Chương 3:
Định danh và Xác thực
(Identification and Authentication)

Khoa Khoa học và Kỹ thuật Máy tính
Đại học Bách Khoa Tp.HCM

Nội dung

1. Giới thiệu về định danh và xác thực
2. Phương pháp định danh
3. Phương pháp xác thực
4. Giao thức xác thực

Giới thiệu về định danh và xác thực

- Các bước trong điều khiển truy cập

Định danh (Identification):
Người dùng cung cấp danh định (identity)

Xác thực (Authentication):
Người dùng chứng minh danh định đó là đúng

Ủy quyền (Authorization):
Xác định quyền mà người dùng có

Giới thiệu về định danh và xác thực

- Các bước trong điều khiển truy cập

Định danh (Identification):

Người dùng cung cấp danh định (identity)

Xác thực (Authentication):

Người dùng chứng minh danh định đó là đúng

Ủy quyền (Authorization):

Xác định quyền mà người dùng có

Định danh

- Người dùng cung cấp danh định của mình cho hệ thống
- Mục đích:
  - Tìm kiếm **sự tồn tại** và **quyền hạn** cho người dùng

Xác thực

- Người dùng cung cấp bằng chứng là danh định đó là đúng và phù hợp với mình.
- Mục đích:
  - Chứng minh danh định là **hợp lệ** và **phù hợp** với người dùng.
  - Quyết định có cho phép người dùng truy cập vào tài nguyên của hệ thống hay không

Nội dung

1. Giới thiệu về định danh và xác thực
2. Phương pháp định danh
3. Điều khiển dữ liệu với SQL
4. DAC và điều khiển dòng thông tin

Phương pháp định danh

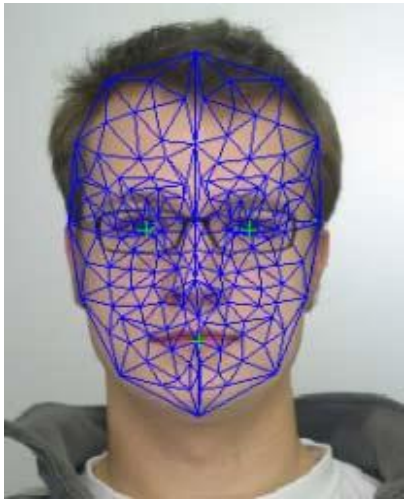
- Có 2 phương pháp:
  - người dùng tự nhập thông tin về danh định
  - Sử dụng danh định số hóa:
    - Danh định sinh trắc học (biometric identity)
    - Danh định máy tính (computer identity)
    - Danh định số (digital identity)

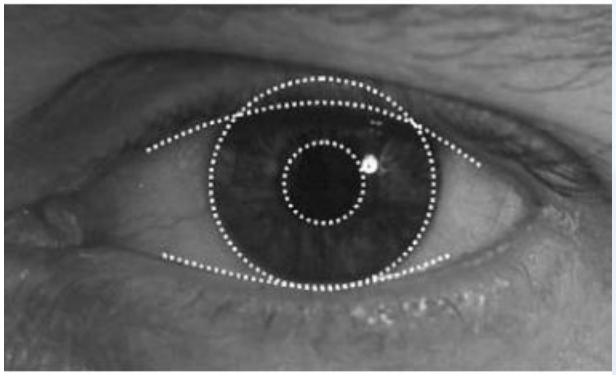
Phương pháp định danh

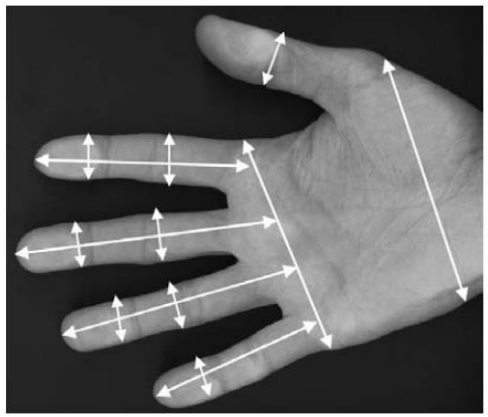
- **Phương pháp 1: người dùng tự nhập thông tin về danh định**
- Đây là phương pháp phổ biến nhất hiện nay
  - Ví dụ: username, số tài khoản
- Bước đầu tiên khi một hacker muốn xâm nhập vào một hệ thống là thu thập danh sách các người dùng hợp lệ của hệ thống.

Phương pháp định danh

- **Phương pháp 2: Sử dụng danh định số hóa**
- Danh định sinh trắc học (Biometric identity)
  - Nhận dạng khuôn mặt (Facial recognition)
  - Quét tròng mắt (iris scanners)
  - Hình học bàn tay (hand geometry)
  - Nhận dạng vân tay (fingerprint)







Phương pháp định danh

- **Phương pháp 2: Sử dụng danh định số hóa**
- Danh định máy tính (Computer identity)
  - Tên máy tính
  - Địa chỉ MAC
  - Địa chỉ IP

Phương pháp định danh

- **Phương pháp 2: Sử dụng danh định số hóa**
- Danh định số (Digital identity)
  - Chứng nhận số (Digital certificate)
  - Thẻ thông minh (Smart card)

Nội dung

1. Giới thiệu về định danh và xác thực
2. Phương pháp định danh
3. Phương pháp xác thực
4. Giao thức xác thực

Phương pháp xác thực

- Các phương pháp xác thực:
  - **Những gì bạn biết (Something you know)**
  - **Những gì bạn có (Something you have)**
  - **Những gì là chính bạn (Something you are)**
- Một phương pháp xác thực tốt là phương pháp mà không dễ bị đoán hoặc bị làm giả.

Những gì bạn biết

- Ví dụ:
  - Password
  - Số PIN (Personal Identification Number)
- Ưu điểm
  - Tiện lợi
  - Chi phí thấp
- Khuyết điểm
  - Mức độ bảo mật phụ thuộc vào độ phức tạp của password

Những gì bạn biết

- Những vấn đề của password:
  - Password yếu: dễ đoán (tên người dùng, ngày sinh nhật ,…)

    → Xây dựng chính sách password:
    - Độ dài
    - Có các ký tự đặc biệt (non-letter), có ký viết hoa, viết thường
    - Khác với username, các từ dễ đoán
    - Thay đổi password định kỳ

    Cần cân bằng giữa: hacker khó đoán và người dùng có thể nhớ
  - Thu thập thông tin bất hợp pháp (Social engineering)
  - Các phần mềm gián điệp (spyware), keystroke logging

Những gì bạn có

- Thẻ thông minh (smart card): có bộ nhớ nhỏ và có khả năng thực hiện một vài tính toán
- Trong thẻ có lưu thông tin về người dùng và cả password.
  - người dùng có thể chọn những password phức tạp và thay đổi khi cần
- Địa chỉ MAC, địa chỉ IP

Những gì là chính bạn

- Sử dụng các yếu tố sinh trắc học để xác thực.
  - Nhận dạng khuôn mặt
  - Quét tròng mắt
  - Hình học bàn tay
  - Nhận dạng vân tay
- Xác thực bằng sinh trắc học gồm 2 bước
  - Đăng ký mẫu
  - Nhận dạng

Những gì là chính bạn

- Các lỗi xảy ra khi xác thực bằng sinh trắc học
  - Fraud rate
  - False accept rate

Những gì là chính bạn

- Các lỗi xảy ra khi xác thực bằng sinh trắc học
  - Insult rate
  - False reject rate

Những gì là chính bạn

- Tỷ lệ lỗi sinh trắc học
  - Fraud rate = Insult rate
  - Vân tay (5%)
  - Hình học bàn tay (0.1%)
  - Tròng mắt (0.001%)
- Ưu điểm:
  - Khó tấn công
- Khuyết điểm:
  - Tốn kém: lưu trữ, xử lý

Phương pháp xác thực

- Phương pháp xác thực tốt thì tốn kém
- Xét về khả năng bị tấn công:
  - Biometrics < Smartcard < Password
- Xét về chi phí:
  - Password < Smartcard < Biometrics
- Có thể kế hợp các phương pháp xác thực với nhau

Nội dung

1. Giới thiệu về định danh và xác thực
2. Phương pháp định danh
3. Phương pháp xác thực
4. Giao thức xác thực

Giao thức xác thực

- Giao thức xác thực đơn giản
- Giao thức xác thực challenge-response
- Giao thức xác thực dùng khóa đối xứng
- Giao thức xác thực dùng khóa công khai
- Giao thức xác thực KERBEROS

Giới thiệu

- Giả sử là **Alice** muốn chứng minh với **Bob** là "Tôi chính là Alice"
- Alice cũng cần biết người còn lại có đúng là Bob không.
- **Malice** là người xấu có ý muốn phá giao thức xác thực

Giao thức xác thực đơn giản

Giao thức xác thực đơn giản

- Password để ở dạng văn bản rõ, Malice có thể quan sát được.

Giao thức xác thực đơn giản với hàm hash

- P_A: password của Alice
- h(): hàm hash

Giao thức xác thực đơn giản với hàm hash

- Tấn công bằng cách lặp lại thông điệp

Giao thức xác thực

- Giao thức xác thực đơn giản
- **Giao thức xác thực challenge-response**
- Giao thức xác thực dùng khóa đối xứng
- Giao thức xác thực dùng khóa công khai
- Giao thức xác thực KERBEROS

Giao thức xác thực challenge-response

- N: số nonce (number used once)

- Khuyết điểm: Bob phải biết trước password của Alice

Giao thức xác thực

- Giao thức xác thực đơn giản
- Giao thức xác thực challenge-response
- **Giao thức xác thực dùng khóa đối xứng**
- Giao thức xác thực dùng khóa công khai
- Giao thức xác thực KERBEROS

Giao thức xác thực dùng khóa đối xứng

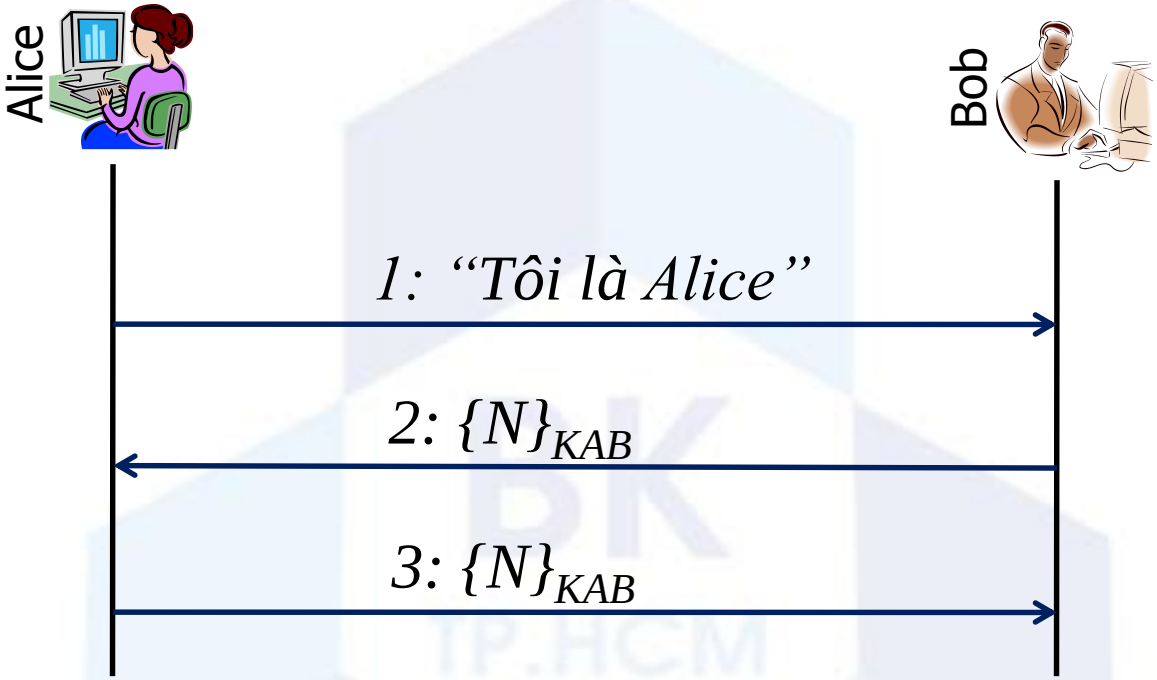
- C: ciphertext
- M: plaintext
- K_A: khóa của Alice
- $C = \{M\}_K$
- K_{AB} : Khoá chung giữa Alice và Bob

Giao thức xác thực dùng khóa đối xứng

- Khuyết điểm:
  - Chỉ có Bob xác thực được Alice
  - Alice không biết có đúng là Bob không

Giao thức xác thực dùng khóa đối xứng

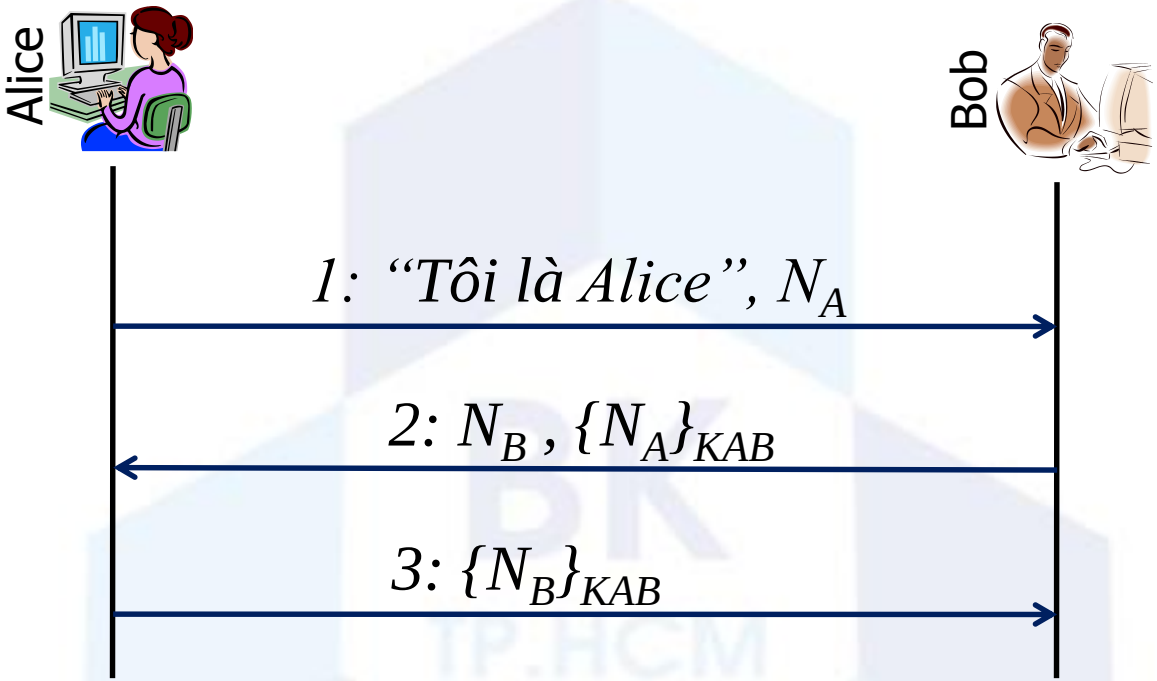
- Giao thức xác thực lẫn nhau (mutual) dùng khóa đối xứng



→Thông điệp ở bước 3 lặp lại từ bước 2: không thể xác thực người gửi

Giao thức xác thực dùng khóa đối xứng

- Giao thức xác thực lẫn nhau cải tiến

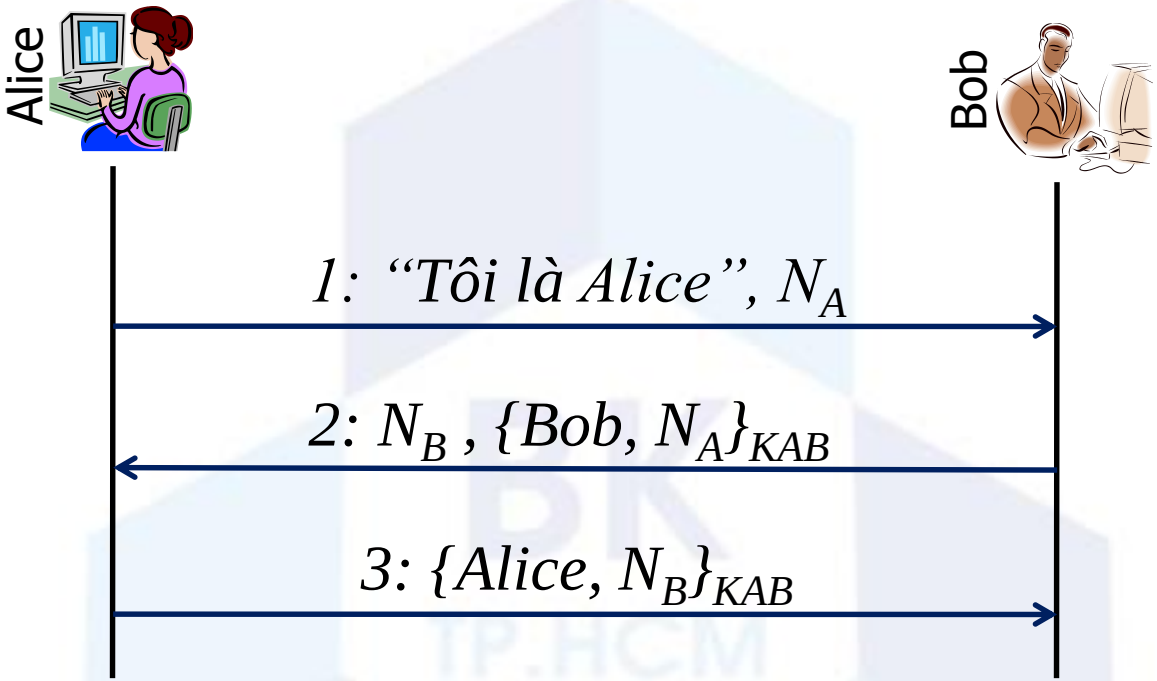


Giao thức xác thực dùng khóa đối xứng

- Tấn công giao thức xác thực lẫn nhau cải tiến

Giao thức xác thực dùng khóa đối xứng

- Giao thức xác thực lẫn nhau cải tiến khác



Giao thức xác thực

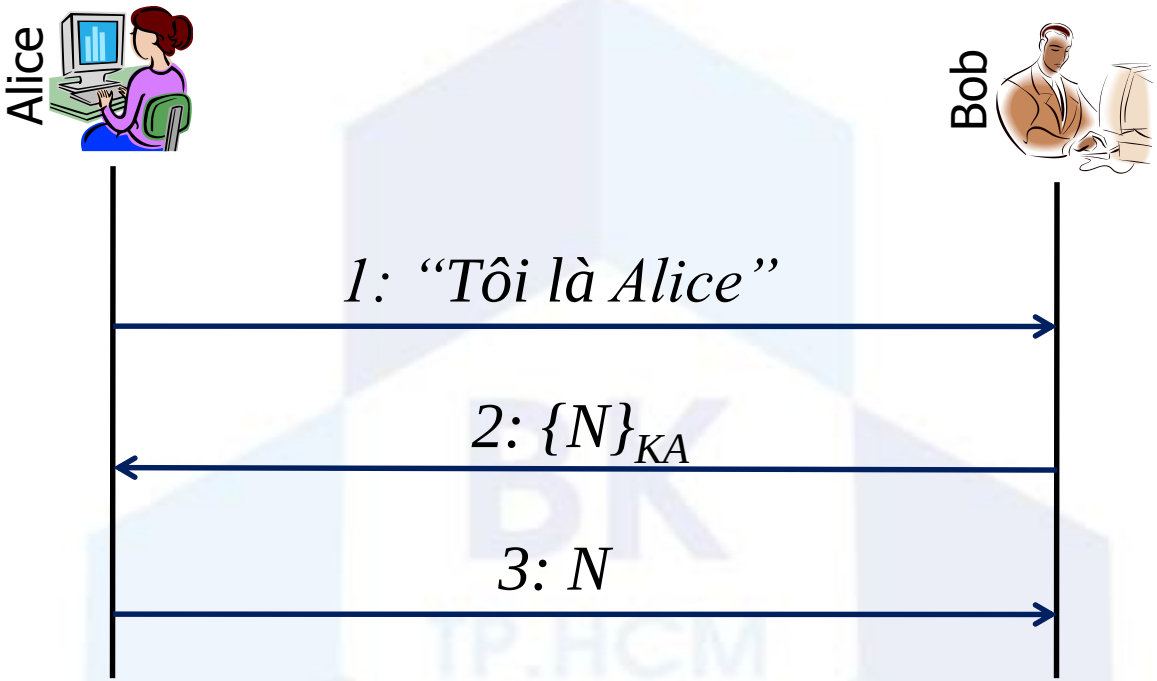
- Giao thức xác thực đơn giản
- Giao thức xác thực challenge-response
- Giao thức xác thực dùng khóa đối xứng
- **Giao thức xác thực dùng khóa công khai**
- Giao thức xác thực KERBEROS

Giao thức xác thực dùng khóa công khai

- C: ciphertext
- M: plaintext
- K_A: cặp khóa bí mật và công khai của Alice
- $C = \{M\}_{KA}$: mã hóa bằng khóa công khai của Alice
- $M = [C]_{KA}$: giải mã bằng khóa bí mật của Alice
- $S = [M]_{KA}$: ký lên M bằng khóa bí mật của Alice
- $[\{M\}_{KA}]_{KA} = M$
- $\{[M]_{KA}\}_{KA} = M$

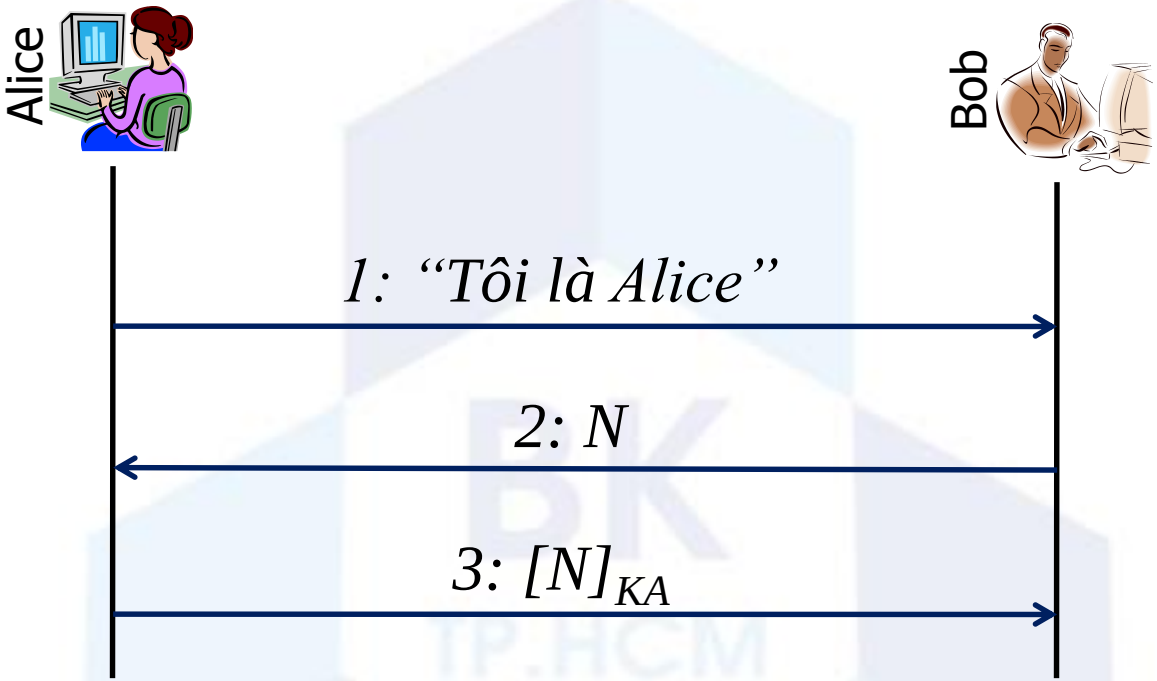
Giao thức xác thực dùng khóa công khai

- Dùng mã hóa công khai



Giao thức xác thực dùng khóa công khai

- Dùng chữ ký số



Giao thức xác thực

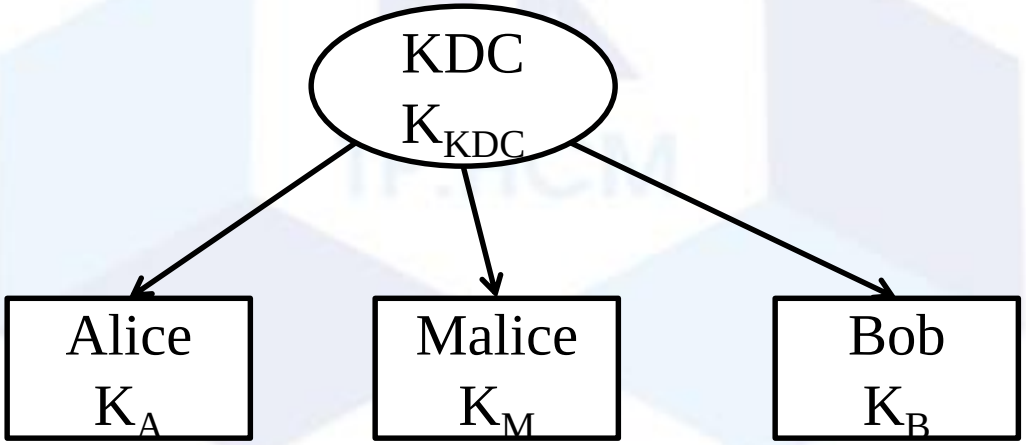
- Giao thức xác thực đơn giản
- Giao thức xác thực challenge-response
- Giao thức xác thực dùng khóa đối xứng
- Giao thức xác thực dùng khóa công khai
- **Giao thức xác thực KERBEROS**

Giao thức xác thực KERBEROS

- Là giao thức được sử dụng trong thực tế
- KERBEROS
  - Dùng mã hóa đối xứng
  - Được thiết kế để dùng trong những hệ thống nhỏ như là mạng nội bộ
  - Dựa vào thành phần thứ 3 tin cậy là Trung tâm phân phối khóa (Key Distribution Center - KDC)
- Với N người dùng
  - Giao thức dùng khóa công khai: 2N khóa
  - Giao thức dùng khóa đối xứng: N^2 khóa
  - Giao thức Kerberos: N khóa

Giao thức xác thực KERBEROS

- Trung tâm phân phối khóa KDC
  - KDC có một siêu khóa K_{KDC}, chỉ có KDC mới biết khóa này
  - KDC cung cấp: Ticket-Granting Ticket (TGT)
  - TGT chứa khóa phiên, user ID và thời hạn
  - TGT được mã hóa bằng K_{KDC}
  - Chỉ có KDC mới đọc được TGT

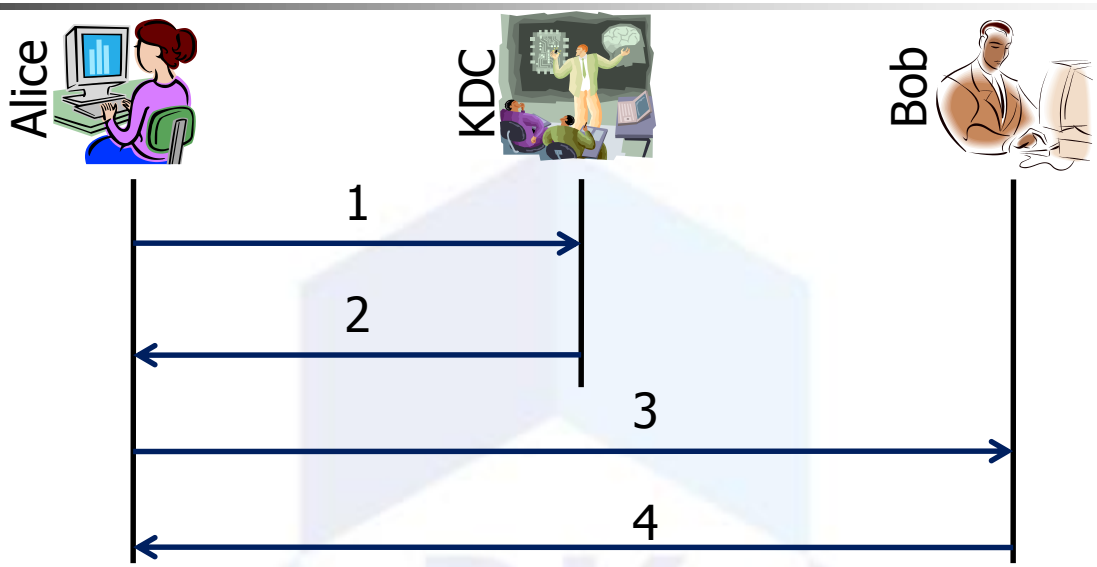


Giao thức xác thực KERBEROS

- Quá trình Alice login vào hệ thống sử dụng KERBEROS

- K_A: khóa chung giữa Alice và KDC, $K_A = h(password)$
- S_A: khóa phiên
- $TGT_A = \{Alice, S_A\}_{KKDC}$

Giao thức xác thực KERBEROS



1. Alice gửi cho KDC: *Alice, Bob,* TGT_A, $\{timestamp\}_{SA}$
2. KDC gửi cho Alice: $\{Bob, K_{AB}, ticket\text{-}to\text{-}Bob\}_{SA}$

   ticket-to-Bob: $\{Alice, K_{AB}\}_{KB}$
3. Alice gửi cho Bob: *ticket-to-Bob,* $\{timestamp\}_{KAB}$
4. Bob gửi cho Alice: $\{timestamp + 1\}_{KAB}$

Giao thức xác thực KERBEROS

- Một thao tác dư thừa trong KERBEROS:
  - KDC gửi cho Alice: $\{S_A, TGT_A\}_{KA}$

    Trong khi $TGT_A = \{Alice, S_A\}_{KKDC}$

    → KDC gửi cho Alice: $\{S_A\}_{KA}, TGT_A$

    → *Tiết kiệm chi phí*
- KDC dùng K_{KDC} để giải mã tất cả các TGT

  → không cần biết ai gửi yêu cầu

Nội dung

1. Giới thiệu về định danh và xác thực
2. Phương pháp định danh
3. Phương pháp xác thực
4. Giao thức xác thực


Question ?