INDUSTRIAL UNIVERSITY OF HOCHIMINH CITY

Chương 7:
CHỨNG THỰC và
ĐIỀU KHIỂN TRUY CẬP
(Authentication and Access Control)

Nội dung

1. Khái niệm cơ bản
2. Các phương pháp chứng thực và điều khiển truy xuất

INDUSTRIAL UNIVERSITY OF HOCHIMINH CITY

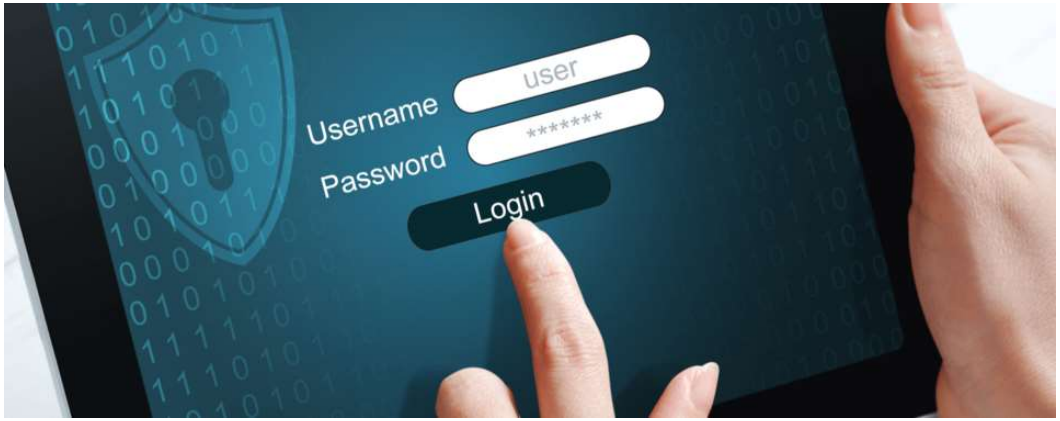
1. Khái niệm cơ bản

Chứng thực/xác thực

- **Chứng thực (Authentication)**
  - là một hành động nhằm thiết lập hoặc chứng thực một cái gì đó (hoặc một người nào đó) đáng tin cậy, có nghĩa là, những lời khai báo do người đó đưa ra hoặc về vật đó là sự thật.
  - một quy trình dùng để xác minh sự nhận dạng của một người dùng, hoặc thông điệp/dữ liệu
  - Phải cung cấp một nhân tố nào đó để chứng thực

Chứng thực/xác thực

- **Ví dụ: Web Application Authentication**
  - Nhận dạng bạn là ai
  - Bạn được quyền sử dụng/ truy xuất thông tin dữ liệu nào



Chứng thực/xác thực

- Mobile Connect Authentication

Sự ủy quyền

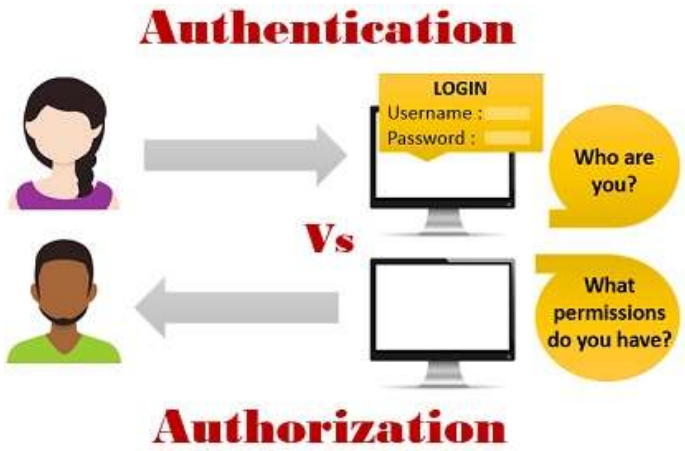
- **Sự ủy quyền hay sự cấp phép (Authorization)**
  - một quy trình nhằm xác minh rằng một người dùng biết trước, có quyền lực để thao tác một quá trình hoạt động nào đó hay không.
  - Sự chứng thực phải được tiến hành trước sự ủy quyền

Sự ủy quyền

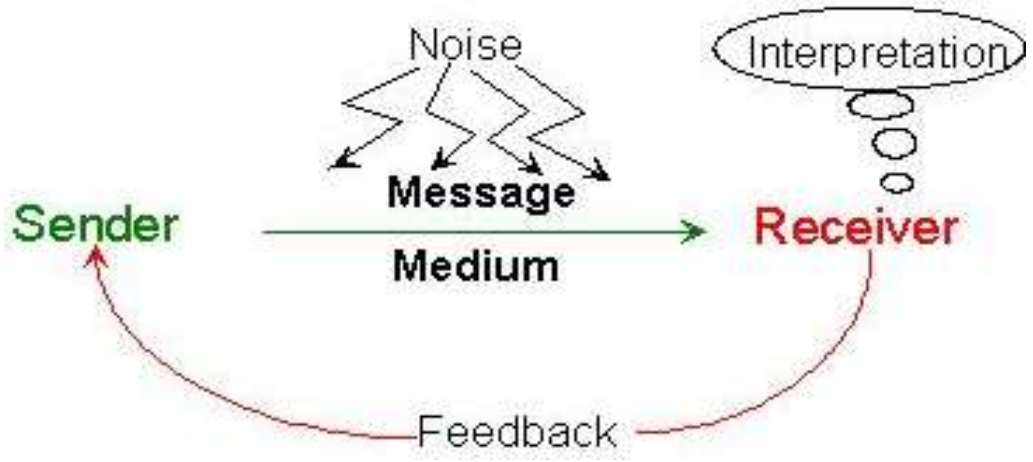
Các quyền:

- Quyền đọc (*Read (R)*)
  - Đọc nội dung của tập tin
  - Liệt kê danh sách thư mục
- Quyền viết (*Write (W)*)
  - Cộng thêm
  - Sinh tạo cái mới
  - Xóa bỏ
  - Đổi tên
- Quyền thi hành (*Execute (X)*): thi hành (chạy) chương trình ứng dụng.

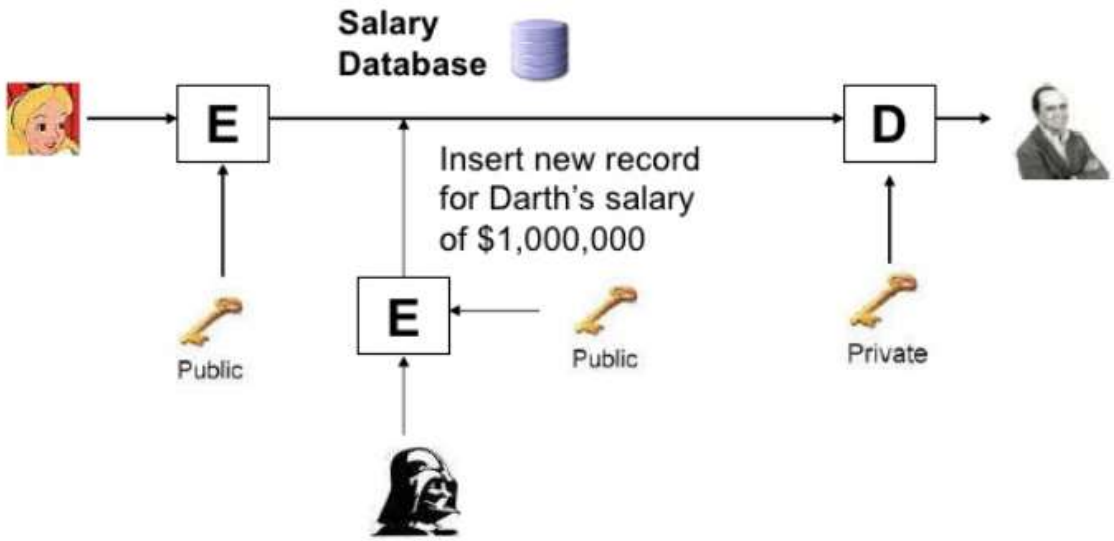
Authentication vs. Authorization



Trao đổi thông điệp

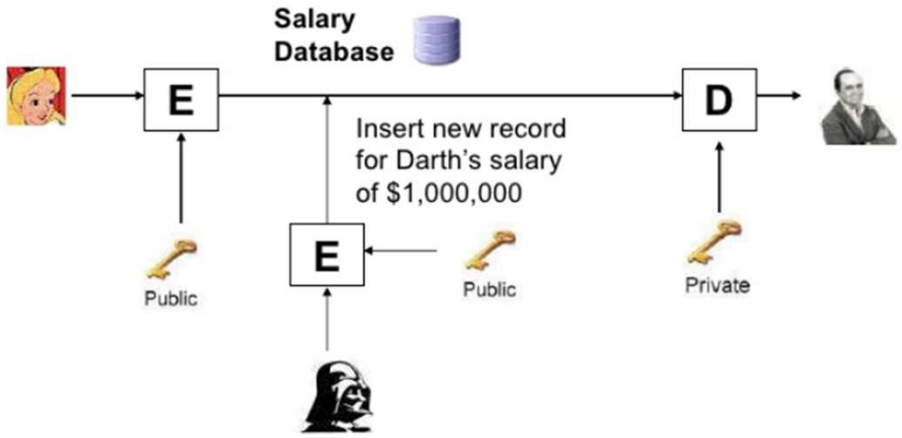


Trao đổi thông điệp



Trao đổi thông điệp

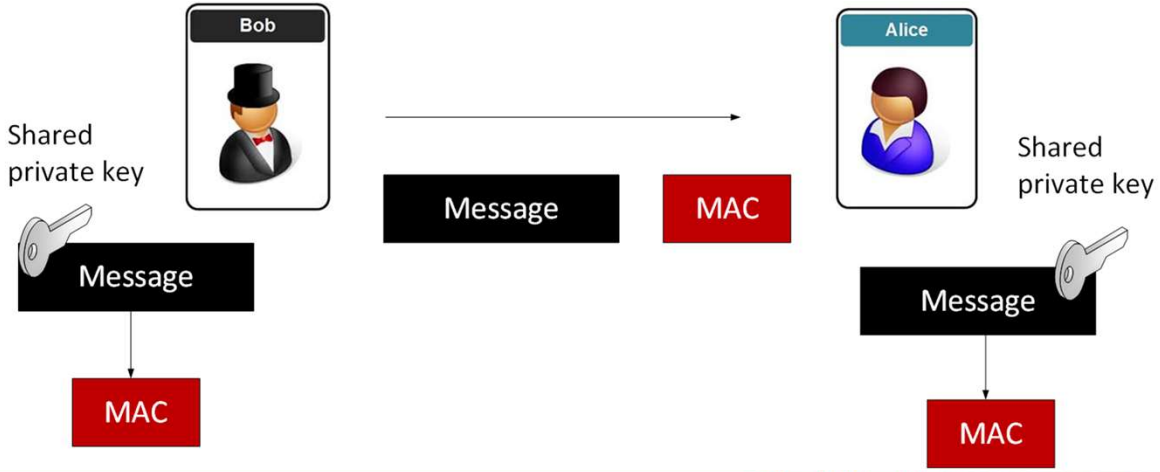
- Vấn đề?



- Cần có cơ chế nhận dạng sự thay đổi thông điệp bất hợp pháp

Chứng thực thông điệp

- Chứng thực thông điệp (Message Authentication)
  - Xác thực nguồn gốc thông điệp
  - Xác thực tính toàn vẹn của thông điệp
  - Chống từ chối thông điệp



Chứng thực thực thể

- **Chứng thực thực thể (Entity Authentication)**:

  là một kỹ thuật được thiết kế cho phép một bên (party) chứng minh sự nhận dạng (identity) của một bên khác.

- **Thực thể (Entity) là gì:**

  Có thể là một con người, tiến trình, client, hoặc một server. Thực thể mà danh tính cần được chứng minh được gọi là **người thỉnh cầu (Claimant);** bên mà cố gắng chứng minh identity của claimant được gọi là **người thẩm định (verifier)**

Chứng thực thực thể

- Một cái gì đó để người thẩm tra có thể nhận dạng ra người thỉnh cầu được gọi là vật chứng
- Có ba loại vật chứng:
  - **Những gì bạn biết (Something known)**: Là một bí mật chỉ được biết bởi thỉnh cầu có thể được kiểm tra bởi người thẩm tra. Ví dụ: Password, Pin, secret key, private key.
  - **Những gì bạn có (Something possessed)**: là một thứ mà có thể chứng minh nhận dạng của người thỉnh cầu. Ví dụ: passport, bằng lái xe, chứng minh nhân dân, credit card, smart card
  - **Những gì vốn sẵn có (Something inherent)**: là một đặc tính vốn sẵn có của người thỉnh cầu. Ví dụ: Chữ ký thông thường, vân tay, giọng nói, đặc tính khuôn mặt, võng mạc, và chữ viết tay.

Chứng thực thực thể

Chứng thực thực thể

Chứng thực thực thể

Chứng thực thông điệp và chứng thực thực thể

- Chứng thực thông điệp
  - Không cần xảy ra theo thời gian thực; Ví dụ: Alice gửi thông điệp cho Bob, khi Bob chứng thực thông điệp thì Alice có thể không cần phải có mặt ngay trong tiến trình giao tiếp
  - Chứng thực cho từng thông điệp

- Chứng thực thực thể
  - Theo thời gian thực. Ví dụ: Alice cần online và tham gia tiến trình giao tiếp, thông điệp chỉ được trao đổi khi được chứng thực
  - Chứng thực trong suốt section

Điều khiển truy cập

- Cấp phép hoặc từ chối phê duyệt sử dụng các tài nguyên xác định.
- Là cơ chế của hệ thống thông tin cho phép hoặc hạn chế truy cập đến dữ liệu hoặc các thiết bị.
- Nhiệm vụ điều khiển truy cập trong an ninh máy tính bao gồm:
  - Nhận diện: Người dùng trình ra các vật chứng để chứng minh sự nhận diện
  - Chứng thực: Kiểm tra, xác minh các ủy quyền
  - Ủy quyền: Cấp các quyền để thực hiện hành động truy cập
  - Truy cập: thực hiện truy xuất các tài nguyên xác định

2. Phương pháp chứng thực và điều khiển truy cập

Mật khẩu (Password)
Sinh trắc học (Biometrics)

2.1 Dùng mật khẩu (Password)

- Là phương pháp đơn giản và lâu đời nhất, được gọi là Password-based Authentication, password là một thứ mà người dùng biết.
- Một Password được dùng khi một người dùng cần truy xuất một hệ thống để sử dụng nguồn tài nguyên của hệ thống.
- Khi đăng nhập vào hệ thống, người dùng được yêu cầu
  - Xác định danh tính – một **định danh người dùng (user identification) công khai**
  - Cung cấp thông tin xác thực - một **password bí mật**.
- Có 2 cơ chế password:
  - **Fixed password**
  - và **one-time password**

2.1 Dùng mật khẩu (Password)

Nhược điểm:

- Điểm yếu của mật khẩu có liên quan đến trí nhớ con người
  - Con người chỉ có thể nhớ một số lượng mật khẩu nhất định
  - Mật khẩu dài, phức tạp đem lại hiệu quả tốt nhưng khó nhớ
- Mỗi tài khoản có mật khẩu khác nhau
- Chính sách an toàn mật khẩu đòi hỏi mật khẩu chỉ có hiệu lực trong một khoảng thời gian
  - Người dùng ghi nhớ mật khẩu nhiều lần
- Người dùng thường chọn đường tắc
  - Dùng mật khẩu yếu
  - Sử dùng 1 mật khẩu cho nhiều tài khoản

Tấn công mật khẩu

- Kỹ nghệ xã hội
  - Lừa đảo, nhìn trộm, lục lọi
- Chụp lén
  - Trình theo dõi thao tác bàn phím, phân tích giao thức
  - Tấn công "man in the middle"
- Dò và vét cạn
- Tấn công dò tự điển

2.1.1 Fixed Password

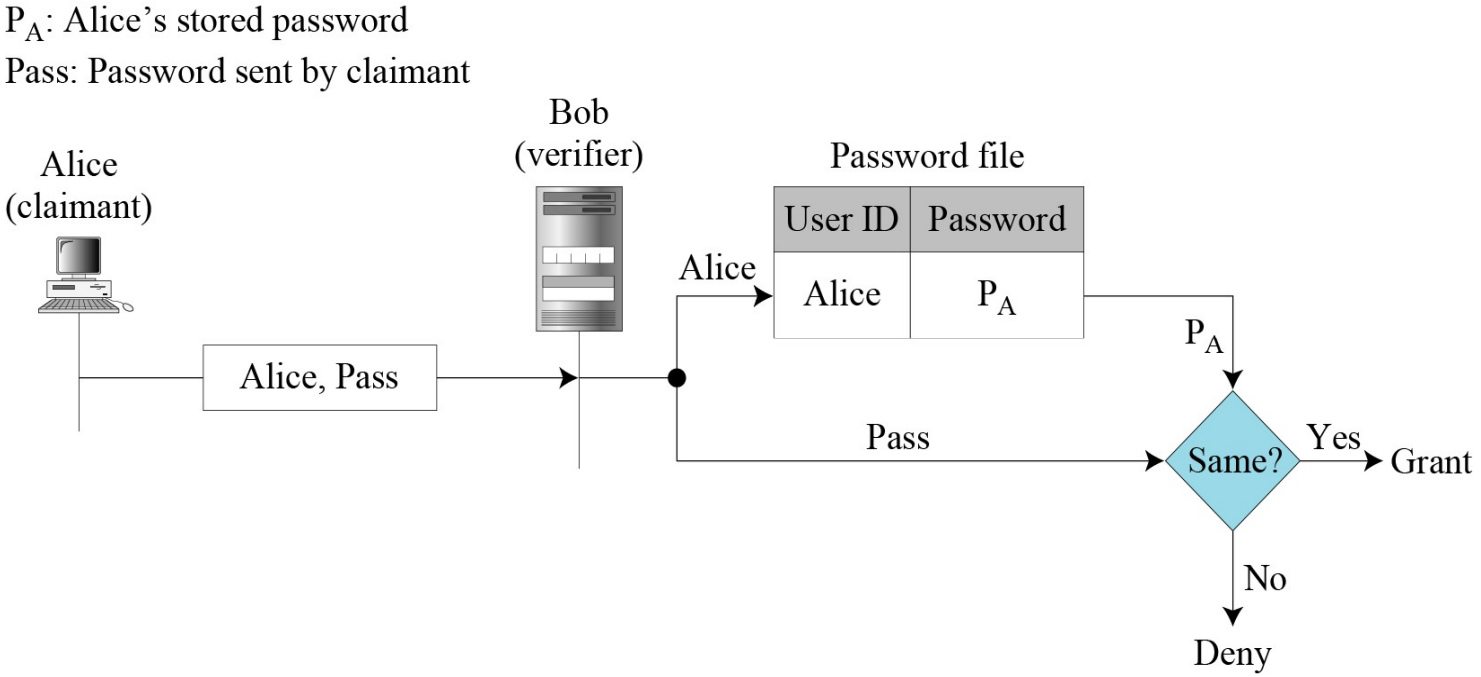
- Là một password được dùng lặp đi lặp lại mỗi lần truy xuất
- Có 3 cơ chế được xây dựng theo hướng này
  - **User ID và Password File**
  - **Hashing the password**
  - **Salting the password**
  - **Two identification techniques are combined**

Fixed Password

- **User ID và Password File**
  - Rất thô sơ, User ID và Password được lưu trong một tập tin.
  - Để truy xuất tài nguyên, người dùng gửi bản rõ của User ID và Password đến hệ thống. Nếu Password trùng khớp với Password trong hệ thống, thì quyền truy xuất được gán ngược lại từ chối.

Fixed Password

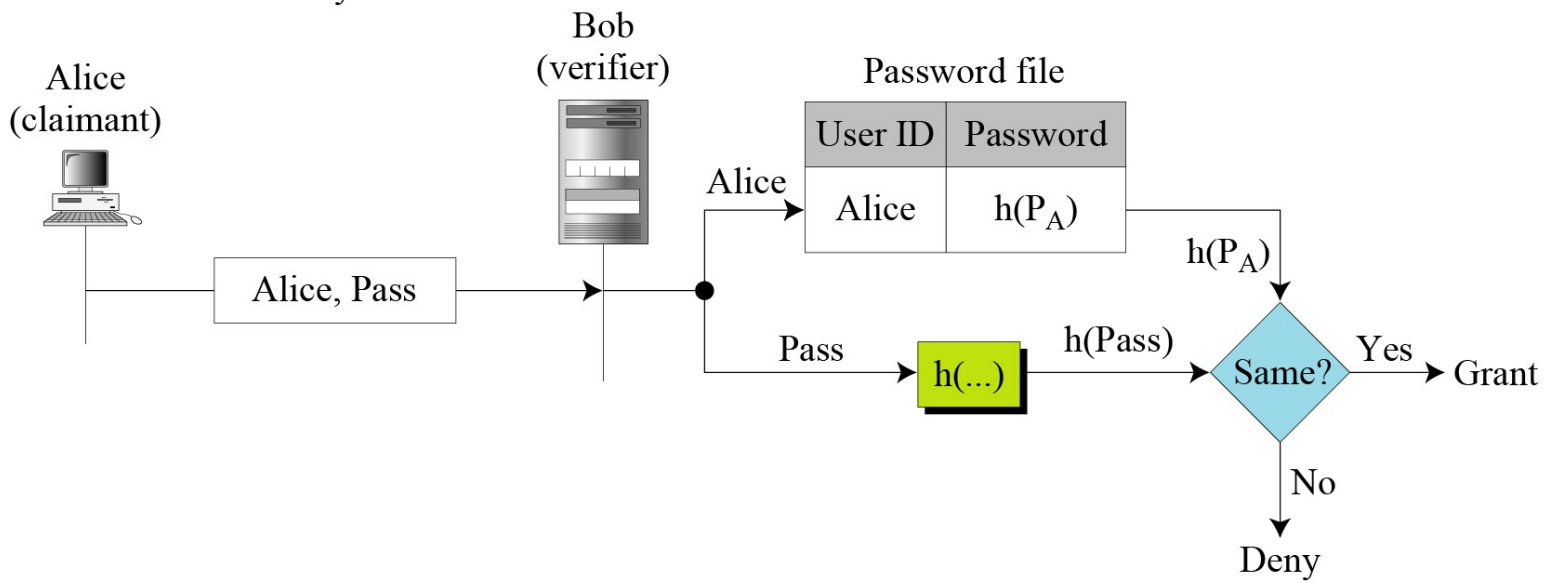
User ID và Password File



Fixed Password

- **Hashing the password**

P_A: Alice's stored password
Pass: Password sent by claimant



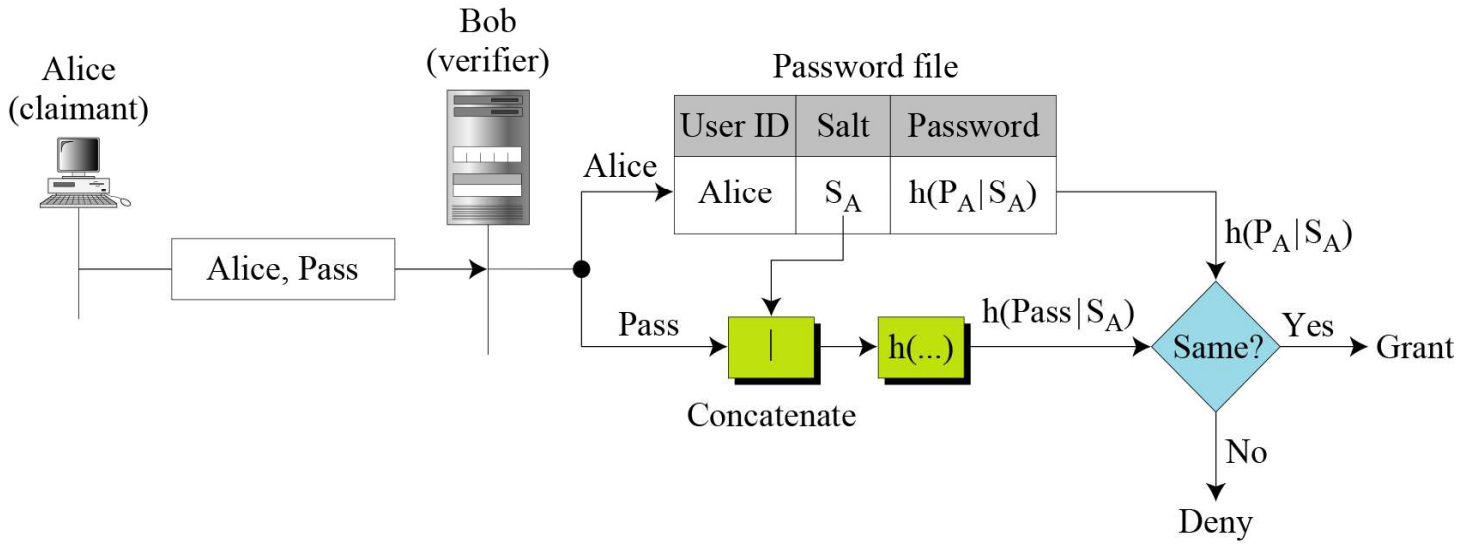
Fixed Password

Salting the password

P_A: Alice's password

S_A: Alice's salt

Pass: Password sent by claimant



Fixed Password

- **Two identification techniques are combined**

  A good example of this type of authentication is the use of an ATM card with a PIN (personal identification number).

2.1.2 One-Time Password

- Là mật khẩu **sử dụng một lần duy nhất** gồm một dãy các ký tự hoặc chữ số ngẫu nhiên được gửi đến số điện thoại nhằm xác nhận giao dịch.
- Mã OTP được tạo ra dựa trên bộ vi xử lý hoặc thẻ khóa kích thước bỏ túi tạo mã số và chữ số để xác thực quyền truy cập vào hệ thống hoặc giao dịch. Sau 30s đến 2 phút, mã này lại bị thay đổi một lần.

2.1.2 One-Time Password

- Mã OTP có thể được triển khai bằng phần cứng, phần mềm hoặc theo yêu cầu.
- Mã OTP được dùng làm **bảo mật 2 lớp** trong các giao dịch xác minh đăng nhập và đặc biệt là giao dịch với tài khoản ngân hàng, nhờ đó, giảm thiểu tối đa rủi ro bị tấn công khi lộ mật khẩu hay tin tặc tấn công.

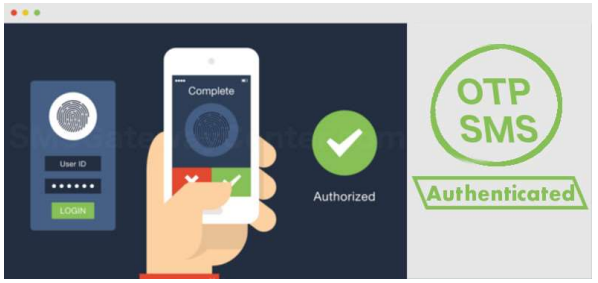
2.1.2 One-Time Password

Những loại mã OTP phổ biến hiện nay

- SMS OTP
- TOKEN KEY (TOKEN CARD)
- SMART OTP – SMART TOKEN

SMS OTP

- Mã OTP được gửi qua SMS đến số điện thoại của khách hàng khi cần xác thực giao dịch
- Đa số ngân hàng tại Việt Nam: OTP vietcombank, otp techcombank, otp sacombank, otp bidv
- Bạn đang ở trong khu vực sóng kém hoặc ngoài vòng phủ sóng thì bạn không thể nhận được mã SMS OTP→ SMS OTP sẽ không sử dụng được.



TOKEN KEY (TOKEN CARD)

- Là thiết bị bảo mật mà doanh nghiệp cung cấp dịch vụ cung cấp cho khách hàng
- Token Key có thể tạo ra **mã OTP gồm 6 ký tự**, cứ sau mỗi phút nó sẽ tự động được tạo ra mà không cần thông qua Internet.
- Mỗi tài khoản phải đăng ký riêng một Tokey key, và thông tin về Token key được thay đổi sau một khoản thời gian quy định.
- Loại thiết bị này cực kỳ tiện lợi khi luôn mang theo bên người. Tuy nhiên, bạn cần phải bảo quản thật cẩn thận.

SMART OTP

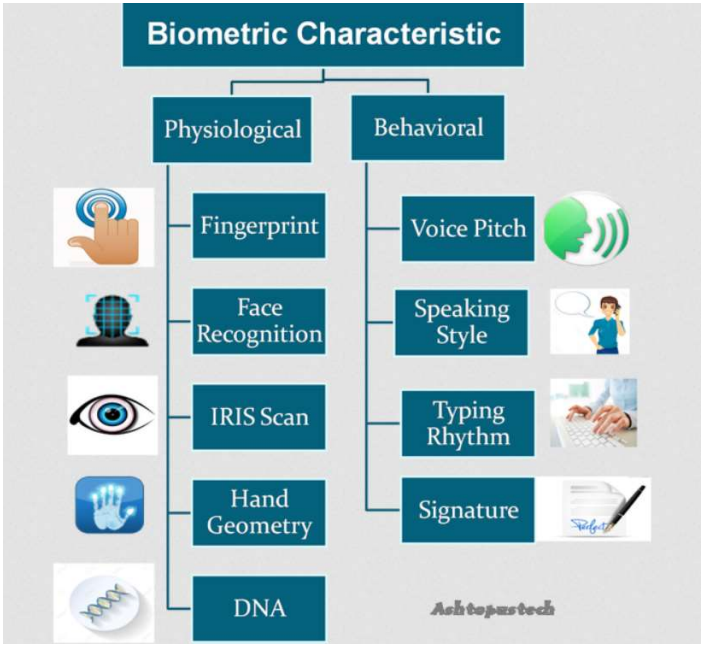
- Smart OTP là dạng OTP tốt nhất hiện nay
- Smart OTP là sự kết hợp hài hoà giữa Token Key và SMS OTP.
- Smart OTP có thể được sử dụng mọi lúc mọi nơi vì nó được tích hợp sẵn trên ứng dụng của điện thoại. Khi có phiên giao dịch trực tuyến thì Smart OTP sẽ được gửi về ứng dụng trên smartphone.
- Hai ngân hàng đã sử dụng cách thanh toán tiền Online bằng phương thức Smart OTP và SMS OTP là Vietcombank và TPBank. Người dùng phải kê khai thông tin và đăng ký trực tiếp với ngân hàng họ muốn. Lưu ý, mỗi thiết bị chỉ nên dùng 1 mã OTP riêng biệt.

Mã OTP có thực sự an toàn?

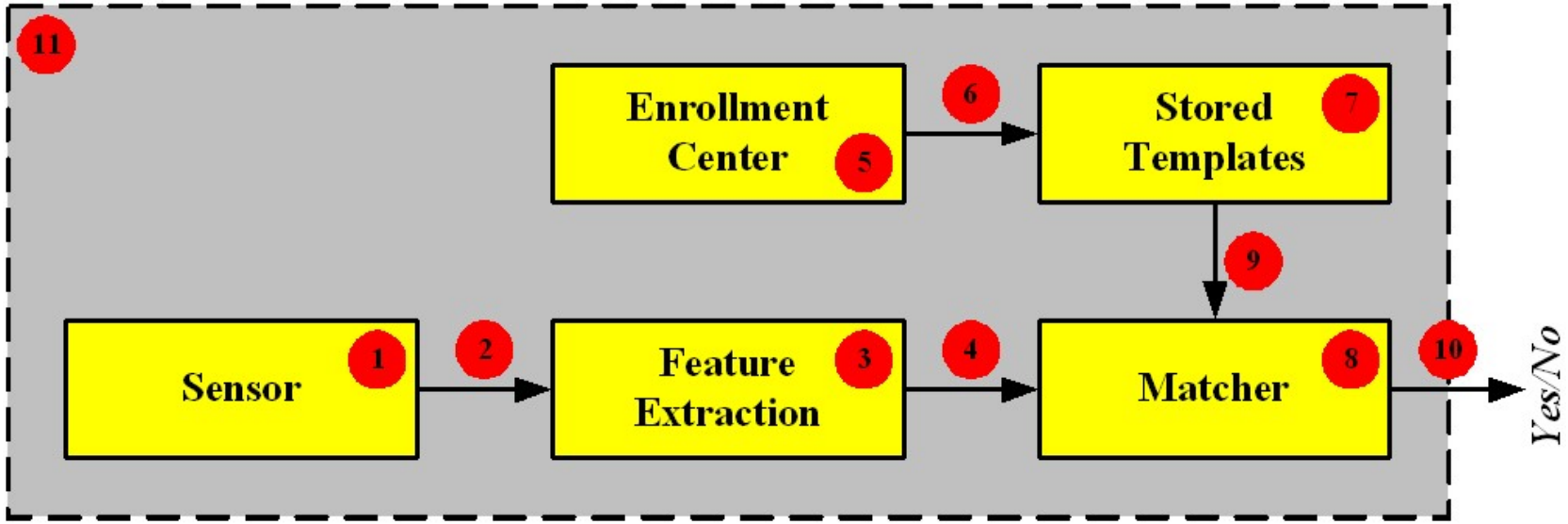
- Mã OTP là lớp bảo mật cuối cùng trước khi hoàn tất giao dịch. Do đó, phải cẩn thận kiểm tra lý do và số tiền (nếu có trong tin nhắn xác thực giao dịch) trước khi nhập mã OTP.
- Với SMS OTP, khi mất điện thoại, bạn cần phải báo ngay cho ngân hàng để khóa tạm thời tính năng này. Với Token, bạn phải luôn mang theo nó bên mình và đặt mật khẩu có tính phức tạp và lưu giữ để phòng khi quên.
- Mã OTP sẽ an toàn tuyệt đối nếu như bạn tuân thủ đúng các nguyên tắc cũng như quy trình sử dụng dịch vụ Internet Banking mà ngân hàng đưa ra.

2.2 Biometrics

- Sinh trắc học (Biometric) là phép đo lường về các đặc tính sinh lý học hoặc hành vi học để nhận dạng một người.
- Sinh trắc học đo lường các đặc tính mà không thể đoán, ăn cắp hoặc chia sẻ.



Qui trình xác thực bằng Biometrics

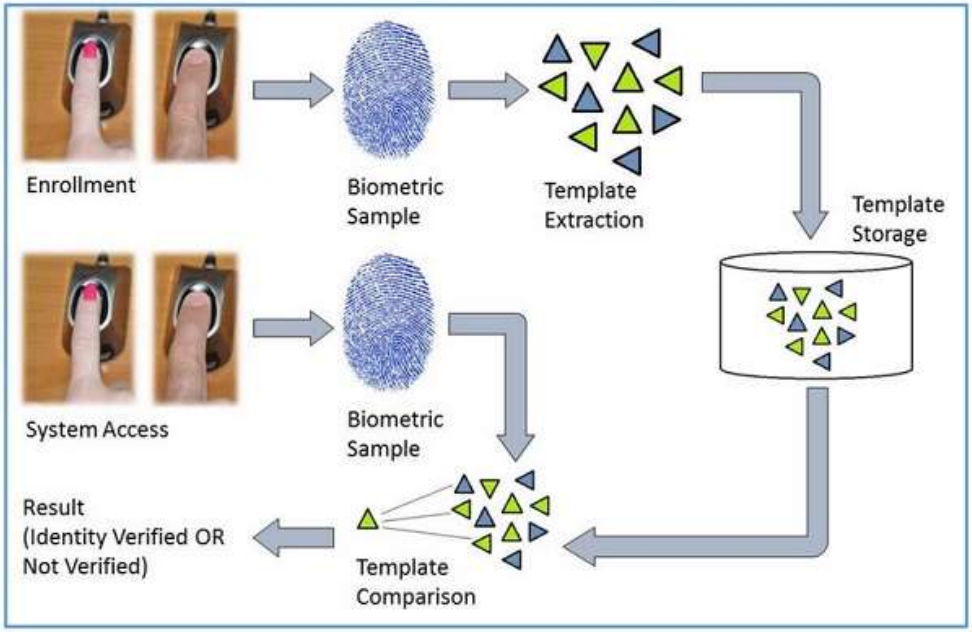


Qui trình xác thực bằng Biometrics

- Chúng ta sẽ thảo luận các vấn đề sau
  - Components (thành phần)
  - Enrollment (ghi nhận vào)
  - Authentication (chứng thực)
  - Techniques (Kỹ thuật)
  - Accuracy (độ chính xác)
  - Applications (các cứng dụng)

Components

- Vài Component cần cho sinh trắc học, bao gồm:
  - các thiết bị thu nhận đặc tính của sinh trắc học
  - Chương trình xử lý các đặc tính sinh trắc học
  - Các thiết bị lưu trữ.



Enrollment

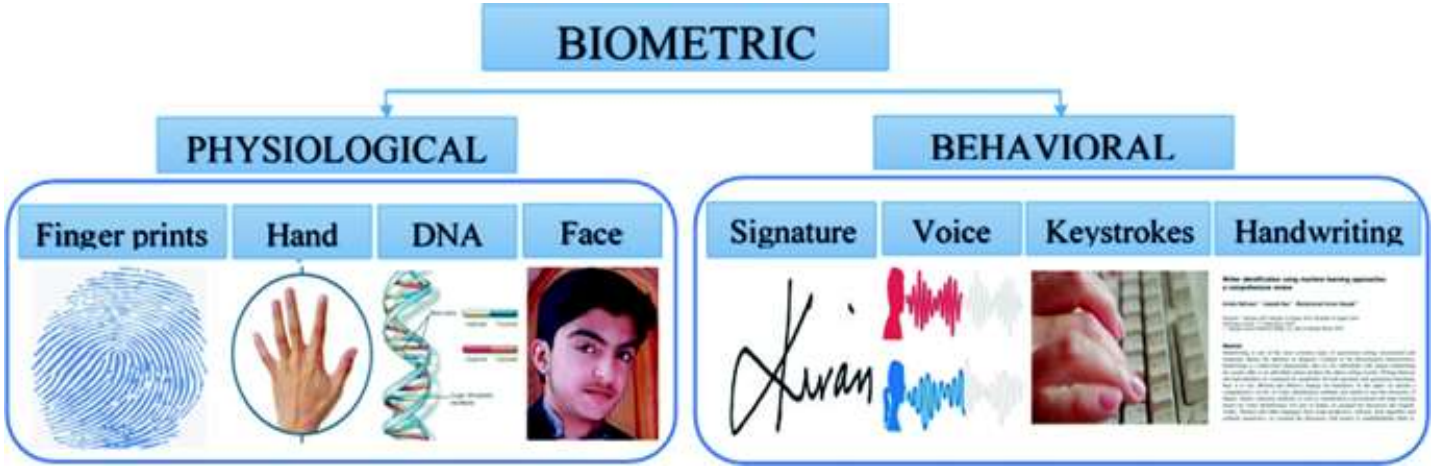
- Trước khi dùng bất cứ kỹ thuật sinh trắc học để chứng thực, đặc tính tương ứng của mỗi người trong cộng đồng cần phải có sẵn trong CSDL, quá trình này được gọi là enrollment

Authentication

- Chứng thực (Authentcation) được thực hiện bởi sự thẩm tra (Verification) hoặc nhận dạng (identication)
  - Verification: Đặc tính của một người được so khớp với một mẫu tin đơn trong CSDL để xác định cô ta có phải là người mà cô ta đang tự khai không
  - Identication: Đặc tính của một người được so khớp với tất cả các mẫu tin có trong CSDL để xác định cô ta có một mẫu tn trong CSDL.

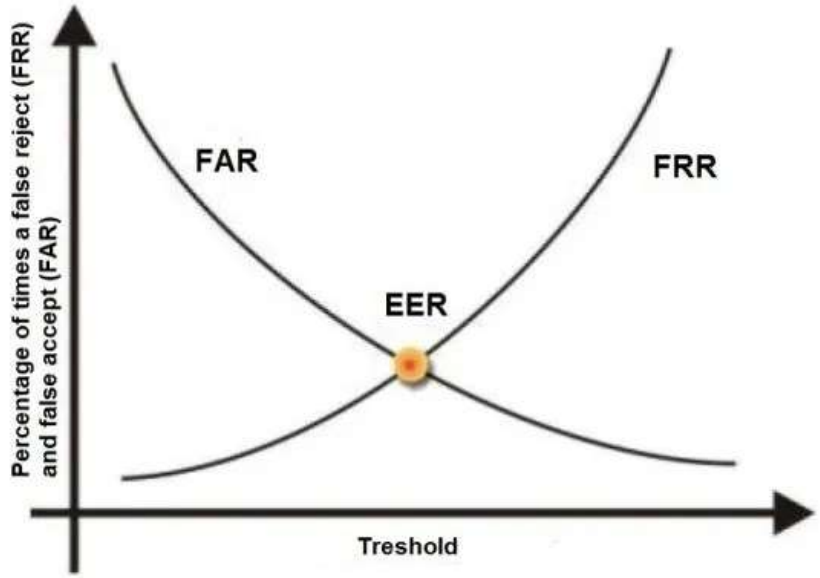
Techiques

- Chúng ta nên chọn kỹ thuật sinh trắc học nào phù hợp cho ứng dụng



Accuracy

- Độ chính xác (Accuracy) của các kỹ thuật sinh trắc học được đo lường bằng cách dùng hai tham số:
  - **False Rejection Rate (FRR)**
  - **False Acceptance Rate (FAR)**



Applications

- Rất nhiều ứng dụng của sinh trắc học đã được áp dụng trong nhiều lĩnh vực khác nhau.
  - Kiểm soát truy cập nơi làm việc
  - Điều khiển truy xuất hệ thống và thông tin nhạy cảm
  - Thực thi các giao dịch thương mại điện tử trực tuyến
  - Nhận dạng tội phạm bằng cách phân tích DNA
  - Kiểm soát nhập cư

Ưu và nhược điểm của Biometric

Ưu điểm:

- Biometrics không thể bị mất, đánh cắp, bỏ quên. Nó nhất quán và vĩnh cửu
- Nó không thể được chia sẻ hoặc dùng bởi người khác
- Không đòi hỏi phải ghi nhớ như mật khẩu, mã Pin
- Biometric luôn luôn sẵn dùng cho cá nhân và duy nhất

Ưu và nhược điểm của Biometric

Nhược điểm:

- Chi phí cho thiết bị phần cứng
- Các bộ đọc đặc tính của sinh trắc học có những lỗi nhất định
  - Từ chối người dùng hợp lệ
  - Chấp nhận người dùng không hợp lệ