

CƠ SỞ AN TOÀN THÔNG TIN

Bài 04. Định danh và xác thực

1

Nhân tổ xác thực

2

Mật khẩu

3

Xác thực bằng
mật khẩu

1

Nhân tố xác thực

2

Mật khẩu

3

Xác thực bằng
mật khẩu

Định danh

- ❑ **Định danh** (identification) là việc gắn định danh (identifier) cho người dùng và kiểm tra sự tồn tại của định danh đó
 - Qua xưng danh ở trạm kiểm tra (công cơ quan, cửa khẩu...)
 - Qua tên người dùng được truyền tới máy chủ (từ cửa sổ đăng nhập, từ webpage...)
 - Qua địa chỉ email trong một thư điện tử
 -
- ❑ **Quá trình định danh không bao gồm việc kiểm tra tính chân thực của danh tính**

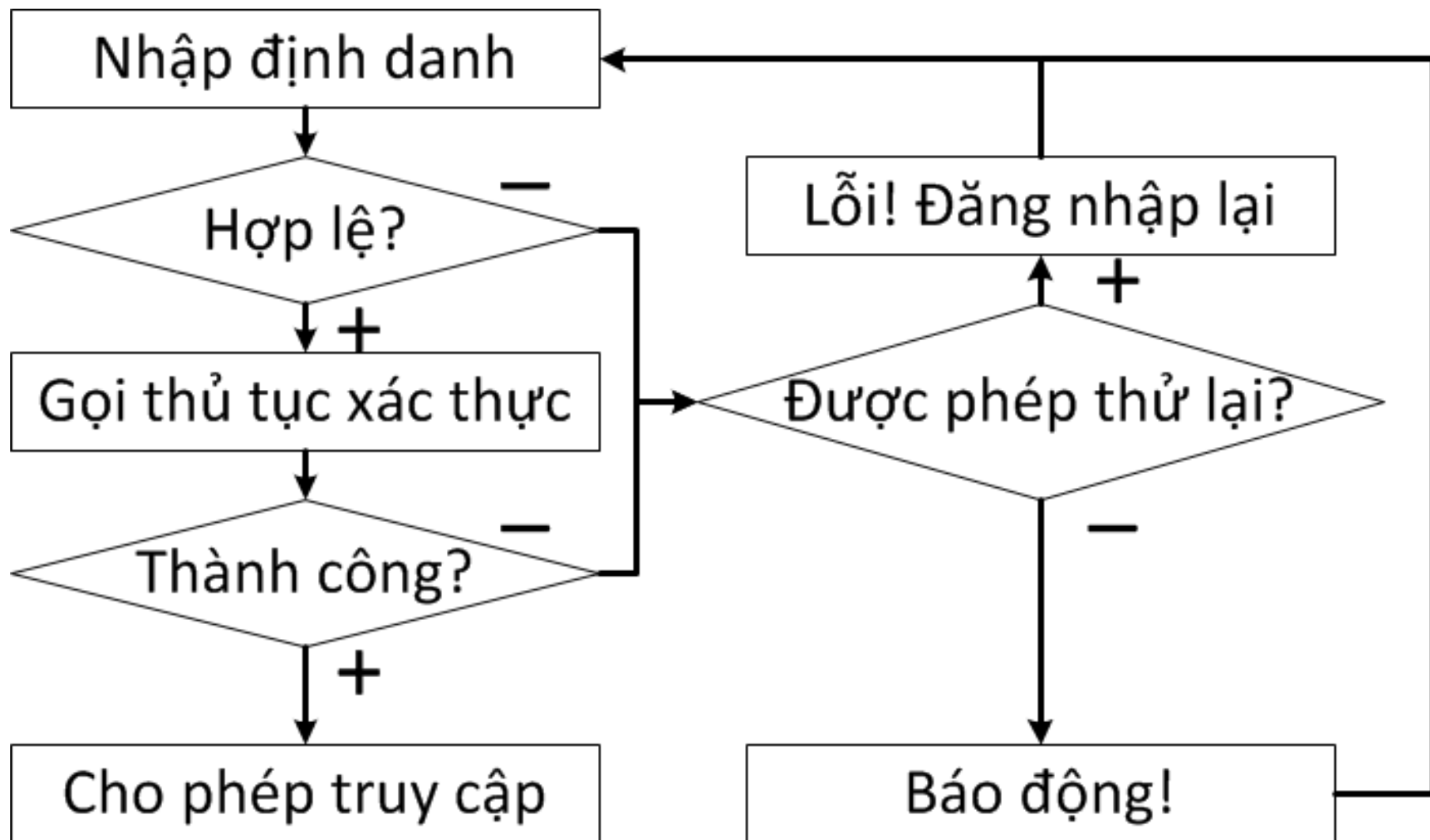
Giải pháp định danh

- Số hiệu (ID)
- Username
- Số điện thoại
- Email
- Tài khoản mạng xã hội
-

Xác thực

- ❑ **Xác thực** (authentication) là quá trình kiểm tra tính chân thực của danh tính được xác lập trong quá trình định danh
 - Là kiểm tra xem một người có đúng là có danh tính như đã đưa lên/ gửi lên hay không.
 - Việc kiểm tra được thực hiện nhờ các nhân tố xác thực và giao thức xác thực.
 - Không bao gồm việc xác định quyền hạn của người dùng trong hệ thống.
- ❑ **Các bên tham gia xác thực**
 - Claimant: Bên yêu cầu xác thực (client)
 - Verifier: Bên xác thực (server)

Sơ đồ định danh và xác thực



Nhân tố xác thực

- ❑ **Nhân tố xác thực** (authentication factor) là thông tin sử dụng cho quá trình xác thực.
- ❑ Có 3 loại nhân tố xác thực chính
 - Cái người dùng biết (Something you know)
 - Cái người dùng có (Something you have)
 - Cái thuộc về bản thể người dùng (Something about you/that you are)
- ❑ Có 2 nhóm nhân tố xác thực khác
 - Đặc điểm hành vi người dùng
 - Vị trí của người dùng

Nhân tố xác thực

❑Cái người dùng biết

- Thường là mật khẩu (password)
- Ngoài ra: trả lời cho một số câu hỏi riêng tư. Chủ yếu để khôi phục mật khẩu.
- **Ưu điểm:** đơn giản, chi phí thấp
- **Nhược điểm:**
 - Có thể bị lộ (đánh cắp)
 - Có thể bị quên

Nhân tố xác thực

❑Cái người dùng có

- Chìa khóa, giấy tờ tùy thân
- Thẻ từ, smartcard
- OTP token, Cryptographic token, khóa mật mã
- SIM điện thoại
- **Ưu điểm:** phù hợp cho xác thực đa nhân tố
- **Nhược điểm:**
 - Chi phí cao
 - Có thể bị mất, chiếm đoạt, làm giả

Nhân tố xác thực

❑ Cái thuộc về bản thể người dùng

- Khuôn mặt, vân tay, bàn tay
- Vỗng mạc
- Giọng nói
- **Ưu điểm:** không bị sao chép, làm mất, đánh cắp
- **Nhược điểm:**
 - Chi phí rất cao
 - Có thể thay đổi theo thể trạng
 - Không phù hợp cho xác thực qua mạng

Nhân tố xác thực

❑ Đặc điểm hành vi người dùng

- Chữ ký bàn phím
- Chữ ký viết tay (tốc độ và gia tốc)
- **Ưu điểm:** không bị sao chép, đánh cắp
- **Nhược điểm:**
 - Chi phí cao
 - Không ổn định; có thể thay đổi theo thời gian
 - Không phù hợp cho xác thực qua mạng

Nhân tố xác thực

❑ Các đặc trưng liên quan đến người dùng

- Vị trí trên mặt đất (qua hệ thống định vị toàn cầu)
- **Nhược điểm:**
 - Chi phí rất cao
 - Làm lộ thông tin riêng tư người dùng

Nhân tố xác thực

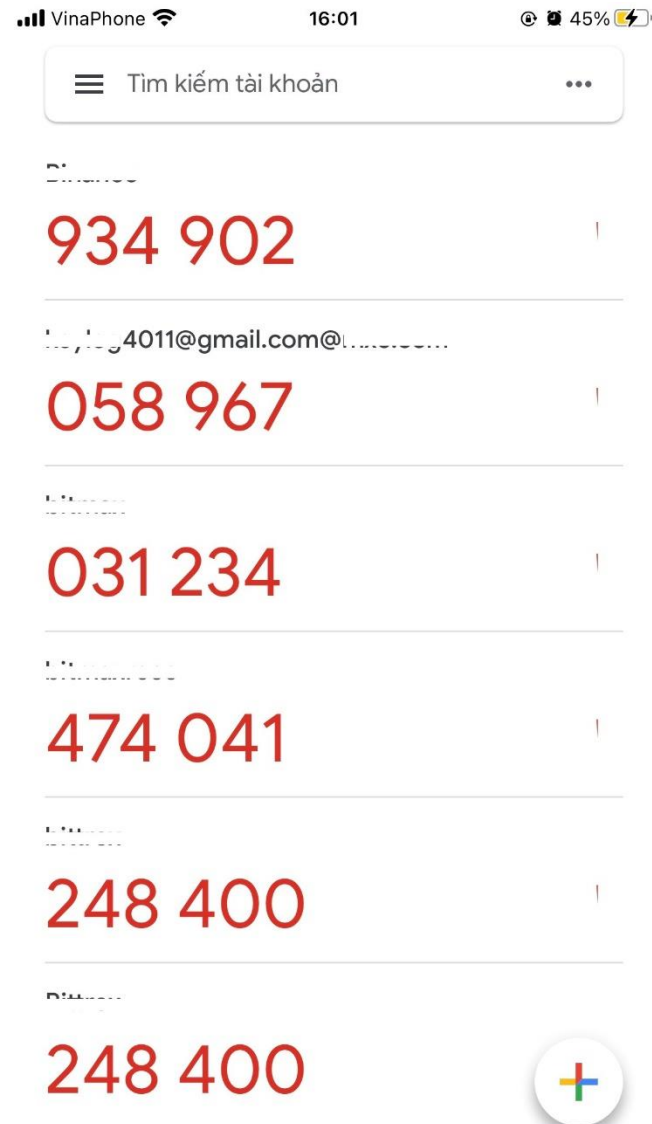
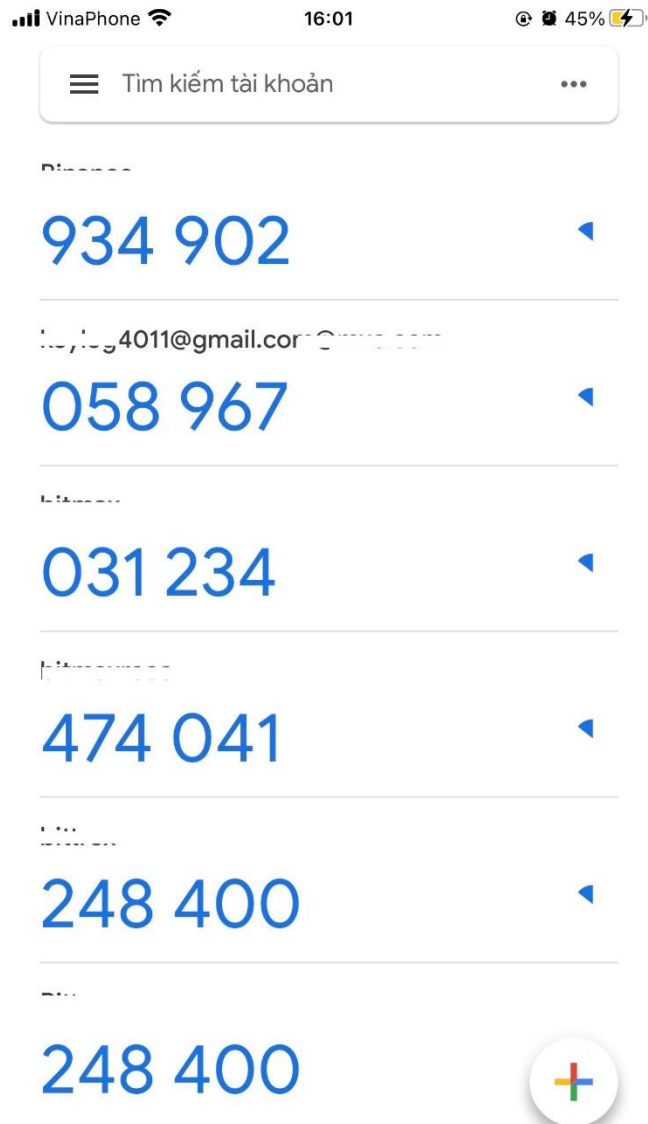
Xác thực đa nhân tố

- Thẻ từ, smartcard, token + mã PIN
- Mật khẩu + mật khẩu một lần (OTP – One Time Password)
- Mật khẩu + vị trí địa lý

❑ Mật khẩu một lần OTP

- Sinh ngẫu nhiên bởi verifier
- Sinh bởi cả hai bên dựa trên đồng bộ bộ đếm (RFC-4226)
- Sinh bởi cả hai bên dựa trên đồng bộ thời gian (RFC-6238)

Nhân tố xác thực



1

Nhân tổ xác thực

2

Mật khẩu

3

Xác thực bằng
mật khẩu

Khái niệm mật khẩu

- ❑ **Mật khẩu** là một lượng thông tin mật nào đó, mà chỉ có người dùng và hệ mật khẩu được biết, người dùng cần phải nhớ và đưa ra để đi qua thủ tục xác thực.
- ❑ **Mật khẩu một lần** để người dùng xác thực một lần
- ❑ **Mật khẩu dài hạn** có thể để qua xác thực nhiều lần

Đặc điểm của mật khẩu

- Là kỹ thuật xác thực được sử dụng phổ biến nhất hiện nay
- Đơn giản, thuận tiện, chi phí thấp
- Về lý thuyết, nếu chọn mật khẩu một cách đúng đắn thì sẽ đảm bảo an toàn
- Độ an toàn của mật khẩu phụ thuộc độ dài mật khẩu và kích thước tập kí tự
 - Tập kí tự thường: $N = 26^n$
 - Tập kí tự thường và hoa: $N = 52^n$
 - Tập kí tự thường, hoa và số: $N = 62^n$

An toàn mật khẩu

❑ Nguyên nhân mật khẩu kém an toàn

- Để không bị quên, người dùng có xu hướng chọn mật khẩu đơn giản, dễ nhớ
- Nhiều người sử dụng mật khẩu mặc định của sản phẩm, không thay đổi
- Người dùng có thể lưu mật khẩu vào đâu đó để xem lại khi lỡ quên
- Sử dụng chung một tài khoản cho nhiều hệ thống khác nhau

An toàn mật khẩu

Top 25 most common passwords by year according to SplashData

Rank	2011 ^[4]	2012 ^[5]	2013 ^[6]	2014 ^[7]	2015 ^[8]	2016 ^[3]	2017 ^[9]	2018 ^[10]	2019 ^[11]
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1234567
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	12345
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty	111111
10	dragon	baseball	adobe123 ^[a]	football	baseball	1234	iloveyou	iloveyou	123123

An toàn mật khẩu

Vị trí	Mật khẩu	Số người dùng	Thời gian bẻ khoá	Số lần xâm nhập
99. ↑ (186)	jordan23	22,711	Ít hơn 1 giây	333,759
100. mới	789456123	22,592	Ít hơn 1 giây	389,398
101. ↓ (55)	jordan	22,449	Ít hơn 1 giây	305,014
102. mới	anhyeuem	22,265	Ít hơn 1 giây	47,486
103. ↑ (171)	killer	22,242	Ít hơn 1 giây	322,975
104. ↓ (75)	basketball	22,060	10 giây	224,737
105. ↓ (49)	michelle	22,012	3 giờ	285,542
106. mới	1q2w3e	21,906	Ít hơn 1 giây	513,929
107. ↑ (187)	lol123	21,881	Ít hơn 1 giây	188,087
108. ↑ (167)	qwerty1	21,610	Ít hơn 1 giây	586,071
109. mới	789456	21,589	Ít hơn 1 giây	293,902

Hiểm họa an toàn đối với mật khẩu (1/3)

- Thông qua tìm kiếm, dò đoán
- Nhìn trộm
- Qua bàn giao định trước mật khẩu cho người khác
- Đánh cắp CSDL của hệ mật khẩu
- Chặn bắt các thông tin chứa mật khẩu
- Khai thác các lỗi ở giai đoạn thiết kế.

Hiểm họa an toàn đối với mật khẩu (2/3)

- Làm hỏng hệ mật khẩu
- Lựa chọn mật khẩu dễ nhớ và cũng dễ đoán
- Ghi các mật khẩu khó nhớ và lưu ghi chép đó tại nơi dễ tiếp cận
- Cho người khác mật khẩu một cách cố ý hoặc do nhầm lẫn.

Hiểm họa an toàn đối với mật khẩu (3/3)

HIỂM HỌA AN TOÀN KHI TRUYỀN MẬT KHẨU QUA MẠNG

1. Chặn bắt và dùng lại thông tin.
2. Chặn bắt và khôi phục mật khẩu
3. Thay đổi thông tin với mục đích đánh lừa phía kiểm tra.
4. Kẻ xấu bắt chước hành động của phía kiểm tra để đánh lừa người dùng.

Công cụ dò mật khẩu

- Hiện có rất nhiều công cụ để dò mật khẩu (password cracking tool)
- Nhiều công cụ được phát triển riêng cho các ứng dụng cụ thể (WinRAR, WinZIP, PDF, Word,...)
- Nhiều công cụ (gồm công cụ online) để dò mật khẩu từ giá trị băm (chủ yếu là MD5)

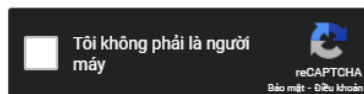
Công cụ dò mật khẩu

```
root@DESKTOP-9E3K85O:/home/longtn
File Actions Edit View Help
(root@DESKTOP-9E3K85O)-[/home/longtn]
# john hash.txt --show
backup.zip:741852963::backup.zip:style.css, index.php:backup.zip
1 password hash cracked, 0 left
```

```
~/backup/index.php [Read Only] - Mousepad
File Edit Search View Document Help
1<!DOCTYPE html>
2<?php
3session_start();
4if(isset($_POST['username']) && isset($_POST['password'])) {
5    if($_POST['username'] == 'admin' && md5($_POST['password']) ==
6        "2cb42f8734ea607eefed3b70af13bbd3") {
7        $_SESSION['login'] = "true";
8        header("Location: dashboard.php");
9    }
10 ?>
```

Enter up to 20 non-salted hashes, one per line:

2cb42f8734ea607eefed3b70af13bbd3



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
2cb42f8734ea607eefed3b70af13bbd3	md5	querty789

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Công cụ dò mật khẩu

❑ Cách dò mật khẩu của các công cụ

- Dò bằng từ điển (phụ thuộc ngôn ngữ)
- Vét cạn (brute force)

❑ Dò mật khẩu thủ công

- Dựa vào thông tin cá nhân của người dùng

❑ Tấn công đánh cắp mật khẩu

- Keylogger. Xem mật khẩu lưu trong ứng dụng
- Chặn bắt trên đường truyền (sniffing, DNS spoofing...)
- XSS, SQL Injection
- Lừa đảo (social engineering)

Dò mật khẩu thủ công

- Dò mật khẩu của “John”:
 - **Sally** (his wife)
 - **George** (his child)
 - **Randoff** (his wife’s maiden name)
 - **Tennis** (John’s favorite sport)
 - **March9** (date of John’s, or his child’s or wife’s bday)
 - **Waterfall** (a poster or some object seen in office)
 - **Alpha** (the brand of computer John uses)

YÊU CẦU QUẢN LÝ MẬT KHẨU (1/4)

1. Xác định độ dài cực tiểu của MK
 - Làm khó cho kẻ xấu muốn nhìn trộm hoặc tấn công bằng phương pháp “vét cạn”
2. Trong MK dùng các nhóm ký hiệu khác nhau
 - Hạn chế phương pháp tấn công “vét cạn” của đối phương
3. Kiểm tra và loại bỏ MK theo từ điển
 - Chống lại phương pháp đoán nhận MK theo từ điển của đối phương

YÊU CẦU QUẢN LÝ MẬT KHẨU (2/4)

4. Xác định độ dài cực đại thời gian MK có tác dụng

- Hạn chế tấn công theo kiểu “vét cạn”, kể cả khi tiếp cận từ xa (chế độ off-line)

5. Xác định độ dài cực tiểu thời gian dùng MK

- Ngăn cản ý định người dùng đổi MK như cũ sau khi đến hạn đổi theo yêu cầu trên

6. Hạn chế số lượng các ý định đưa MK vào

- Hạn chế ý đồ tấn công lựa chọn tích cực của đối phương

YÊU CẦU QUẢN LÝ MẬT KHẨU (3/4)

7. Duy trì chế độ bắt buộc thay đổi MK người dùng
 - Bảo đảm hiệu quả cho đòi hỏi hạn chế độ dài cực đại tác dụng MK
8. Dùng biện pháp dùng kéo dài khi có MK sai đưa vào
 - Hạn chế phương pháp lựa chọn tích cực của đối phương
9. Nghiêm cấm việc tự người dùng chọn MK và sinh MK tự động hoá bằng thuật toán
 - Chống lại việc đoán MK theo từ điển và chống lại tấn công “vét cạn” của đối phương

YÊU CẦU QUẢN LÝ MẬT KHẨU (4/4)

10. Bắt buộc đổi MK khi lần đầu tiên ghi nhận người dùng trong HT

- Ngăn cản các hành vi trái phép của nhà quản trị HT có quyền tiếp cận hệ MK ở thời điểm bắt đầu ghi danh sách kiểm toán

11. Đưa ra sổ ghi lý lịch các MK

- Tăng cường khả năng an toàn của các MK, kèm với các đòi hỏi khác

Tiêu chí mật khẩu an toàn

- Gồm chữ thường, chữ hoa, chữ số, kí tự đặc biệt
- Đủ dài (6-8-10 ký tự trở lên)
- Không sử dụng từ có trong từ điển
- Không sử dụng mật khẩu liên quan đến thông tin cá nhân, bao gồm người thân

Quy tắc sử dụng mật khẩu an toàn

- Chọn mật khẩu đủ phức tạp
- Không ghi ra giấy, không lưu trong ứng dụng
- Thay đổi định kỳ nhưng không thường xuyên (khoảng 45 ngày)
- Không dùng 1 tài khoản trên nhiều hệ thống
- Phòng chống tấn công đánh cắp mật khẩu
- Nếu là admin:
 - Thiết lập chính sách mật khẩu
 - Định kì thử crack mật khẩu của người dùng

1

Nhân tổ xác thực

2

Mật khẩu

3

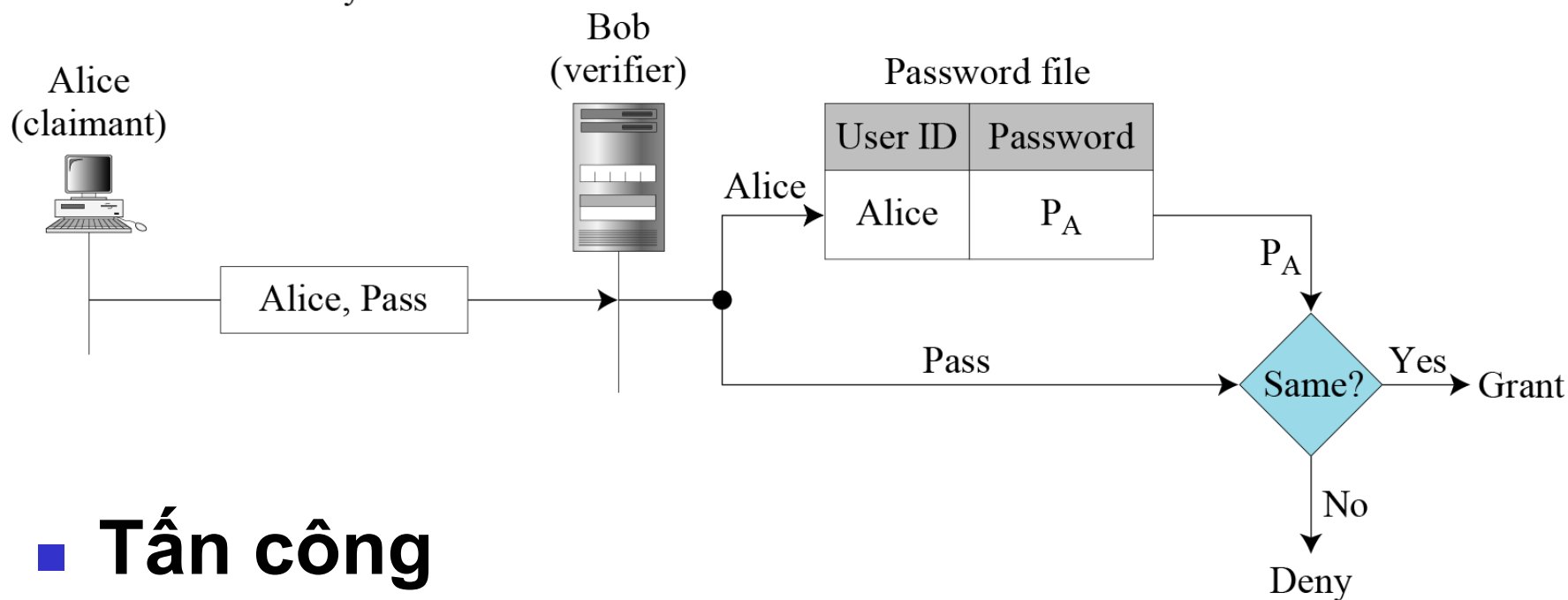
Xác thực bằng
mật khẩu

Xác thực bằng mật khẩu

1. Lưu mật khẩu dạng rõ

P_A : Alice's stored password

Pass: Password sent by claimant



■ Tấn công

■ Chặn bắt mật khẩu

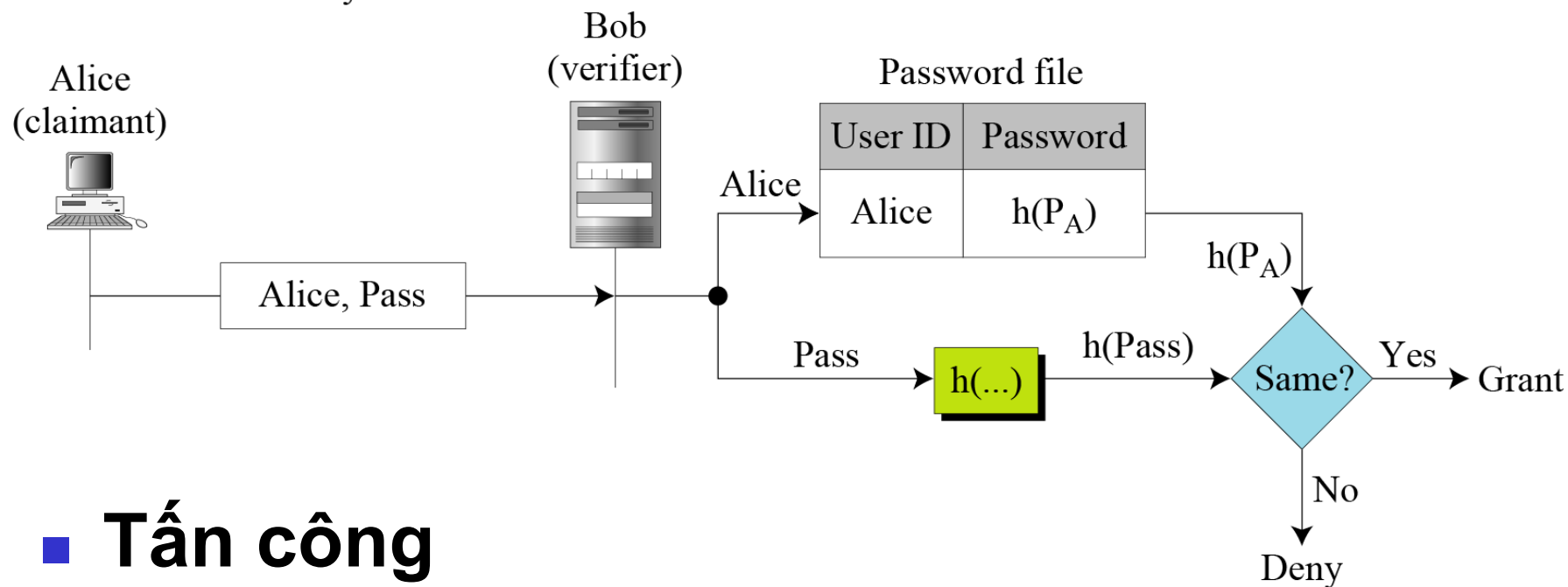
■ Chiếm file chứa mật khẩu

Xác thực bằng mật khẩu

2. Lưu mật khẩu dạng băm

P_A : Alice's stored password

Pass: Password sent by claimant



■ Tấn công

- Tấn công từ điển 1 mật khẩu
- Tấn công từ điển cả file

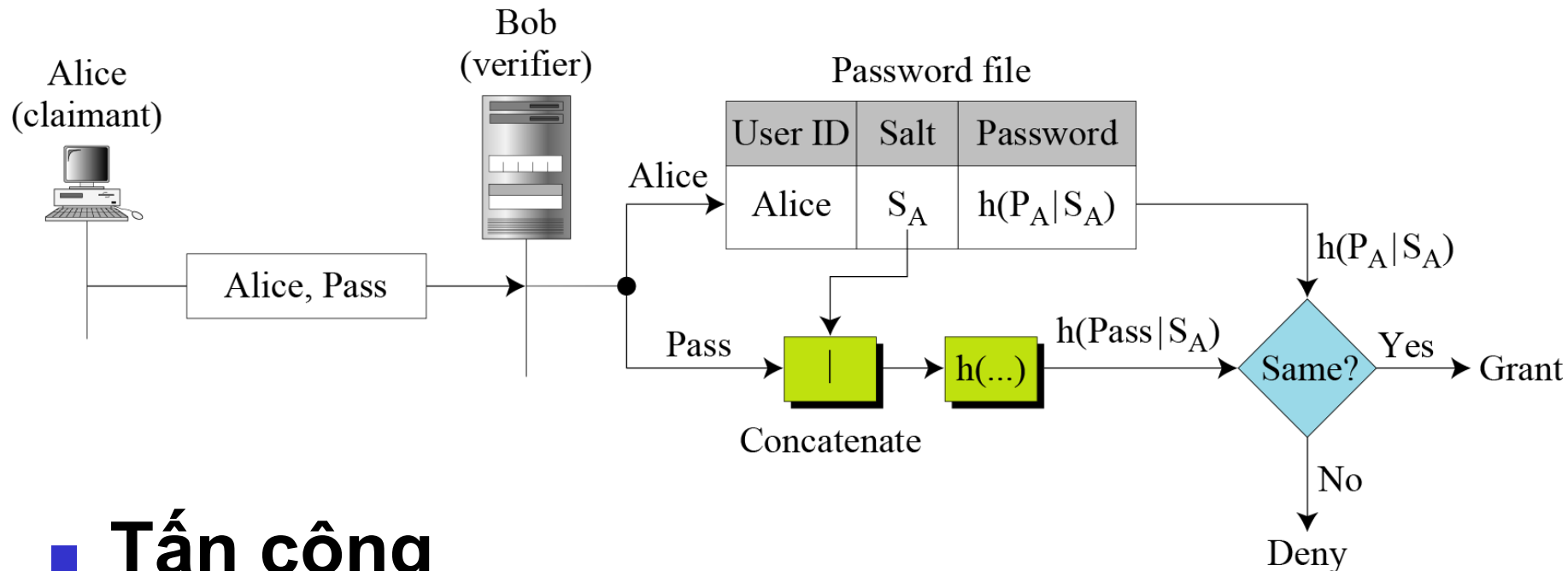
Xác thực bằng mật khẩu

3. Lưu mật khẩu dạng băm có salt

P_A : Alice's password

S_A : Alice's salt

Pass: Password sent by claimant



■ Tấn công

■ Tấn công từ điển 1 mật khẩu

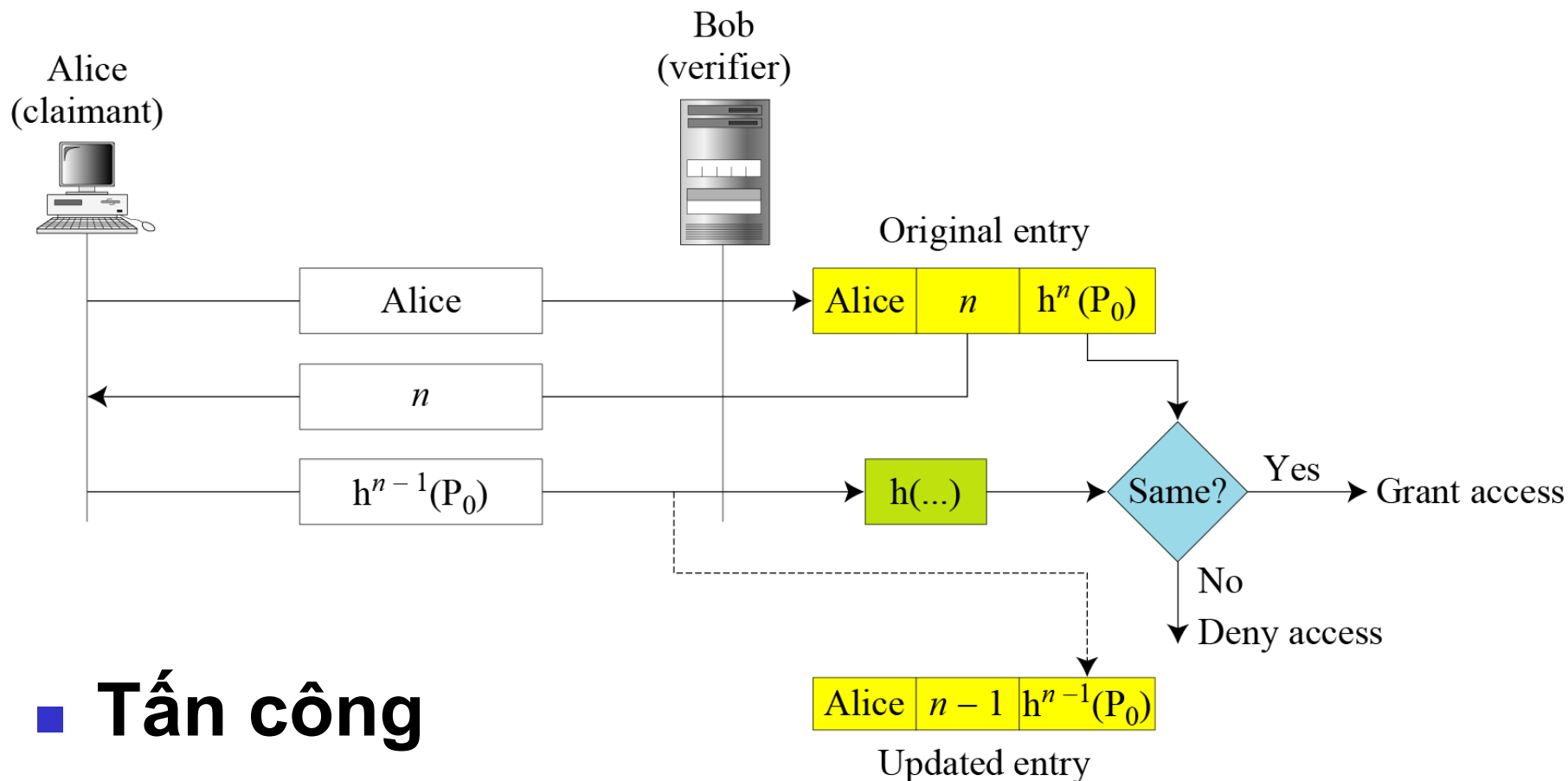
Xác thực bằng mật khẩu

❑ Nhận xét:

- claimant chứng minh bản thân bằng cách cung cấp yếu tố bí mật
- yếu tố bí mật được truyền trực tiếp qua kênh không an toàn

Xác thực bằng mật khẩu

4. Mật khẩu một lần Lamport



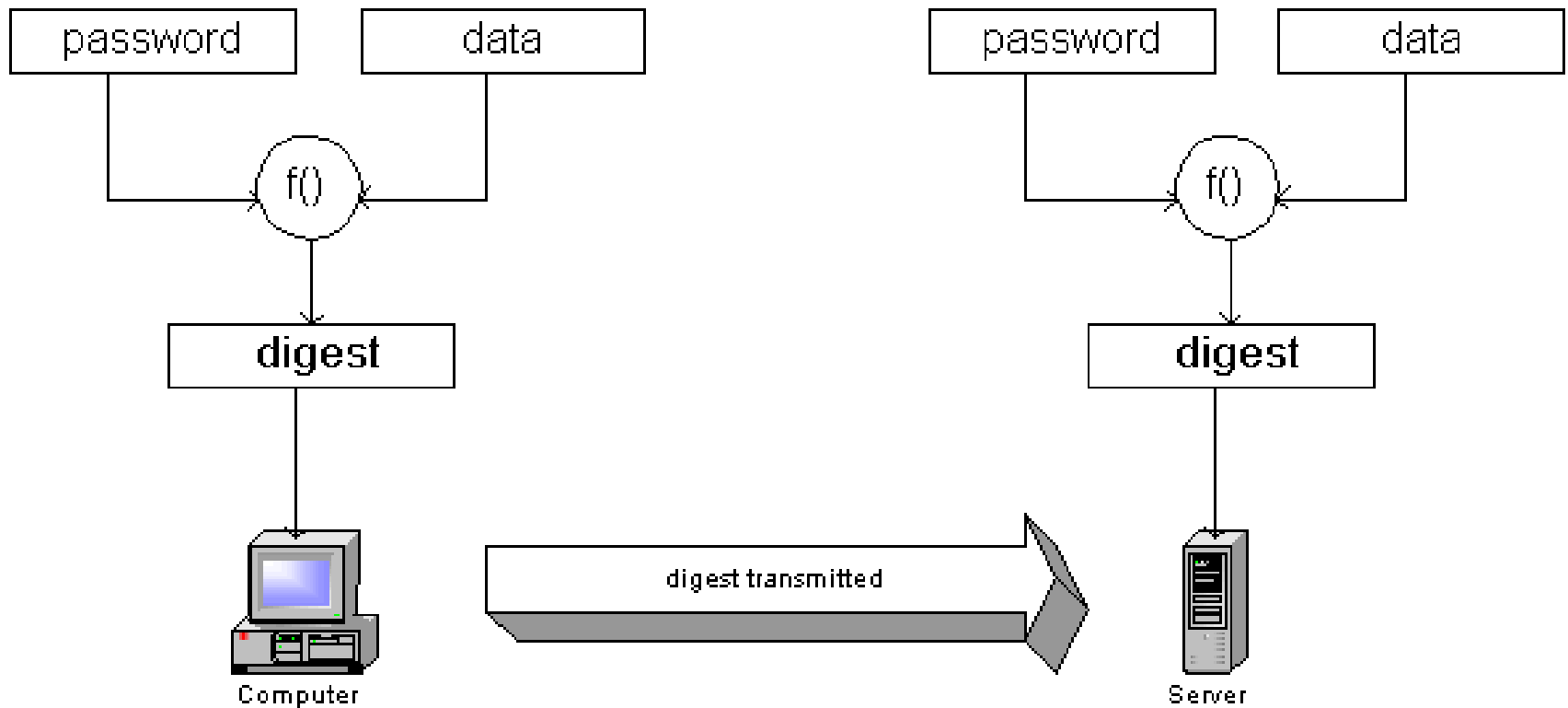
■ Tấn công

■ Man-in-the-middle

■ Tấn công từ điển!?

Xác thực bằng mật khẩu

5. Digest Authentication (RFC2617)



if digest a == digest b then
password a is same as
password b



memegenerator.net