**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐH CÔNG THƯƠNG TP HỒ CHÍ MINH**

**KHOA: CÔNG NGHỆ THÔNG TIN**

**ĐỒ ÁN CHUYÊN NGÀNH**

**ĐỀ TÀI: TÌM HIỂU VỀ CƠ CHẾ XÁC THỰC ĐĂNG NHẬP, TRIỄN KHAI HỆ THỐNG MINH HỌA**

*Thành Phố Hồ Chí Minh, tháng 12 năm 2024*

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐH CÔNG THƯƠNG TP HỒ CHÍ MINH**

**KHOA: CÔNG NGHỆ THÔNG TIN**

**ĐỒ ÁN CHUYÊN NGÀNH**

**ĐỀ TÀI**: **TÌM HIỂU VỀ CƠ CHẾ XÁC THỰC ĐĂNG NHẬP, TRIỄN KHAI HỆ THỐNG MINH HỌA**

**Giáo viên hướng dẫn:**

1. Cô Trần Thị Bích Vân

**Sinh viên thực hiện:**

1. 2033210426 - Nguyễn Đình Phát
2. 2033216454 - Nguyễn Hoàng Minh Khoa
3. 2033211001 - Cao Trương Hoàng Vinh

*Thành Phố Hồ Chí Minh, tháng 12 năm 2024*

# LỜI CAM ĐOAN

Nhóm em xin cam đoan đây là công trình nghiên cứu của riêng nhóm. Các số liệu, kết quả nêu trong Đồ án là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Nhóm em xin cam đoan rằng mọi sự giúp đỡ cho việc thực hiện Đồ án này   
đã được cảm ơn và các thông tin trích dẫn trong Đồ án đã được chỉ rõ nguồn gốc.

**Nhóm sinh viên thực hiện Đồ án**

|  |  |  |
| --- | --- | --- |
| **Sinh viên thực hiện 1** | **Sinh viên thực hiện 2** | **Sinh viên thực hiện 3** |

# LỜI CÁM ƠN

Trong suốt thời gian học tập, thực tập và hoàn thành đồ án tốt nghiệp trước hết, chúng em muốn xin gửi đến quý thầy, cô giáo trong khoa Công nghệ thông tin trường Đại học Công Thương Thành Phố Hồ Chí Minh lời cảm ơn chân thành nhất. Đặc biệt, chúng em xin gửi đến cô Trần Thị Bích Vân, người trực tiếp hướng dẫn và theo sát hỗ trợ, giúp đỡ chúng em tận tình để chúng em có thể hoàn thành báo cáo đồ thật hoàn chỉnh lời cảm ơn sâu sắc nhất. Và trong quá trình làm bài báo cáo thực tập, đồng thời do trình độ lý luận cũng như kinh nghiệm thực tiễn còn hạn chế nên bài báo cáo có thể không tránh khỏi những thiếu sót, rất mong quý thầy cô sẽ thông cảm và góp ý để chúng em có thể khắc phục và hoàn thiện bản thân mình trong thời gian sắp tới.

Chúng em xin chân thành cảm ơn!

TPHCM, tháng 12 năm 2024

Nhóm sinh viên thực hiện

# NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

Tên đề tài: “Tìm hiểu về cơ chế xác thực đăng nhập, triễn khai hệ thống minh họa”

Sinh viên thực hiện:

1. 2033210426 - Nguyễn Đình Phát

2. 2033216454 - Nguyễn Hoàng Minh Khoa

3. 2033211001 - Cao Trương Hoàng Vinh

Khoá: 12DHBM

**Nội dung nhận xét**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn 1** | Ngày …… tháng……..năm 2024  **Giảng viên hướng dẫn 2** |

# NHẬN XÉT CỦA GIẢNG VIÊN PHẢN BIỆN

Tên đề tài: “Tìm hiểu về cơ chế xác thực đăng nhập, triễn khai hệ thống minh họa”

Sinh viên thực hiện:

1. 2033210426 - Nguyễn Đình Phát

2. 2033216454 - Nguyễn Hoàng Minh Khoa

3. 2033211001 - Cao Trương Hoàng Vinh

Khoá: 12DHBM

**Nội dung nhận xét**

|  |  |
| --- | --- |
| **Giảng viên phản biện 1** | Ngày …… tháng……..năm 2024  **Giảng viên phản biện 2** |

# MỤC LỤC

# DANH MỤC CÁC HÌNH ẢNH

# DANH MỤC BẢNG BIỂU

# LỜI MỞ ĐẦU

Trong kỷ nguyên số hiện nay, bảo mật thông tin trở thành một yếu tố sống còn đối với mọi hệ thống công nghệ. Một trong những lớp phòng vệ quan trọng nhất chính là cơ chế **xác thực đăng nhập (Authentication mechanisms)** – bước đầu tiên để đảm bảo rằng người dùng truy cập vào hệ thống thực sự là người họ tuyên bố.

Trước đây, xác thực bằng mật khẩu truyền thống là phương thức chủ yếu, nhưng với sự phát triển mạnh mẽ của các kỹ thuật tấn công mạng như **phishing**, **brute-force**, **credential stuffing**, phương pháp này đã bộc lộ nhiều hạn chế. Từ đó, nhiều mô hình xác thực hiện đại hơn ra đời như **xác thực hai yếu tố (2FA)**, **đa yếu tố (MFA)**, **OAuth 2.0**, **SAML**, **JWT**, v.v... với mục tiêu tăng cường khả năng phòng vệ của hệ thống.

Đề tài **“Tìm hiểu về cơ chế xác thực đăng nhập và triển khai hệ thống minh họa”** được thực hiện nhằm hệ thống hóa các phương thức xác thực phổ biến hiện nay, đồng thời triển khai thử nghiệm một số cơ chế điển hình để đánh giá hiệu quả bảo mật trong môi trường giả lập.

Thông qua đề tài này, nhóm thực hiện mong muốn mang đến cái nhìn toàn diện về các mô hình xác thực, từ đó hỗ trợ việc lựa chọn, thiết kế và triển khai cơ chế phù hợp cho từng loại hệ thống thực tế.

# CHƯƠNG 1: TỔNG QUAN

## 1.1. Lý do chọn đề tài

Xác thực đăng nhập là bước đầu tiên trong quá trình bảo vệ hệ thống thông tin, nhưng đồng thời cũng là điểm yếu dễ bị khai thác nhất. Theo thống kê của **Verizon Data Breach Report**, hơn 80% các vụ rò rỉ dữ liệu bắt nguồn từ lỗ hổng trong cơ chế xác thực. Trong bối cảnh đó, việc nghiên cứu và hiểu rõ các phương thức xác thực hiện đại là yêu cầu cấp thiết.

Bên cạnh đó, sự đa dạng của các mô hình xác thực (mật khẩu, sinh trắc học, token, xác thực dựa trên danh tính liên kết...) khiến cho việc lựa chọn cơ chế phù hợp trở thành một bài toán phức tạp. Do đó, đề tài này được lựa chọn nhằm mục tiêu tổng hợp, phân tích và thử nghiệm các mô hình xác thực tiêu biểu để làm sáng tỏ những điểm mạnh – yếu của từng phương pháp.

## 1.2. Mục tiêu nghiên cứu

### 1.2.1. Mục tiêu tổng quát

* Tìm hiểu và phân tích các cơ chế xác thực đăng nhập phổ biến hiện nay.
* Triển khai thử nghiệm một số mô hình xác thực trên hệ thống giả lập.
* Đánh giá mức độ bảo mật và tính khả thi của từng phương pháp.

### 1.2.2. Mục tiêu cụ thể

* Phân loại và mô tả nguyên lý hoạt động của các cơ chế xác thực như: mật khẩu truyền thống, xác thực hai yếu tố, OAuth 2.0, JWT, SAML, Kerberos.
* So sánh các cơ chế theo tiêu chí: độ an toàn, tính ứng dụng, khả năng triển khai.
* Xây dựng hệ thống mô phỏng đăng nhập sử dụng một hoặc nhiều phương thức xác thực.
* Phân tích rủi ro bảo mật và đề xuất giải pháp nâng cao.

## 1.3. Phạm vi nghiên cứu

### 1.3.1. Phạm vi lý thuyết

* Tập trung nghiên cứu các loại xác thực:
  + Mật khẩu (Password-based)
  + Xác thực bằng token (Token-based: JWT, OAuth 2.0, SAML)
  + Xác thực hai/đa yếu tố (2FA, MFA)
  + Xác thực không mật khẩu (Passwordless)
* Nghiên cứu các giao thức xác thực: LDAP, Kerberos, OAuth 2.0, OpenID Connect, SAML.

### 1.3.2. Phạm vi thực nghiệm

* Triển khai hệ thống thử nghiệm xác thực trên môi trường máy ảo (Ubuntu, Windows Server, Web server).
* Mô phỏng các tình huống tấn công cơ bản như brute-force, session hijacking.
* Đánh giá hiệu quả và tính bảo mật qua thử nghiệm thực tế.

## 1.4. Cấu trúc báo cáo

Nội dung báo cáo được chia thành 5 chương chính:

* **Lời mở đầu:** Trình bày lý do chọn đề tài, ý nghĩa và mục tiêu tổng thể.
* **Chương 1 - Tổng quan:** Trình bày bối cảnh, mục tiêu, phạm vi và cấu trúc đề tài.
* **Chương 2 - Cơ sở lý thuyết:** Trình bày các khái niệm nền tảng và phân loại cơ chế xác thực.
* **Chương 3: Triển khai hệ thống minh họa:** Xây dựng hệ thống thử nghiệm và đánh giá kết quả thực tế.
* **Chương 4 - Kết quả nghiên cứu:** Phân tích và đánh giá chi tiết từng mô hình xác thực.
* **Chương 5 - Kết luận và hướng phát triển:** Đúc kết kết quả đạt được, nêu ra điểm mạnh, hạn chế và định hướng mở rộng trong tương lai.

# CHƯƠNG 2 CƠ SỞ LÝ THUYẾT

## 2.1. Các khái niệm cơ bản

**2.1.1. Authentication (Xác thực)**

**Authentication** là quá trình xác minh danh tính của người dùng hoặc hệ thống, nhằm đảm bảo rằng chủ thể đang yêu cầu truy cập thực sự là ai mà họ tuyên bố. Đây là bước đầu tiên trong hệ thống an ninh thông tin, giúp bảo vệ dữ liệu, dịch vụ và hệ thống khỏi truy cập trái phép.

**Vai trò của xác thực**

* Đảm bảo chỉ người dùng hợp lệ mới được truy cập tài nguyên.
* Là nền tảng cho các bước bảo mật tiếp theo như authorization (ủy quyền) và accounting (ghi nhật ký truy cập).
* Giảm thiểu rủi ro rò rỉ dữ liệu, chiếm quyền truy cập hoặc giả mạo danh tính.

**Phân biệt Authentication & Authorization**

|  |  |  |
| --- | --- | --- |
| **Tiêu chí** | **Authentication** | **Authorization** |
| Mục tiêu | Xác minh danh tính thành công | Xác định quyền truy cập của người dùng |
| Thứ tự thực hiện | Thực hiện trướcThực hiện trước | Thực hiện sau khi xác thực thành công |
| Dữ liệu sử dụng | Tên người dùng, mật khẩu, vân tay… | Danh sách quyền truy cập, vai trò (roles)... |

### 2.1.2. AAA (Authentication - Authorization - Accounting)

**AAA** là viết tắt của Authentication (Xác thực), Authorization (Phân quyền), và Accounting (Ghi chú tài khoản). Cấu hình AAA thường được thực hiện trong các môi trường mạng để quản lý quyền truy cập vào tài nguyên.

Mô hình AAA là khung quản lý bảo mật trong nhiều hệ thống mạng và ứng dụng hiện đại:

* Authentication: Xác minh danh tính người dùng.
* Authorization: Xác định quyền hạn của người dùng sau khi xác thực.
* Accounting: Ghi nhận lại hoạt động của người dùng để phục vụ giám sát và kiểm toán.

## 2.2. Các yếu tố xác thực (Authentication Factors)

### 2.2.1. Knowledge factors (Yếu tố tri thức)

Yếu tố kiến thức yêu cầu người dùng cung cấp dữ liệu hoặc thông tin trước khi truy cập vào một hệ thống được bảo mật. Mật khẩu (password) hoặc mã số nhận dạng cá nhân (PIN - Personal Identification Number) là những yếu tố xác thực dựa trên kiến thức phổ biến nhất được sử dụng để hạn chế quyền truy cập vào hệ thống. Các ứng dụng phổ thông hoặc đăng nhập vào mạng đều hầu hết yêu cầu tên người dùng (username) hoặc địa chỉ email cùng với mật khẩu hoặc mã PIN tương ứng để được cấp quyền truy cập.

### 2.2.2. Possession factors (Yếu tố sở hữu)

Yếu tố sở hữu yêu cầu người dùng phải sở hữu một thông tin hoặc thiết bị cụ thể trước khi được cấp quyền truy cập vào hệ thống. Các yếu tố sở hữu thường được kiểm soát thông qua một thiết bị được xác định là thuộc về người dùng hợp lệ.

Yếu tố này tăng cường bảo mật trong xác thực đa yếu tố (multifactor authentication) bằng cách yêu cầu người dùng phải vật lý nắm giữ một thiết bị hoặc đối tượng, bên cạnh yếu tố kiến thức (knowledge) hoặc sinh trắc học (biometric). Thiết bị đó có thể là token phần cứng (hardware token), khóa bảo mật (security key), hoặc thiết bị di động (mobile device).

### 2.2.3. Inherence factors (Yếu tố sinh trắc học)

Yếu tố sinh trắc học xác thực danh tính dựa trên các đặc điểm duy nhất của người dùng (unique to the user). Bao gồm: xác thực sinh trắc học qua vân tay (fingerprint), dấu vân ngón tay cái (thumbprint), lòng bàn tay hoặc dấu tay (palm/handprint). Ngoài ra còn có giọng nói (voice recognition), nhận diện khuôn mặt (facial recognition), và quét võng mạc hoặc mống mắt (retina/iris scan).

### 2.2.4. Location factors (Yếu tố vị trí)

Quản trị viên mạng có thể triển khai các dịch vụ sử dụng kiểm tra vị trí địa lý (geolocation security checks) để xác minh vị trí của người dùng trước khi cấp quyền truy cập vào ứng dụng, mạng hoặc hệ thống.

Địa chỉ IP (IP address) là một yếu tố hữu ích để xác định nguồn gốc lưu lượng mạng, nhưng tin tặc có thể dùng VPN để che giấu vị trí. Do đó, địa chỉ MAC (MAC address) – là duy nhất cho từng thiết bị – có thể được dùng như một yếu tố xác thực dựa trên vị trí, nhằm giới hạn quyền truy cập hệ thống từ một số lượng thiết bị được ủy quyền cụ thể.

### 2.2.5. Behavior factors (Yếu tố hành vi)

Yếu tố xác thực dựa trên hành vi phụ thuộc vào **các hành động người dùng thực hiện để truy cập vào hệ thống**. Các hệ thống hỗ trợ yếu tố này có thể cho phép người dùng cấu hình mật khẩu trước bằng cách thực hiện **một hành vi cụ thể trong giao diện xác định**, rồi lặp lại hành vi đó để xác minh danh tính sau này.

## 2.3. Các cơ chế xác thực phổ biến

### 2.3.1. Xác thực bằng mật khẩu

**Mô tả:**  
Người dùng nhập tên đăng nhập và mật khẩu để truy cập hệ thống. Đây là phương pháp xác thực truyền thống và phổ biến nhất.

**Ưu điểm:**

* Dễ triển khai và sử dụng.
* Không yêu cầu phần cứng hoặc phần mềm bổ sung.

**Nhược điểm:**

* Bảo mật thấp: Mật khẩu yếu hoặc sử dụng lại mật khẩu có thể dẫn đến việc bị tấn công. Theo nghiên cứu, nhiều người dùng có xu hướng sử dụng cùng một mật khẩu cho nhiều tài khoản, làm tăng nguy cơ bị xâm nhập.
* Dễ bị tấn công: Các phương pháp như tấn công từ điển, brute-force, và phishing thường nhắm vào mật khẩu.

**Biện pháp cải thiện:**

* Chính sách mật khẩu mạnh: Yêu cầu mật khẩu có độ dài tối thiểu, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.
* Hạn chế số lần đăng nhập sai: Khóa tài khoản sau một số lần đăng nhập thất bại để ngăn chặn tấn công brute-force.

### 2.3.2. Xác thực hai yếu tố (2FA) & đa yếu tố (MFA)

**Mô tả:**  
Yêu cầu người dùng cung cấp hai hoặc nhiều yếu tố xác thực khác nhau để truy cập hệ thống, kết hợp giữa các yếu tố như mật khẩu (knowledge factor), thiết bị di động (possession factor), hoặc sinh trắc học (inherence factor).

**Ưu điểm:**

* Tăng cường bảo mật: Ngay cả khi một yếu tố bị xâm phạm, kẻ tấn công vẫn cần vượt qua các lớp bảo vệ bổ sung.
* Linh hoạt: Có thể kết hợp nhiều phương pháp xác thực khác nhau tùy theo nhu cầu và khả năng của hệ thống.

**Nhược điểm:**

* Phức tạp hơn cho người dùng: Yêu cầu thêm bước xác thực có thể làm giảm trải nghiệm người dùng.
* Chi phí triển khai: Cần đầu tư vào phần cứng hoặc phần mềm bổ sung.

**Ví dụ về phương pháp 2FA/MFA:**

* Mã OTP qua SMS hoặc email: Hệ thống gửi mã xác thực tạm thời đến số điện thoại hoặc email của người dùng.
* Ứng dụng xác thực (Authenticator Apps): Sử dụng ứng dụng như Google Authenticator hoặc Microsoft Authenticator để tạo mã xác thực.
* Thiết bị token vật lý: Thiết bị phần cứng tạo mã xác thực, như YubiKey.

### 2.3.3. Xác thực không mật khẩu (Passwordless Authentication)

**Mô tả:**  
Cho phép người dùng đăng nhập vào hệ thống mà không cần nhập mật khẩu, thay vào đó sử dụng các phương pháp xác thực khác như sinh trắc học hoặc thiết bị sở hữu.

**Ưu điểm:**

* Giảm rủi ro liên quan đến mật khẩu: Loại bỏ nguy cơ mật khẩu yếu, bị lộ hoặc bị quên.
* Cải thiện trải nghiệm người dùng: Đăng nhập nhanh chóng và thuận tiện hơn.

**Nhược điểm:**

* Yêu cầu thiết bị hoặc phần mềm bổ sung: Cần có các thiết bị hỗ trợ như cảm biến vân tay, camera nhận diện khuôn mặt hoặc ứng dụng xác thực.
* Khả năng tiếp cận: Không phải tất cả người dùng đều có thiết bị hỗ trợ xác thực không mật khẩu.

**Ví dụ về phương pháp xác thực không mật khẩu:**

* Sinh trắc học: Sử dụng vân tay, nhận diện khuôn mặt hoặc giọng nói để xác thực.
* Liên kết đăng nhập qua email hoặc SMS: Hệ thống gửi liên kết đăng nhập một lần đến email hoặc số điện thoại của người dùng.
* Khóa bảo mật vật lý: Thiết bị như YubiKey sử dụng giao thức FIDO2 để xác thực**.**

### 2.3.4. Xác thực bằng token (Token-based Authentication)

**Mô tả:**  
Người dùng nhận được một token sau khi xác thực thành công, và sử dụng token này để truy cập các tài nguyên mà không cần xác thực lại.

**Ưu điểm:**

* **Hiệu suất cao:** Giảm tải cho máy chủ xác thực bằng cách sử dụng token cho các yêu cầu tiếp theo.
* **Linh hoạt:** Token có thể được sử dụng trên nhiều dịch vụ và nền tảng khác nhau.

**Nhược điểm:**

* **Quản lý token:** Cần cơ chế bảo vệ và làm mới token để đảm bảo an ninh.
* **Rủi ro khi token bị đánh cắp:** Nếu token không được bảo vệ đúng cách, kẻ tấn công có thể sử dụng để truy cập trái phép.

**Ví dụ về token:**

* **JSON Web Token (JWT):** Token dạng JSON chứa thông tin xác thực và quyền hạn của người dùng.
* **OAuth 2.0:** Giao thức cho phép ứng dụng bên thứ ba truy cập tài nguyên của người dùng mà không cần chia sẻ mật khẩu.
* **OpenID Connect:** Lớp nhận dạng xây dựng trên OAuth 2.0, cho phép xác thực người dùng và thu thập thông tin hồ sơ cơ bản.

### 2.3.5. Xác thực sinh trắc học (Biometric Authentication)

**Mô tả:**

Sử dụng các đặc điểm sinh học độc nhất của người dùng như vân tay, khuôn mặt, mống mắt hoặc giọng nói để xác thực.

**Ưu điểm:**

* Bảo mật cao: Khó giả mạo hoặc sao chép các đặc điểm sinh học.
* Tiện lợi: Người dùng không cần nhớ mật khẩu hoặc mang theo thiết bị bổ sung.

**Nhược điểm:**

* Chi phí triển khai: Yêu cầu phần cứng chuyên dụng như cảm biến vân tay hoặc camera chất lượng cao.
* Vấn đề riêng tư: Cần đảm bảo dữ liệu sinh trắc học được lưu trữ và xử lý an toàn để bảo vệ quyền riêng tư của người dùng.

**Ví dụ về xác thực sinh trắc học**:

* Nhận diện vân tay: Sử dụng cảm biến vân tay để mở khóa thiết bị hoặc truy cập ứng dụng.
* Nhận diện khuôn mặt: Sử dụng camera để quét và nhận diện khuôn mặt người dùng.

## 2.4. Các giao thức xác thực phổ biến

### 2.4.1. LDAP (Lightweight Directory Access Protocol)

**Khái niệm**

**LDAP** là một giao thức nhẹ (lightweight protocol) được sử dụng để truy cập và quản lý dịch vụ thư mục (directory services) trên các mạng máy tính. LDAP cho phép ứng dụng và hệ thống tìm kiếm và truy xuất thông tin từ các cơ sở dữ liệu thư mục, chẳng hạn như thông tin về người dùng, nhóm, máy chủ, và các tài nguyên khác trong một tổ chức.

**LDAP (Lightweight Directory Access Protocol)** **không phải là một giao thức xác thực chuyên dụng**, nhưng **nó thường được sử dụng trong quá trình xác thực người dùng** vì nó cung cấp cơ chế truy cập vào thông tin định danh người dùng (user identity) được lưu trữ trong hệ thống thư mục (directory service).

**Ứng dụng của LDAP:**

* **Xác thực người dùng:** LDAP được sử dụng rộng rãi trong các tổ chức để quản lý việc xác thực và phân quyền người dùng.
* **Quản lý thông tin người dùng:** LDAP giúp lưu trữ thông tin cá nhân, các nhóm người dùng, và các thuộc tính liên quan như email, tên, số điện thoại.
* **Single Sign-On (SSO):** LDAP là nền tảng cho các hệ thống SSO, nơi người dùng chỉ cần đăng nhập một lần để truy cập vào nhiều ứng dụng khác nhau trong hệ thống.

**Các thành phần chính:**

* **LDAP Client**
* **Đặc điểm:** Là một ứng dụng hoặc hệ thống gửi yêu cầu đến máy chủ LDAP.
* **Chức năng:** Client gửi các yêu cầu truy vấn dữ liệu từ thư mục LDAP (ví dụ: xác thực người dùng, tìm kiếm thông tin).
* **LDAP Server**
* **Đặc điểm:** Máy chủ LDAP lưu trữ dữ liệu thư mục và phục vụ các yêu cầu từ client.
* **Chức năng:** Đáp ứng các yêu cầu của client về việc đọc, viết, cập nhật hoặc xóa thông tin trong thư mục. Máy chủ LDAP sử dụng một cơ sở dữ liệu thư mục (Directory Information Tree - DIT) để lưu trữ dữ liệu.
* **Directory Information Tree (DIT)**
* **Đặc điểm:** Là cấu trúc dữ liệu trong LDAP, nơi lưu trữ tất cả các thông tin thư mục.
* **Chức năng:** Tổ chức các đối tượng dữ liệu (ví dụ: người dùng, nhóm, tài nguyên) theo một cây phân cấp. Cấu trúc này dễ dàng mở rộng và hỗ trợ các thao tác tìm kiếm hiệu quả.
* **Distinguished Name (DN)**
* **Đặc điểm:** Là tên duy nhất dùng để xác định một đối tượng trong thư mục LDAP. DN bao gồm các thành phần như tên miền, tên tổ chức, và các thuộc tính khác.
* **Chức năng:** DN xác định chính xác vị trí của một đối tượng trong DIT.
* **Attributes**
* **Đặc điểm:** Các thuộc tính của mỗi đối tượng trong thư mục LDAP, mô tả thông tin liên quan đến đối tượng đó. Ví dụ: đối với người dùng, các thuộc tính có thể bao gồm tên, địa chỉ email, số điện thoại, v.v.
* **Chức năng:** Lưu trữ dữ liệu chi tiết về đối tượng.
* **Object Classes**
* **Đặc điểm:** Xác định loại đối tượng và các thuộc tính bắt buộc của nó trong thư mục. Ví dụ: "Person" có thể có các thuộc tính như "cn" (common name), "sn" (surname).
* **Chức năng:** Định nghĩa kiểu đối tượng (ví dụ: người dùng, nhóm) và các thuộc tính mà đối tượng đó phải có.

**Quy trình hoạt động**

**Bước 1 - Khởi tạo kết nối:** Client khởi tạo một kết nối tới máy chủ LDAP và có thể sử dụng một trong các giao thức như **TLS/SSL** để bảo mật dữ liệu khi truyền qua mạng.

**Bước 2 - Xác thực người dùng:**

* Trước khi truy cập vào các thông tin trong thư mục LDAP, client có thể cần xác thực người dùng. Quá trình này thường sử dụng **bind operation** (hành động kết nối) trong LDAP để đảm bảo rằng người dùng có quyền truy cập vào thư mục.
* Nếu quá trình bind thành công, client có thể tiếp tục các thao tác truy vấn hoặc thay đổi dữ liệu trong thư mục.

**Bước 3 - Truy vấn thông tin**

* Sau khi kết nối thành công, client gửi yêu cầu truy vấn đến máy chủ LDAP. Yêu cầu này có thể là để tìm kiếm các đối tượng trong thư mục hoặc lấy thông tin chi tiết về một đối tượng.
* Ví dụ, client có thể tìm kiếm tất cả các đối tượng có thuộc tính "email" hoặc "username".

**Bước 4 - Phản hồi từ máy chủ LDAP**

* Máy chủ LDAP xử lý yêu cầu của client và trả về kết quả. Kết quả này có thể là danh sách các đối tượng hoặc các thuộc tính của đối tượng thỏa mãn yêu cầu tìm kiếm.
* Nếu yêu cầu thay đổi dữ liệu, như cập nhật thông tin người dùng, máy chủ LDAP sẽ thực hiện thao tác này và trả về kết quả thông báo thành công hay lỗi.

**Bước 5 - Đóng kết nối:** Khi các thao tác hoàn tất, client có thể đóng kết nối với máy chủ LDAP hoặc tiếp tục thực hiện các thao tác khác.

### 2.4.2. Kerberos

**Kerberos** Là một giao thức bảo mật được sử dụng để xác thực người dùng và các dịch vụ trong một mạng máy tính, giúp bảo vệ các giao dịch mạng và tránh các tấn công giả mạo. Giao thức này sử dụng một hệ thống mật mã để xác thực các thực thể trong một môi trường mạng phân tán mà không cần phải truyền mật khẩu qua mạng.

**Các thành phần chính**

* **Key Distribution Center (KDC):** Là thành phần trung tâm trong giao thức Kerberos, KDC bao gồm hai thành phần con:
* Authentication Server (AS): Chịu trách nhiệm xác thực người dùng khi họ lần đầu tiên đăng nhập vào hệ thống.
* Ticket Granting Server (TGS): Cung cấp "vé" (ticket) cho người dùng để truy cập vào các dịch vụ cụ thể trong mạng sau khi họ đã được xác thực bởi AS.
* **Principal**: là một thực thể trong hệ thống Kerberos, có thể là người dùng, máy tính hoặc dịch vụ mà giao thức Kerberos có thể xác thực. Mỗi principal có một mật khẩu hoặc khóa bí mật (secret key) để xác thực.
* **Ticket** là một phần quan trọng trong Kerberos.

Ticket là một gói thông tin mã hóa mà người dùng có thể sử dụng để chứng minh rằng họ đã được xác thực và có quyền truy cập vào một dịch vụ nào đó.

Các ticket này chứa thông tin về principal, thời gian hết hạn và các quyền hạn truy cập.

* **Session Key** Là một khóa bí mật mà người dùng và dịch vụ có thể sử dụng để mã hóa và giải mã thông tin trong suốt phiên làm việc của họ. Session Key được tạo ra trong quá trình cấp ticket.

**Quy trình hoạt động**

**Bước 1 - Đăng nhập (Initial Login)**

* Người dùng nhập **tên đăng nhập (username)** và **mật khẩu** trên máy tính.
* Máy tính **băm mật khẩu** và sử dụng nó để tạo khóa đối xứng (symmetric key).
* Máy khách (client) gửi yêu cầu đến **AS (Authentication Server)** bao gồm: Tên người dùng (principal name), Tên miền (realm) và Dấu thời gian

**Bước 2 - AS cấp Ticket-Granting Ticket (TGT)**

* **Authentication Server (AS)** kiểm tra tên người dùng.
* Nếu hợp lệ, AS tạo và gửi về:
* **TGT (Ticket Granting Ticket)** – chứa thông tin được mã hóa bằng khóa bí mật của **TGS**.
* **Session key** – được mã hóa bằng khóa đối xứng tạo từ mật khẩu người dùng.

**Bước 3 - Yêu cầu Ticket cho Dịch vụ (Service Ticket)**

* Khi người dùng muốn truy cập một dịch vụ mạng (như file server, email, v.v.), client gửi yêu cầu đến **TGS (Ticket Granting Server)** kèm:
* TGT
* Tên dịch vụ cần truy cập
* Authenticator (mã hóa bằng session key để xác minh danh tính người dùng)

**Bước 4 - TGS cấp Service Ticket**

* TGS xác minh TGT và Authenticator.
* Nếu hợp lệ, TGS tạo và trả về:
* **Service Ticket** – mã hóa bằng khóa bí mật của dịch vụ đích
* Một session key mới dùng giữa client và dịch vụ đích

**Bước 5 - Truy cập Dịch vụ**

* Client gửi Service Ticket đến máy chủ dịch vụ (Service Server – SS).
* Máy chủ dịch vụ giải mã vé bằng khóa của nó → nếu thành công:
* Cho phép truy cập
* Gửi lại xác nhận (có thể là timestamp mã hóa bằng session key)

### 2.4.3. OAuth 2.0

**OAuth 2.0** là một giao thức ủy quyền (authorization) mở rộng và phổ biến được thiết kế để cấp quyền truy cập có kiểm soát cho các tài nguyên của người dùng mà không cần phải chia sẻ mật khẩu của họ, cho phép người dùng ủy quyền cho ứng dụng (client) truy cập vào tài nguyên được lưu trữ trên một dịch vụ khác mà không cần chia sẻ thông tin đăng nhập của mình

**Các thành phần chính**

* **Resource Owner**: Là người dùng hoặc thực thể sở hữu tài nguyên, như thông tin cá nhân, dữ liệu trong các ứng dụng (ví dụ: tài khoản Google, Facebook).
* **Client**: Là ứng dụng hoặc dịch vụ yêu cầu quyền truy cập vào tài nguyên của người dùng.
* **Authorization Server**: Máy chủ xác thực và cấp quyền truy cập, chịu trách nhiệm cấp mã truy cập (access token) sau khi người dùng ủy quyền cho ứng dụng.
* **Resource Server**: Máy chủ chứa tài nguyên mà ứng dụng muốn truy cập. Ví dụ, một dịch vụ API có thể là Resource Server cung cấp dữ liệu của người dùng.
* **Access Token**: Mã token được cấp cho ứng dụng sau khi người dùng ủy quyền, cho phép ứng dụng truy cập tài nguyên trong một khoảng thời gian giới hạn.

**Quy trình hoạt động**

**Bước 1 - Client yêu cầu quyền truy cập**

Ứng dụng (client) chuyển hướng người dùng đến **Authorization Server**, gửi kèm client\_id, redirect\_uri, response\_type=code, scope (quyền truy cập yêu cầu) và state (mã bảo vệ CSRF).

**Bước 2 - Người dùng ủy quyền:**

* Authorization Server hiển thị trang đăng nhập.
* Người dùng đăng nhập và xác nhận ủy quyền cho ứng dụng truy cập tài nguyên.

**Bước 3 - Nhận Authorization Code:** Nếu người dùng đồng ý, Authorization Server **chuyển hướng lại client (qua redirect\_uri)** kèm theo authorization\_code (mã xác thực tạm thời)

**Bước 4 - Client nhận Access Token**: Ứng dụng sử dụng Authorization Code để yêu cầu Access Token từ Authorization Server.

* Client gửi yêu cầu **POST đến Authorization Server** kèm authorization\_code, client\_id, client\_secret, redirect\_uri.
* Authorization Server xác minh thông tin và trả về: access\_token, refresh\_token (tùy chọn)

**Bước 5 - Truy cập tài nguyên**

* Ứng dụng sử dụng access\_token để gửi yêu cầu đến Resource Server (API).
* Resource Server xác minh token → nếu hợp lệ thì trả dữ liệu về.

### 2.4.4. OpenID Connect

**OpenID Connect l**à một lớp mở rộng của OAuth 2.0, cung cấp một cơ chế xác thực người dùng mà OAuth 2.0 không có bằng **ID Token**, được sử dụng để xác minh danh tính người dùng.

**OIDC** cung cấp các tính năng cần thiết để xác thực người dùng, chẳng hạn như trả về thông tin về người dùng (profile, email, v.v.) và cho phép ứng dụng xác minh rằng người dùng đã đăng nhập qua một nhà cung cấp xác thực (Identity Provider - IdP).

**Các thành phần chính**

* ID Token: Là token được sử dụng để xác thực danh tính của người dùng. Đây là một JWT (JSON Web Token) chứa thông tin về người dùng, bao gồm tên, email, và các thuộc tính khác.
* UserInfo Endpoint: Một API được cung cấp bởi Identity Provider, cho phép ứng dụng lấy thông tin chi tiết về người dùng sau khi xác thực.
* ID Provider (IdP): Là máy chủ xác thực người dùng và phát hành ID Token.

**Quy trình hoạt động**

**Bước 1 - Người dùng truy cập ứng dụng:** Người dùng truy cập trang web hoặc ứng dụng (Relying Party – RP) yêu cầu đăng nhập.

**Bước 2 - Ứng dụng yêu cầu xác thực:** Ứng dụng gửi yêu cầu đến Authorization Server (ID Provider) thông qua OAuth 2.0 với yêu cầu xác thực.

**Bước 3 - Người dùng đăng nhập và cấp quyền:** Tại Authorization Server, người dùng đăng nhập (nếu chưa đăng nhập) và đồng ý chia sẻ thông tin với ứng dụng.

**Bước 4 - Nhận Authorization Code:** Nếu đồng ý, Authorization Server chuyển hướng lại về ứng dụng kèm theo authorization\_code

**Bước 5 - ID Token và Access Token:** Ứng dụng dùng authorization\_code để gửi yêu cầu POST đến token endpoint của IDP, Authorization Server sẽ trả về ID Token (JWT chứa thông tin danh tính người dùng) và Access Token cho ứng dụng.

**Bước 6 - Xác thực và truy cập thông tin người dùng:** Ứng dụng sử dụng ID Token để xác thực người dùng và Access Token để truy cập tài nguyên được bảo vệ.

### 2.4.5. SAML 2.0 (Security Assertion Markup Language)

**SAML 2.0** là một giao thức tiêu chuẩn được sử dụng để xác thực và ủy quyền trong các hệ thống phân tán. Nó cho phép chia sẻ thông tin xác thực và ủy quyền giữa các ứng dụng hoặc dịch vụ khác nhau một cách an toàn, chủ yếu trong các môi trường doanh nghiệp hoặc giữa các dịch vụ đám mây và ứng dụng web.

**SAML** là một giao thức XML dựa trên **standard** để trao đổi các thông tin xác thực giữa các thực thể, chẳng hạn như người dùng và dịch vụ, hay giữa các tổ chức hoặc miền (domain). SAML cho phép người dùng đăng nhập một lần và truy cập nhiều ứng dụng mà không cần phải xác thực lại (Single Sign-On - SSO).

**Các thành phần chính**

* + Identity Provider (IdP): xác thực người dùng, phát hành SAML Assertion
  + Service Provider (SP): Dịch vụ mà người dùng muốn truy cập, chấp nhận assertion từ IdP
  + SAML Assertion: là thông điệp XML được phát hành bởi IdP và chứa các tuyên bố về người dùng, chẳng hạn như tên người dùng, email, quyền truy cập, v.v. Assertions có thể có ba loại:
  + **Authentication Assertion**: Xác thực người dùng.
  + **Attribute Assertion**: Cung cấp các thuộc tính liên quan đến người dùng (ví dụ: email, tên người dùng).
  + **Authorization Decision Assertion**: Cung cấp quyết định về quyền truy cập của người dùng.
  + SAML Protocol: Giao thức định nghĩa cách yêu cầu/response được cấu trúc
  + SAML Bindings: Các phương thức dùng để truyền tải các yêu cầu và phản hồi SAML qua mạng, chẳng hạn như HTTP Redirect, HTTP POST, SOAP, v.v.
  + SAML Metadata : Là thông tin cấu hình về các IdP và SP. Metadata định nghĩa cách hai thực thể (IdP và SP) sẽ giao tiếp với nhau, bao gồm thông tin như URL của dịch vụ xác thực, chứng chỉ số, v.v

**Quy trình hoạt động**

**Bước 1 -** User yêu cầu truy cập dịch vụ (SP)

**Bước 2 -** SP chuyển hướng người dùng đến IdP (HTTP Redirect Binding)

**Bước 3 -** Người dùng đăng nhập tại IdP

**Bước 4 -** IdP xác thực người dùng, tạo SAML Assertion

**Bước 5 -** IdP gửi Assertion về lại SP (qua trình duyệt, sử dụng HTTP POST Binding)

**Bước 6 -** SP xác minh Assertion và cấp quyền truy cập

**Bước 7 -** Người dùng được truy cập dịch vụ – thực hiện SSO

### 2.4.6. RADIUS (Remote Authentication Dial-In User Service)

**RADIUS** là một giao thức AAA phổ biến, được sử dụng chủ yếu trong các mạng doanh nghiệp để cung cấp dịch vụ xác thực người dùng và phân quyền truy cập.

**RADIUS** thường được sử dụng trong các kết nối mạng dial-up, VPN (Virtual Private Network), mạng không dây (Wi-Fi), và các thiết bị mạng khác như router và switch.

**Các thành phần chính**

* **Client** **(NAS - Network Access Server):** Là thiết bị yêu cầu xác thực, chẳng hạn như router, switch, hoặc access point (AP). Khi người dùng cố gắng truy cập vào mạng, client sẽ gửi yêu cầu xác thực tới máy chủ RADIUS.
* **RADIUS Server**: Là máy chủ xử lý yêu cầu xác thực, ủy quyền và giám sát (accounting). RADIUS server lưu trữ thông tin người dùng, kiểm tra tính hợp lệ của người dùng và cấp quyền truy cập.
* **User**: người muốn truy cập vào mạng hoặc dịch vụ.

**Quy trình hoạt động**

* **Yêu cầu xác thực**: Khi người dùng cố gắng truy cập vào mạng, client (ví dụ: router, switch) sẽ gửi yêu cầu xác thực tới RADIUS server. Yêu cầu này thường chứa tên người dùng và mật khẩu.
* **Kiểm tra và phản hồi**: RADIUS server kiểm tra thông tin xác thực (thường qua cơ sở dữ liệu người dùng hoặc một hệ thống bên ngoài như Active Directory) và trả về một phản hồi:
  + Access Accept: Nếu thông tin hợp lệ, RADIUS server cho phép truy cập.
  + Access Reject: Nếu thông tin không hợp lệ, RADIUS server từ chối yêu cầu truy cập.
  + Access Challenge: Được sử dụng trong trường hợp yêu cầu thêm thông tin xác thực, chẳng hạn như mã PIN hoặc OTP.
* **Ủy quyền và Giám sát**: Sau khi xác thực, server có thể cấp quyền truy cập vào các tài nguyên cụ thể và ghi lại thông tin (accounting) về hành động của người dùng (ví dụ: thời gian sử dụng, lượng dữ liệu truyền tải).

### 2.4.7. TACACS+ (Terminal Access Controller Access-Control System Plus)

TACACS+ là một giao thức AAA phát triển bởi Cisco, được cải tiến từ TACACS với các tính năng bảo mật mạnh mẽ hơn. TACACS+ chủ yếu được sử dụng để quản lý quyền truy cập của người dùng vào các thiết bị mạng như router, switch, firewall, và các thiết bị mạng khác trong môi trường doanh nghiệp.

**Các thành phần chính**

* **Client**: Tương tự như trong RADIUS, là các thiết bị yêu cầu xác thực (ví dụ: router, switch).
* **TACACS+ Server**: Là máy chủ xử lý xác thực, ủy quyền và giám sát. TACACS+ server lưu trữ thông tin về người dùng và quản lý quyền truy cập vào các thiết bị mạng.
* **User**: Là người dùng muốn truy cập vào các thiết bị mạng, có thể là một quản trị viên hệ thống hoặc người dùng bình thường.

**Quy trình hoạt động**

**Bước 1 - Yêu cầu xác thực**: Khi người dùng muốn đăng nhập vào một thiết bị mạng, yêu cầu xác thực sẽ được gửi tới TACACS+ server.

**Bước 2 - Xác thực**: TACACS+ server kiểm tra thông tin đăng nhập (thường bao gồm tên người dùng và mật khẩu) và trả về một phản hồi.

**Bước 3 - Ủy quyền**: Sau khi xác thực người dùng, TACACS+ server có thể cấp quyền truy cập và quyết định người dùng có quyền thực hiện những thao tác gì trên thiết bị mạng.

**Bước 4 - Giám sát (Accounting)**: TACACS+ ghi lại các thông tin về hành động của người dùng (như lệnh đã thực hiện) để giám sát hoạt động và kiểm tra sau này.

## 2.5. Tổng kết chương 2

Chương 2 đã trình bày những nền tảng lý thuyết quan trọng nhằm giúp hiểu rõ bản chất của các cơ chế xác thực trong lĩnh vực bảo mật hệ thống. Cụ thể:

* **Phần 2.1** giới thiệu khái niệm xác thực (authentication), vai trò trong an ninh thông tin, cũng như sự khác biệt giữa xác thực và ủy quyền (authorization). Đồng thời, mô hình AAA (Authentication – Authorization – Accounting) được đề cập như một nguyên tắc cốt lõi trong thiết kế hệ thống bảo mật.
* **Phần 2.2** đi sâu vào các yếu tố xác thực (authentication factors), bao gồm:
  + Knowledge factors (thông tin người dùng biết, như mật khẩu);
  + Possession factors (thiết bị người dùng sở hữu, như token hoặc điện thoại);
  + Inherence factors (đặc điểm sinh trắc học, như vân tay, khuôn mặt);
  + Location factors (dựa vào vị trí địa lý hoặc IP);
  + Behavior factors (dựa vào hành vi sử dụng thiết bị, cách gõ phím,…).
* **Phần 2.3** trình bày các **cơ chế xác thực phổ biến**, từ phương pháp cơ bản như xác thực bằng mật khẩu, đến các phương pháp hiện đại như xác thực không mật khẩu (passwordless), xác thực sinh trắc học, và xác thực dựa trên token (JWT, OTP,…). Ngoài ra, khái niệm xác thực hai yếu tố (2FA) và đa yếu tố (MFA) cũng được phân tích về mặt an toàn và tính ứng dụng thực tế.
* **Phần 2.4** giới thiệu các **giao thức xác thực phổ biến** được sử dụng rộng rãi trong doanh nghiệp hiện nay:
  + LDAP: Truy vấn thông tin người dùng trong hệ thống thư mục.
  + Kerberos: Cung cấp xác thực mạnh thông qua cơ chế vé (ticket) an toàn.
  + OAuth 2.0 và OpenID Connect: Xác thực và ủy quyền hiện đại cho web và ứng dụng di động.
  + SAML 2.0: Xác thực dựa trên XML cho môi trường doanh nghiệp với hỗ trợ SSO.
  + RADIUS và TACACS+: Các giao thức AAA phục vụ xác thực truy cập vào hạ tầng mạng.

Tóm lại, chương này đóng vai trò như một nền tảng vững chắc về mặt học thuật và kỹ thuật để người đọc có thể hiểu sâu hơn về cách các hệ thống xác thực hoạt động, cũng như chuẩn bị cho chương tiếp theo về phân tích và triển khai các cơ chế xác thực minh họa thực tế.

# CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG MINH HỌA

# CHƯƠNG 4: KẾT QUẢ NGHIÊN CỨU

# CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

**5.1. Điểm mạnh  
5.2. Điểm hạn chế  
5.3. Kết luận  
5.4. Hướng phát triển tiếp theo**

# TÀI LIỆU THAM KHẢO

# PHỤ LỤC