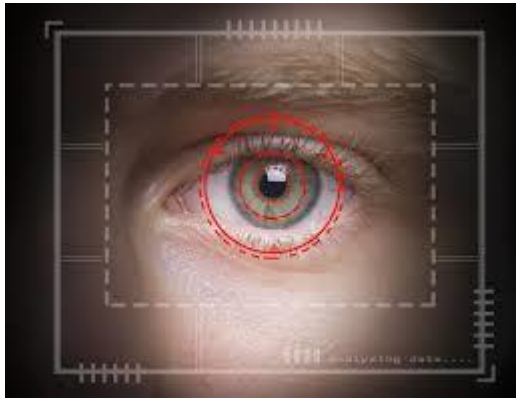
- Authentication is based on individual's physical characteristics.
- Static characteristics: fingerprints, hand geometry, facial characteristics, and retinal and iris patterns.
- Dynamic characteristics: voiceprint and signature,

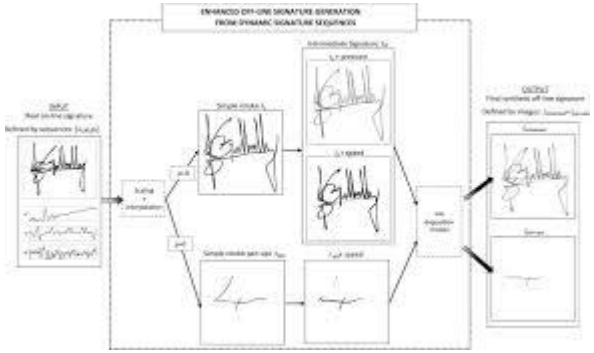




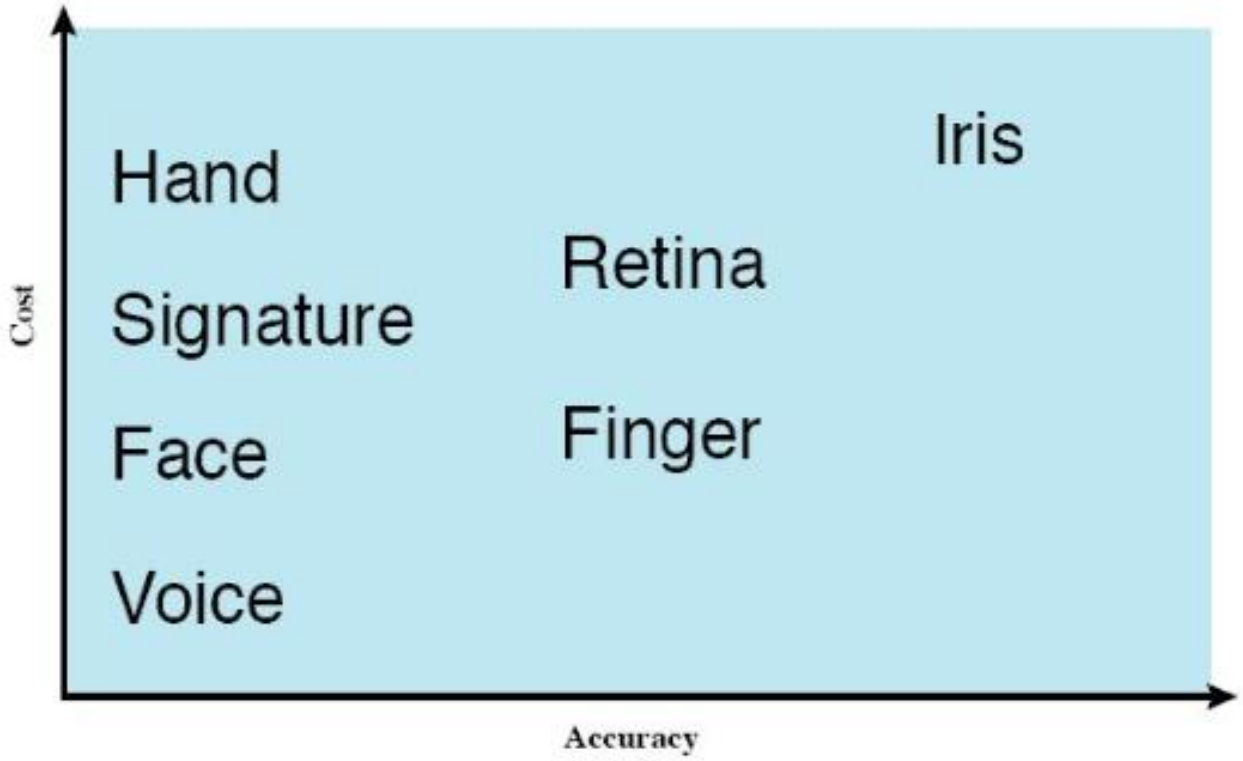
Biometric Authentication

- Authentication is based on individual's physical characteristics.
- Static characteristics: fingerprints, hand geometry, facial characteristics, and retinal and iris patterns.
- Dynamic characteristics: voiceprint and signature

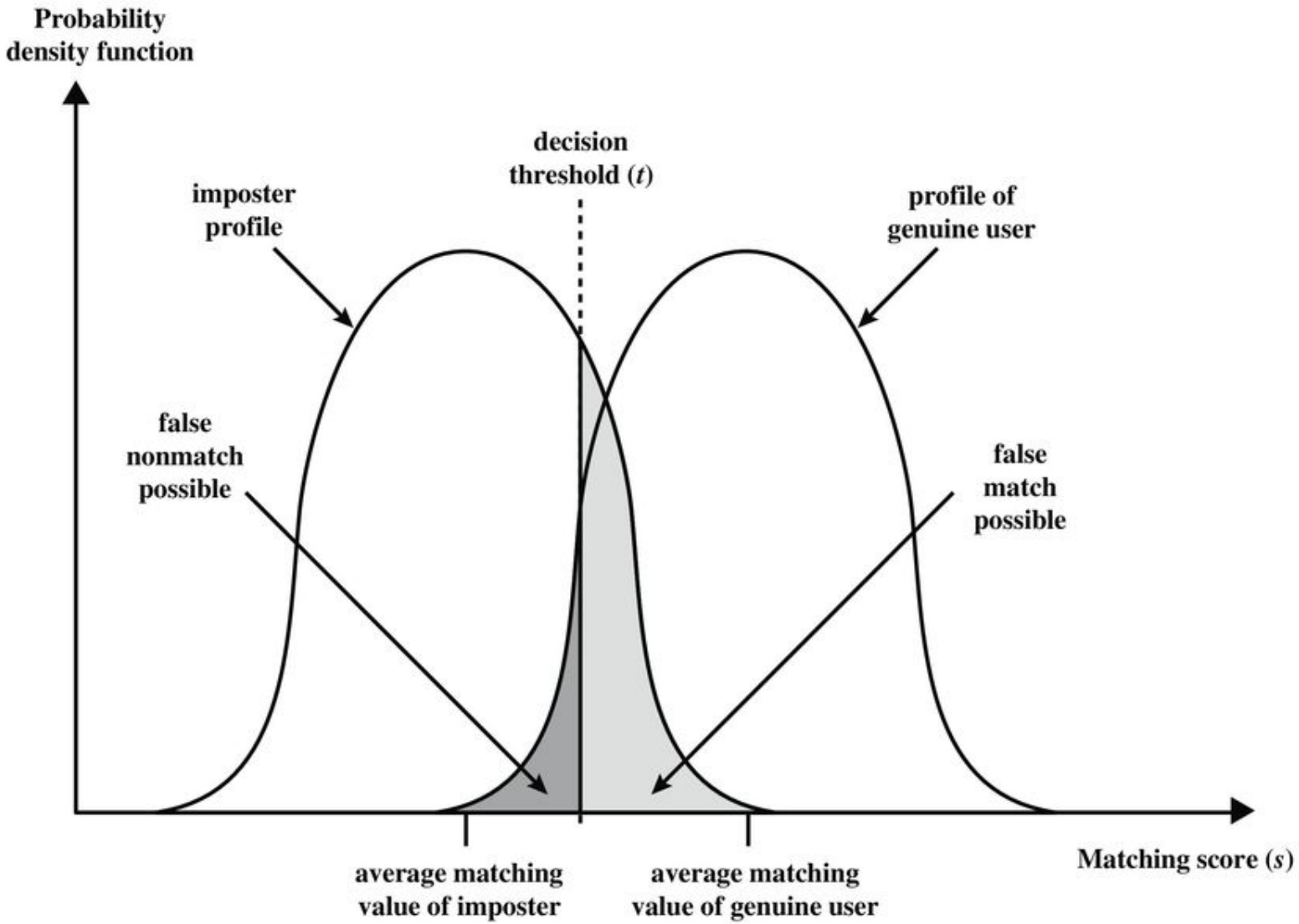




Cost Versus Accuracy



Profiles of a Biometrics Characteristic



Security Issues for User Authentication

- Client attacks: an adversary attempts to achieve user authentication without access to the remote host or to intervening communication.
- Host attacks are directed at the user file at the host where password, token passcodes, or biometrics templates are stored.
- Eavesdropping: in the context of passwords refers to an adversary's attempt to learn the password by observing the user. Such as user's keystrokes.
- Replay attacks involve an adversary repeating a previously captured user response.
- Denial-of-service: disable a user authentication service by flooding the service with numerous authentication attempts.

Bypass Facial Recognition Security


thank you