BÀI 5.
XÁC THỰC CHỦ THỂ

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

Nội dung

- Khái niệm chung
- Xác thực dựa trên mật khẩu
- Các giao thức xác thực dựa trên mật khẩu
- Giao thức zero-knowledge
- Giới thiệu một số phương pháp xác thực khác

1. KHÁI NIỆM CHUNG

Xác thực chủ thể là gì?

- Xác thực chủ thể là tạo ra liên kết giữa định danh và đối tượng, thực thể: 2 bước
  - Chủ thể cung cấp một định danh trong hệ thống
  - Chủ thể cung cấp thông tin xác thực có thể chứng minh sự liên kết giữa định danh và chủ thể
- Các phương pháp xác thực chính:
  - Cái chủ thể biết (What the entity knows)
  - Cái chủ thể có (What the entity has)
  - Chủ thể là gì (What the entity is)
  - Vị trí của chủ thể (Where the entity is)
- Xác thực đa yếu tố: sử dụng >1 yếu tố xác thực

Các thành phần của hệ xác thực

- ***A***: Tập các thông tin đặc trưng mà chủ thể sử dụng để chứng minh định danh của anh ta
- ***C***: Tập các thông tin mà hệ thống lưu trữ và sử dụng để xác minh sự đúng đắn của thông tin trong tập ***A***
- ***F***: Tập các hàm sinh ***C*** từ ***A***

$$f \in F, f: A \to C$$

- ***L***: Tập các hàm xác thực

$$l \in L, l: A \times C \to \{true, false\}$$

- ***S***: Tập các hàm lựa chọn cho phép các thực thể tạo hoặc thay thế các thông tin trong ***A*** và ***C***

5

Một ví dụ - Hệ xác thực bằng mật khẩu

- Hệ xác thực mật khẩu, giả sử mật khẩu lưu dưới dạng rõ
  - ***A***: tập các chuỗi ký tự được chấp nhận là mật khẩu
  - ***C = A***
  - ***F***: hàm đồng nhất thức I
  - ***L:*** hàm so sánh =
  - ***S***: hàm thiết lập, thay đổi mật khẩu

6

2. HỆ XÁC THỰC BẰNG MẬT KHẨU

2. Hệ xác thực bằng mật khẩu

- Mật khẩu: một chuỗi ký tự hoặc một nhóm từ được sử dụng để xác thực chủ thể.
  - Thực thể(Entity) cần xác thực (**người dùng**, thiết bị, ứng dụng...)
  - Người thẩm tra(Verifier): kiểm tra tính hợp lệ của mật khẩu
- Một số điểm yếu trên hệ thống xác thực bằng mật khẩu:
  - Lưu trữ mật khẩu trong CSDL không an toàn
  - Truyền mật khẩu trên kênh không an toàn
  - Người dùng không cẩn trọng:
    - ✓ Sử dụng mật khẩu yếu
    - ✓ Ghi chép mật khẩu vào văn bản
    - ✓ Chia sẻ mật khẩu cho người khác (vô tình hoặc cố ý)

Lưu trữ mật khẩu

- Lưu mật khẩu dưới dạng rõ:
  - Nguy cơ mất an toàn cao nhất
- Lưu mật khẩu dưới dạng bản mã:
  - An toàn khi sử dụng hệ mật mã tốt, bảo vệ khóa giải mã an toàn
  - Hạn chế: cần thao tác giải mã bất cứ khi nào cần xác thực
- Lưu mật khẩu dưới dạng mã băm:
  - Chi phí thấp hơn
  - Hạn chế: nguy cơ bị tấn công dò đoán dựa trên từ điển. Có thể hạn chế bằng cách đưa thêm "salt" vào mật khẩu trước khi băm
- Sử dụng máy chủ lưu trữ:
  - Giải pháp 1: Người thẩm tra yêu cầu máy chủ chuyển mật khẩu để xác thực
  - Giải pháp 2: Người thẩm tra đưa cho máy chủ thông tin người dùng. Máy chủ xác thực và thông báo lại kết quả

9

Tấn công vào hệ xác thực bằng mật khẩu

- Tấn công thụ động: nghe lén, quan sát quá trình nhập mật khẩu
  - Nhìn trộm
  - Sử dụng chương trình key logging
  - Tấn công kênh bên
  - Chặn bắt gói tin
- Tấn công chủ động:
  - Giải mạo chương trình cung cấp dịch vụ (server)
  - Giả mạo chương trình khách (client)
  - Tấn công man-in-the-middle
  - Tấn công vào máy chủ vật lý cung cấp dịch vụ

10

Tấn công dạng off-line

- Kẻ tấn công biết:
  - Tập thông tin ***C*** hệ thống dùng để xác thực
  - Tập các hàm biến đổi ***F***
- Mục tiêu: tìm các thông tin $a \in A$
- Đặc điểm: không tương tác với hệ xác thực
- Ví dụ: kẻ tấn công biết có cơ sở dữ liệu chứa mã băm của mật khẩu và hàm băm sử dụng
- Nguy cơ: người dùng sử dụng các mật khẩu dễ đoán, kẻ tấn công có một bộ từ điển chưa mã băm tương ứng
- Giảm thiểu nguy cơ: Hash(Password, Salt)

11

Tấn công dạng online

- Kẻ tấn công biết tập hàm xác thực ***L***
- Mục đích: dò thử lần lượt các mật khẩu dựa trên kết quả xác thực hệ thống trả lại
- Đặc điểm:
  - Tương tác trực tiếp với hệ xác thực
  - Có thể thử trên 1 hoặc đồng thời nhiều tài khoản
- Xác suất tấn công thành công: $P \geq (T \times G)/N$
  - G: Tốc độ kẻ tấn công dò thử
  - T: Thời gian kẻ tấn công dò thử
  - N: Số mật khẩu hệ thống có thể tạo ra
- Giảm thiểu:
  - Tăng độ dài của mật khẩu
  - Quy định số lần thử xác thực tối đa trong một khoảng thời gian

12

Khôi phục mật khẩu

- Làm thế nào để người dùng có thể khôi phục mật khẩu khi họ quên?
  - Gửi trực tiếp qua email
  - Reset qua email
  - Câu hỏi bí mật
  - Sử dụng tin nhắn SMS
  - ...
- Lưu ý: xây dựng giao thức an toàn

13

Một số chính sách sử dụng mật khẩu

- Mục đích: tăng cường an toàn cho hệ xác thực dựa trên mật khẩu
- Quy định độ dài tối thiểu
- Quy định các ký tự bắt buộc phải sử dụng
- Thay đổi mật khẩu định kỳ
- Hạn chế sử dụng lại mật khẩu cũ trong một khoảng thời gian nhất định
- Hạn chế số lần thử xác thực
- Tăng thời gian chờ thử xác thực lại
- Yêu cầu đổi mật khẩu sau lần đăng nhập đầu tiên
- ...

14

3. MỘT SỐ GIAO THỨC XÁC THỰC

15

Giao thức PAP

- Password Authentication Protcol
- Được sử dụng trong giao thức mạng PPP trước đây
- Nội dung:

(1) U → S: ID || Password

(2) Server kiểm tra trong CSDL

S → U: ACK/NAK

- Không an toàn

16

Xác thực 1 chiều dựa trên hệ mật mã KĐX

- Giả sử 2 bên đã trao đổi một giá trị khóa bí mật K_S

(1) U → S: Request

(2) S → U: Challenge

(3) U → S: f(Pass, Challenge)

Hàm f: có thể là các hàm mã hóa KĐX, hàm băm

Pass : mật khẩu

- **Bài tập:** Phân tích các điểm yếu của sơ đồ này

17

Xác thực 1 chiều dựa trên hệ mật mã KCK

ISO/IEC 9798-3 / FIPS-196

(1) A → B: Request

(2) B → A: TokenID || N_B

(3) A → B: TokenID || $Cert_A$ || TokenAB

TokenID: chứa thông tin của phiên

TokenAB = N_A || N_B || $E(K_{RA}, N_A || N_B)$

18

Giao thức CHAP

- Challenge Handshake Authentication Protocol

(1) U → S: Request

(2) S → U: Challenge

(3) U → S: ID || Hash(ID || Hash(Password) || Challenge)

(4) Server kiểm tra

S → U: ACK / NAK

- Challenge: chuỗi ký tự ngẫu nhiên
- Hash: MD5

19

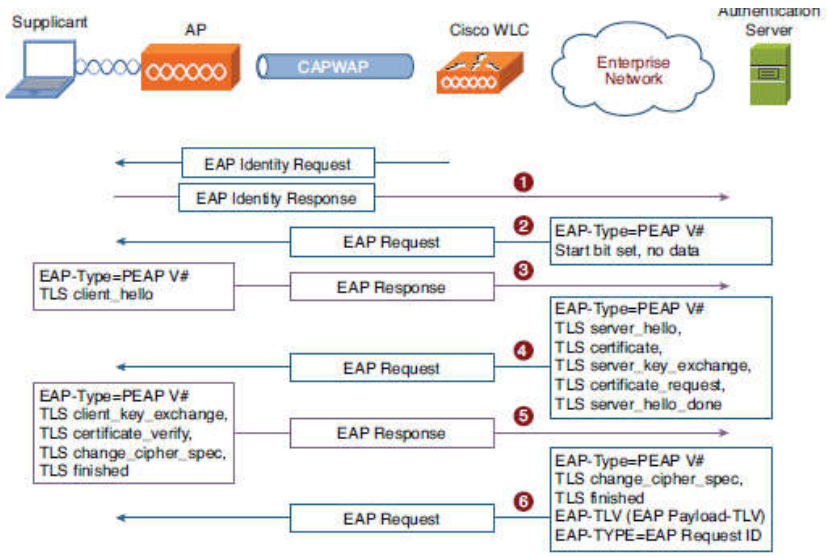
Giao thức EAP

- Extensible Authentication Protocol
- Có khoảng 40 biến thể kết hợp thêm nhiều cơ chế khác nhau:
  - EAP-MD5: tương tự CHAP
  - EAP-TLS, EAP-TTLS, PEAP: kết hợp TLS
  - EAP-POTP: kết hợp One-Time-Password
  - EAP-PSK: kết hợp pre-shared key

  ...

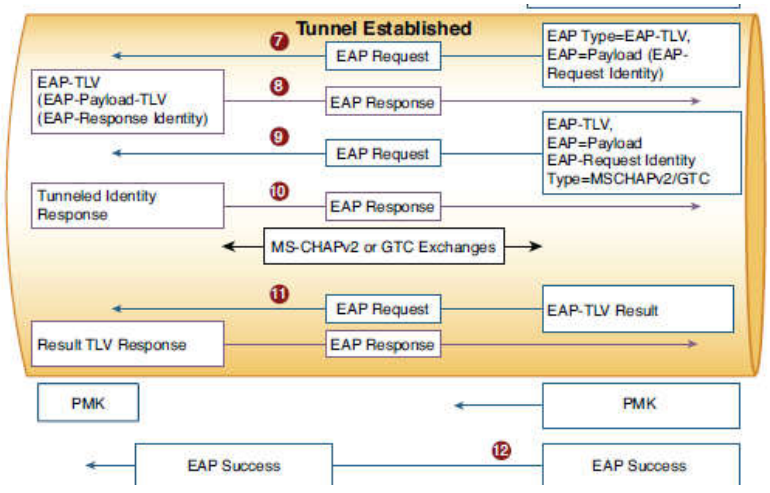
20

Ví dụ: EAP-PEAP



21

Ví dụ: EAP-PEAP



22

Xác thực 2 chiều sử dụng hệ mật mã KĐX

- Giả sử A và B đã chia sẻ khóa K_S

(1) A → B: ID_A

(2) B → A: N_B

(3) A → B: $f(K_S, N_B) \,||\, N_A$

(4) B → A: $f(K_S, N_A)$

Hàm f: có thể là các hàm mã hóa KĐX, hàm băm

K_S : khóa hoặc mật khẩu

23

Bài tập

- Xem xét tính an toàn của giao thức xác thực sau:

(1) A → B: $ID_A \,||\, N_A$

(2) B → A: $f(K_S, N_A) \,||\, N_B$

(3) A → B: $f(K_S, N_B)$

- Nhận xét: người bắt đầu giao dịch phải là người chứng minh trước

24

Xác thực 2 chiều sử dụng hệ mật mã KCK

ISO/IEC 9798-3 / FIPS-196

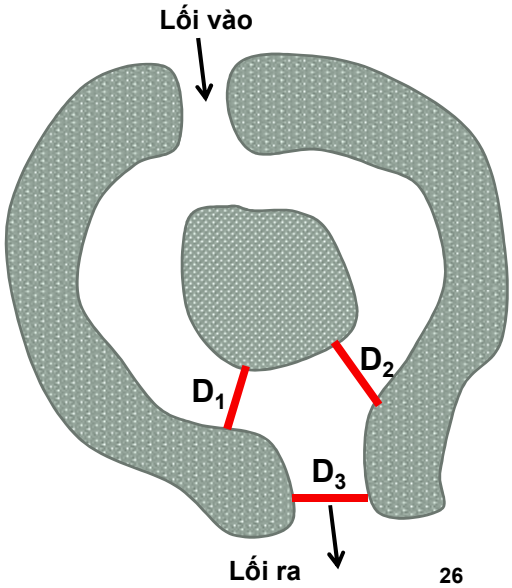
(1) A → B: Request
(2) B → A: TokenID || N_B
(3) A → B: TokenID || $Cert_A$ || TokenAB
(4) B → A: TokenID || $Cert_B$ || TokenBA

TokenAB = N_A || N_B || $E(K_{RA}, N_A || N_B)$
TokenBA = N_A || N_B || $E(K_{RB}, N_A || N_B)$

25

Giao thức dạng zero-knowledge (ZKP)

- Trong hang động có một căn phòng bí mật được khóa bởi 3 cửa D_1, D_2, D_3
- Peggy biết mật khẩu để mở các cánh cửa (VD. "Vừng ơi, mở ra!" ☺)
- Victor muốn bỏ tiền để mua lại mật khẩu
- Làm thế nào để Peggy chứng minh với Victor có thể vào căn phòng mà không làm lộ mật khẩu?



26

Giao thức ZKP

- Là các giao thức cho phép một bên chứng minh được thông tin của mình mà không làm lộ nội dung thông tin đó cho các bên còn lại (bên thứ 2 hoặc kẻ tấn công)
- Các bên tham gia giao thức:
  - Peggy-Người chứng minh: Peggy nắm được một số thông tin nào đó và muốn chứng minh cho Victor nhưng không muốn để lộ thông tin này
  - Victor-Người thẩm tra: Được quyền hỏi một số câu hỏi đến khi chắc chắn Peggy nắm thông tin. Victor không thể đoán thông tin từ câu trả lời của Peggy, hoặc do cố tình lừa Peggy tiết lộ thông tin
  - Eve-Kẻ nghe lén: Giao thức cần chống lại việc Eve nghe lén thông tin
  - Mallory: có nhiều quyền hơn Eve, có thể nghe lén, sửa đổi bản tin hoặc phát lại bản tin

27

Một ví dụ - Giao thức Feige–Fiat–Shamir

- Khởi tạo: Peggy chọn p, q là 2 số nguyên tố:
  - Tính $n = p \times q$
  - Chọn s sao cho $UCLN(s, n) = 1$, v sao cho $v = s^2 \ mod \ n$
  - Công bố (n,v). Peggy cần chứng minh cho Victor biết mình nắm giữ giá trị s
- Giao thức:

(1) P → V: $x = r^2 \ mod \ n$ r: số ngẫu nhiên

(2) V chọn ngẫu nhiên $b \in \{0, 1\}$

V → P: b

(3) P → V: $y = r \times s^b \ mod \ n$

(4) V kiểm tra phương trình đồng dư $y^2 \equiv x \times v^b \ (mod \ n)$

Hoặc viết dưới dạng khác $y^2 \ mod \ n = x \ \times \ v^b \ mod \ n$

28

Giả mạo

- Mallory có thể giả mạo bằng 2 cách:

(1) Bắt các cặp giá trị *(x, y)* và phát lại

(2) Phán đoán giá trị của bit *b* mà Victor thử thách:

  - Đoán b = 0, Mallory gửi $x = r^2 \ mod \ n$ và $y = r \ mod \ n$
  - Đoán b = 1, Mallory chọn *y* trước và tính *x* sao cho

$$y^2 \equiv x \times v \ (mod \ n)$$

- Xác suất thành công của Mallory là bao nhiêu?
- Làm thế nào để giảm xác suất thành công của Mallory trong 1 vòng kiểm tra?

29

Nhận xét

- Vì Peggy nắm được giá trị của s nên có thể qua được vô số vòng kiểm tra (Tính đầy đủ - Completeness)
- Nếu Mallory không biết s, thì xác suất giả mạo thành công lớn nhất là 2^{-n} với n là số vòng kiểm tra (Tính vững chãi-Soundness)
- Mallory không thể sử dụng lại bộ số *(x,y)* để lừa Victor
- Victor không biết gì về s vì bài toán tính căn bậc 2 rời rạc là khó
- Tương tự, Eve nghe trộm được mọi bộ số *(x,y,b)* cũng không thể đoán được s

30

Các nguy cơ

- Peggy không thay đổi r sau mỗi vòng kiểm tra
- Chess Grandmaster Problem
- Mafia Problem
- Terrorist Problem

31

Giao thức ZKP dựa trên hệ mật mã RSA (Một ví dụ khác)

- Peggy có khóa công khai K_U = (e,n) cần chứng minh anh ta có bí mật m
- Khởi tạo: Peggy tính $c = m^e \bmod n$
- Giao thức:

(1) P → V: $x = r^e \bmod n$ r: số ngẫu nhiên

(2) V chọn ngẫu nhiên $b \in \{0, 1\}$

V → P: b

(3) P → V: $y = r \times m^b \bmod n$

(4) V kiểm tra phương trình đồng dư $y^e \equiv x \times c^b \pmod n$

Tự kiểm tra tính đầy đủ và bền vững của giao thức.

Hãy đọc thêm lý thuyết tổng quan về ZKP trong tài liệu.

32

4. ONE TIME PASSWORD (OTP)

Xác thực đa yếu tố

- Phương pháp xác thực sử dụng mật khẩu không đủ an toàn (Nguyên nhân chủ yếu từ người dùng!)
- Sử dụng mật khẩu một cách an toàn:
  - Đủ dài và khó đoán
  - Không dùng chung cho nhiều tài khoản
  - Thay đổi thường xuyên
  - … → hầu hết người dùng không thực hiện được

→cần thêm các yếu tố xác thực an toàn hơn, không phụ thuộc vào thói quen của người dùng

- Xác thực đa yếu tố (thông thường là 2 yếu tố)
  - Cái người dùng biết: mật khẩu
  - Cái người dùng có: (thường) thiết bị phần cứng

One Time Password

- Mật khẩu chỉ dùng để xác thực cho 1 phiên hoặc 1 giao dịch
- Phân loại:
  - S/Key OTP
  - Hash-based OTP (HOTP)
  - Time-based OTP (TOTP)

  } Event-based OTP
- Cách thức phân phối:
  - SMS
  - Ứng dụng
  - Email
  - Token

35

SMS OTP

- Giá trị OTP được sinh ở server và gửi cho người dùng qua tin nhắn SMS
- Không đảm bảo an toàn:
  - Điện thoại người dùng bị nghe lén
  - Giả mạo trạm BTS
  - Tấn công lợi dụng lỗ hổng của giao thức SS7

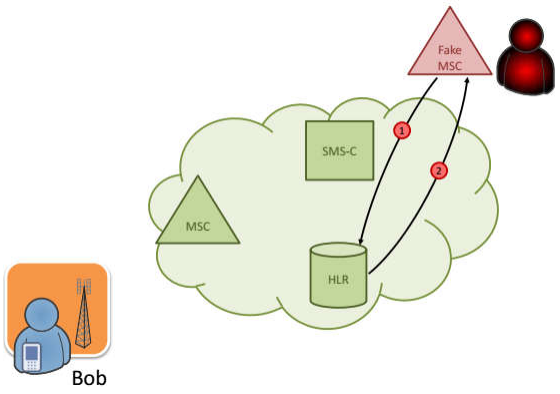
36

Tấn công lợi dụng lỗ hổng của SS7

- SS7(Signaling System 7): bộ giao thức điều khiển truyền dữ liệu giữa các cell trong mạng đi động
- Không có cơ chế xác thực
- IMSI: Định danh của thẻ SIM
- IMEI: Định danh của thiết bị
- MSISDN: Số thuê bao
- HLR(Home Location Register): CSDL thuê bao
- MSC(Mobile Switching Center): Bộ chuyển mạch
- MAP(Mobile Application Part): giao thức điều phối truyền dữ liệu giữa các thành phần trong phiên dịch vụ

37

Tấn công SS7 – Bước 1



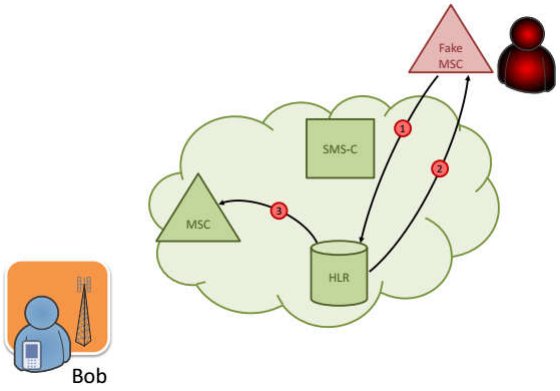
(1) Kẻ tấn công gửi thông điệp SendRoutingInfoForSM chứa MSISDN tới HLR

(2) HLR gửi thông điệp trả lời chứa:

- Số thuê bao
- Địa chỉ của MSC đang xử lý kết nối của nạn nhân(Bob)
- IMSI của nạn nhân

38

Tấn công SS7 – Bước 2



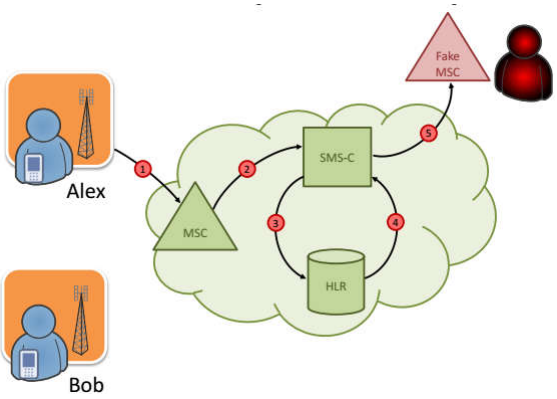
(1) Kẻ tấn công đăng ký thông tin của Bob trên MSC giả mạo (Fake MSC)

(2) HLR cập nhật vị trí mới của Bob

(3) HLR yêu cầu MSC cũ giải phóng thông tin

39

Tấn công SS7 – Bước 3



(1) Alex gửi tin nhắn SMS cho Bob

(2) MSC chuyển tiếp tin nhắn tới SMS-C

(3)SMS-C gửi thông điệp tới HLR yêu cầu vị trí của Bob

(4) HLR trả lại địa chỉ của Fake MSC

(5) SMS-C chuyển tiếp tin nhắn tới Fake MSC

40

Một vụ việc tấn công xác thực người dùng

Một vụ việc tấn công xác thực người dùng

Kịch bản sử dụng dịch vụ:

- B1: Khách hàng đăng nhập vào hệ thống eBanking
- B2: Khách hàng nhập lệnh chuyển tiền
- B3: Hệ thống eBanking gửi mã OTP qua tin nhắn SMS tới số điện thoại mà khách hàng đã đăng ký
- B4: Khách hàng nhập mã OTP nhận được vào hệ thống để xác nhận chuyển tiền

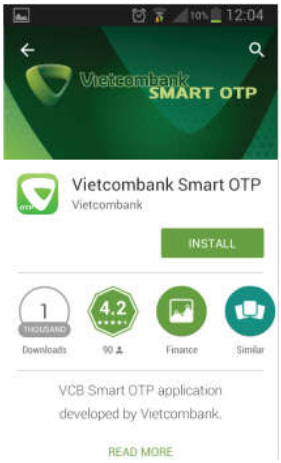
→Xác thực đa yếu tố:

(1) Mật khẩu truyền thống

(2) SMS OTP

Một vụ việc tấn công xác thực người dùng

- Vietcombank cung cấp ứng dụng di động Vietcombank Smart OTP cung cấp mã xác thực OTP
- B1: Mở ứng dụng và điền số ĐT đăng ký SMS Banking
- B2: Hệ thống gửi mã xác thực OTP tới số điện thoại
- B3: Người dùng nhập mã xác thực vào ứng dụng
- B4: Nếu mã OTP đúng, ứng dụng được kích hoạt



43

Thảo luận

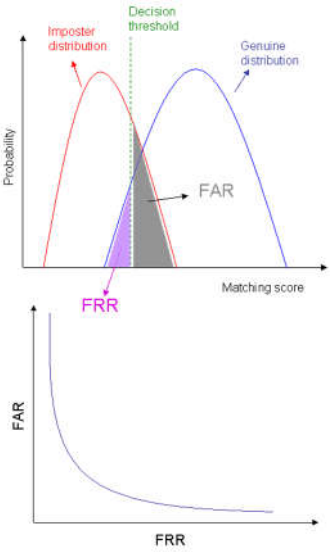
- Kịch bản tấn công có thể có là gì?

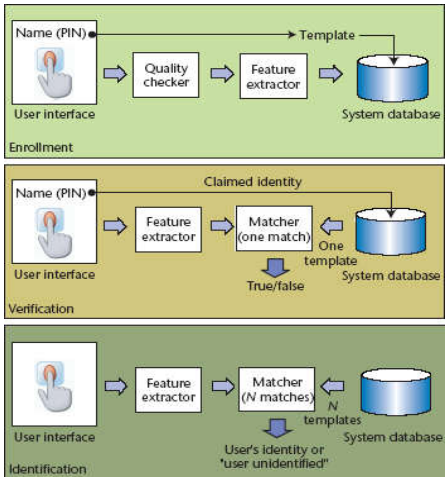
44

4. XÁC THỰC SỬ DỤNG SINH TRẮC

45

Xác thực bằng sinh trắc (biometric)



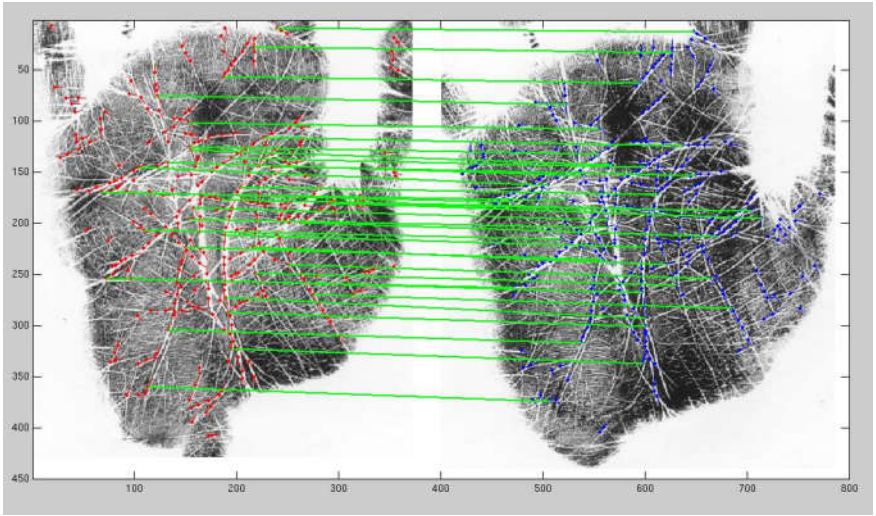


46

Dấu vân tay

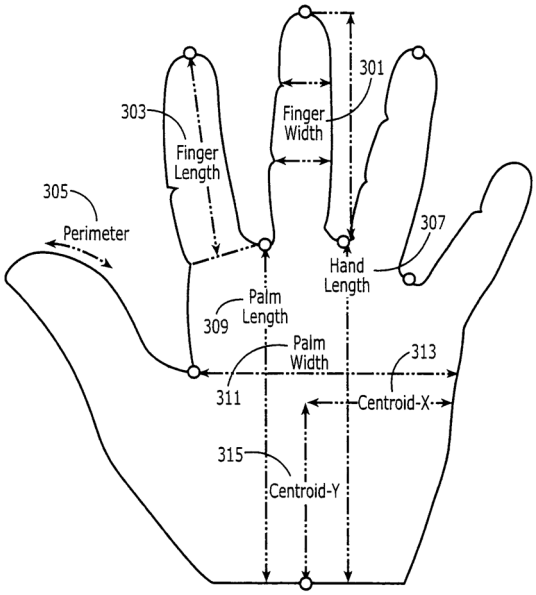
47

Vân lòng bàn tay



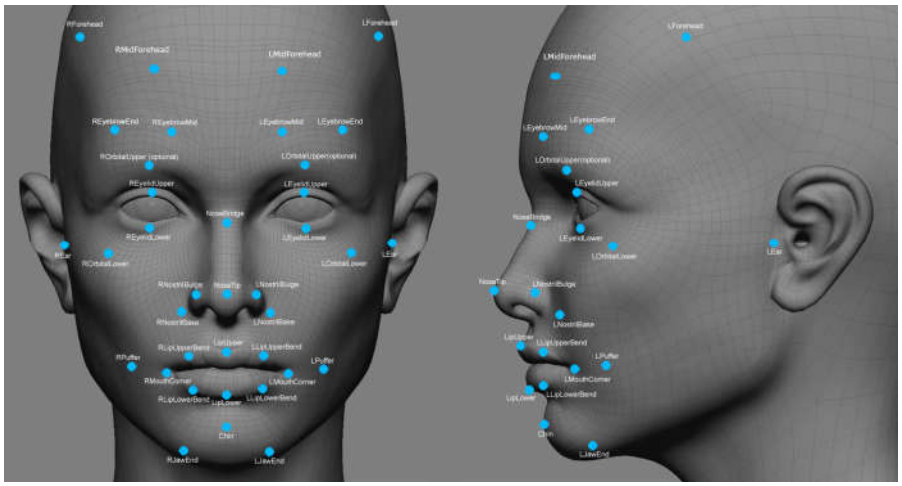
48

Cấu trúc bàn tay



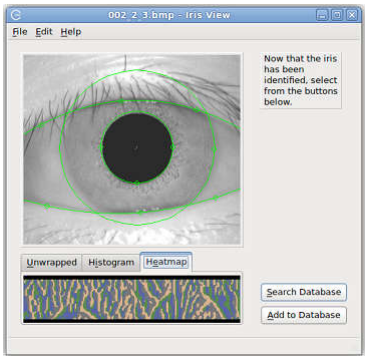
49

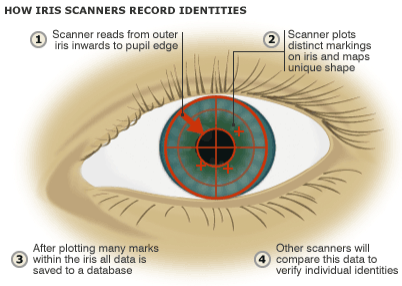
Khuôn mặt



50

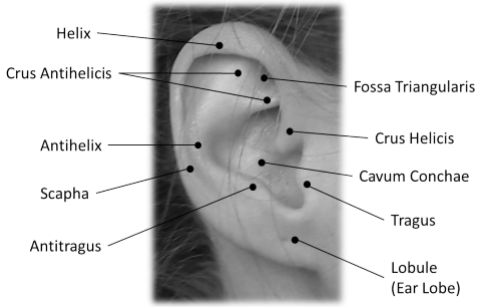
Mống mắt

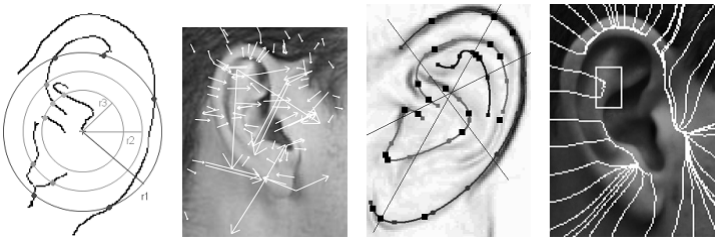




51

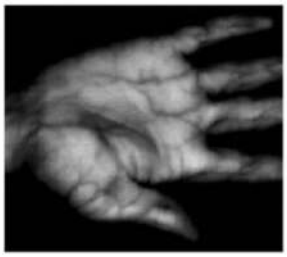
Vành tai

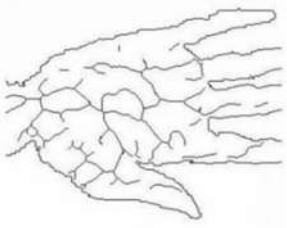




52

Mạch máu





53

Xác thực bằng sinh trắc

54

Những khó khăn khi sử dụng hệ xác thực bằng sinh trắc

- Chi phí tính toán
- Giá thành cao
- Tính không ổn định
- Không bền vững
- Lo ngại của người dùng liên quan đến sức khỏe

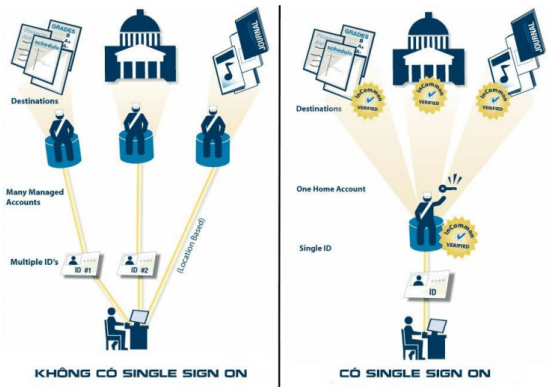
55

5. SINGLE SIGN ON(SSO)

56

Khái niệm

- SSO là một cơ chế xác thực yêu cầu người dùng đăng nhập vào chỉ một lần với một tài khoản và mật khẩu để truy cập vào nhiều ứng dụng trong 1 phiên làm việc (session).



57

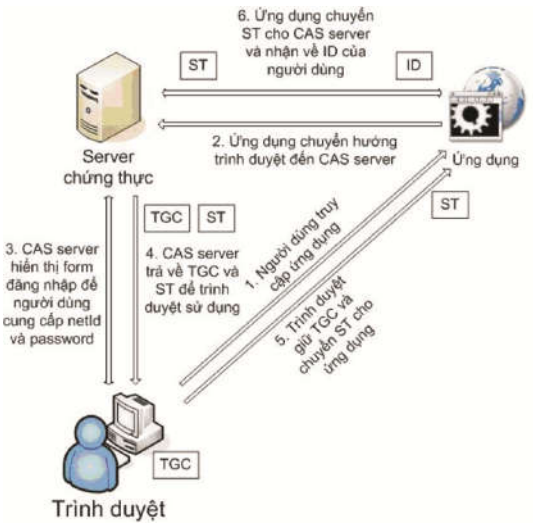
Single Sign On

- CAS (Central Authentication Service) là một giải pháp SSO mã nguồn mở được phát triển bởi đại học Yale
- CAS hỗ trợ nhiều thư viện phía máy khách được viết bởi nhiều ngôn ngữ: PHP, Java, PL/SQL
- Các thông tin phiên đăng nhập đặt trong cookie do CAS sinh ra(Ticket Granting Cookie)
- Hỗ trợ xác thực đa yếu tố

58

Single Sign On

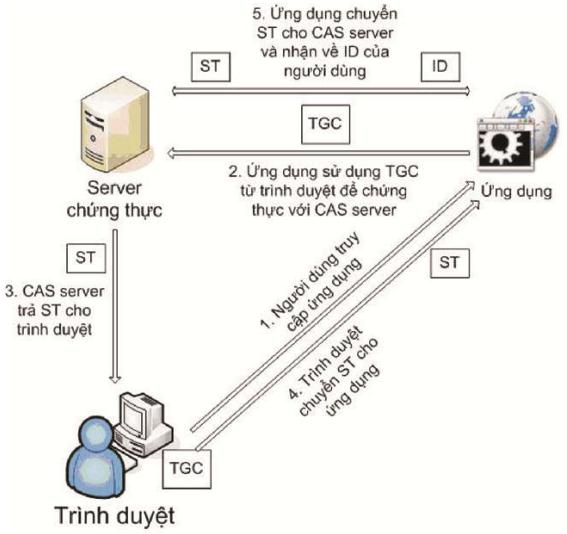
- Người dùng chưa được chứng thực trên CAS
- TGC: Ticket Granting Cookie
- ST: Session Token



59

Single Sign On

- Người dùng đã chứng thực trên CAS



60

Các giải pháp SSO khác

- Open SAML
- OpenID Connect
- CA Single Sign On
- Java Open Single Sign On
- Google Sign-In
- Facebook Login

61