Access Control

Khái niệm & Mục tiêu

- **Access Control** = tập hợp cơ chế cho phép quản trị viên kiểm soát hành vi, tài nguyên và nội dung trong hệ thống.
- **Mục tiêu**: Giảm rủi ro truy cập trái phép tới hệ thống **vật lý** và **logic**.
- **Thành phần cốt lõi**:
    - **Authentication** – Xác thực.
    - **Authorization** – Cấp quyền.
    - **Audit** – Ghi log & giám sát.

Loại Access Control

- **Physical Access Control**: Cổng, khóa, thẻ từ, camera.
- **Technical/Logical Access Control**: Quyền đọc/ghi/thực thi file, truy vấn DB, chạy chương trình. (file - program - data permission)

Thuật ngữ chính

- **Identification** – "Bạn là ai?"
- **Authentication** – "Chứng minh bạn là ai?"
- **Authorization** – "Bạn được làm gì?".

Identification

Bước **khai báo danh tính** với hệ thống – trả lời câu hỏi *"Bạn là ai?"*.

- Thực hiện ở giai đoạn đầu khi truy cập (nhập username, ID, số thẻ, …).
- Chỉ **khai báo** chứ chưa chứng minh → cần bước **authentication** tiếp theo để xác thực.
- Có thể kèm **verification** (đối chiếu thông tin giấy tờ, sinh trắc học) để đảm bảo danh tính là thật

Authentication - Xác thực người dùng

Yếu tố xác thực (Factors)

1. **Something you know** – mật khẩu, PIN, passphrase.
2. **Something you have** – token, smart card, digital cert.
3. **Something you are/do** – sinh trắc học: vân tay, khuôn mặt, giọng nói, chữ ký.

Phương thức

- **SFA** – Single Factor Authentication.

- **2FA** – Two Factor Authentication.
- **MFA** – Multi Factor Authentication.

Ưu & Nhược

- **Ưu**: Dễ triển khai (SFA), tăng bảo mật (MFA).
- **Nhược**: SFA dễ bị tấn công; MFA phức tạp và tốn chi phí.

Rủi ro mật khẩu

- Bị đoán, brute-force, dictionary, rainbow table, social engineering.
- Giải pháp: Chính sách mật khẩu mạnh, proactive/reactive checking, OTP.

OTP

Loại OTP	Công thức / Cơ chế	Yếu tố đầu vào	Cần đồng bộ gì?	Ưu điểm	Nhược điểm	Ví dụ thực tế
HOTP (HMAC-based One-Time Password)	OTP = `Truncate(HMAC(secret, counter))`	Secret key + Counter	Counter (server & client phải sync)	Đơn giản, dễ triển khai	Counter có thể lệch, phải resync	Một số token đời cũ
TOTP (Time-based One-Time Password)	OTP = `Truncate(HMAC(secret, floor(time / step)))`	Secret key + Thời gian	Đồng bộ thời gian (thường ±30s)	Không cần kết nối mạng, bảo mật hơn HOTP	Nếu lệch giờ → fail	Google Authenticator, Microsoft Authenticator
Challenge-Response OTP	Response = `f(secret, challenge)`	Secret key + Challenge (server random)	Không cần đồng bộ, chỉ cần chung secret	Chống replay attack, rất an toàn	Người dùng phải nhập challenge (hơi phiền)	RSA SecurID (chế độ challenge), smartcard

Loại OTP	Công thức / Cơ chế	Yếu tố đầu vào	Cần đồng bộ gì?	Ưu điểm	Nhược điểm	Ví dụ thực tế
SMS/Email OTP	Server random OTP gửi qua kênh phụ	Random OTP từ server	Không yêu cầu đồng bộ	Dễ dùng, không cần app	Dễ bị intercept (SIM swap, email hack), phụ thuộc mạng	Hầu hết Internet Banking, ví điện tử
Push-based OTP / Approval	Server gửi request đến app → user Approve	Secret key + Challenge (ẩn trong push)	Internet connection	Tiện lợi, chỉ cần bấm "Yes/No"	Phụ thuộc mạng, dễ bị phishing giả push	Duo Security, Microsoft Authenticator push

Tiêu chí	RADIUS	Kerberos	TACACS+	LDAP
Tên đầy đủ	Remote Authentication Dial-In User Service	Kerberos	Terminal Access Controller Access-Control System Plus	Lightweight Directory Access Protocol
Loại giao thức	AAA (Authentication, Authorization, Accounting)	Authentication protocol (dựa trên ticket & symmetric key)	AAA protocol (Cisco proprietary)	Directory access protocol
Transport	UDP (1812 auth, 1813 acct)	TCP/UDP (88)	TCP (49)	TCP (389), LDAPS (636)
Mã hóa / Bảo mật	Chỉ mã hóa password (MD5, yếu)	Sử dụng ticket, session key, mutual authentication	Mã hóa toàn bộ gói tin	TLS/SSL (LDAPS) để bảo mật
Cơ chế xác thực	Username + password, token, cert (qua NAS)	Ticket Granting Ticket (TGT) từ KDC	Username/password → TACACS+ server check	Bind (simple, SASL, Kerberos)

AAA support	Có đủ (Auth, Authz, Accounting – nhưng Auth & Authz gộp chung)	Chỉ Authentication (Authorization do hệ thống khác lo)	Có đủ (Auth, Authz, Accounting tách biệt rõ)	Authentication (user info), không phải AAA protocol
Ứng dụng chính	ISP, VPN, Wi-Fi Enterprise (802.1X)	Domain login trong Windows/AD, SSO	Quản trị thiết bị mạng (router, switch, firewall)	Quản lý thông tin user/group/policy trong AD, OpenLDAP
Ưu điểm	Nhẹ, đơn giản, chuẩn mở, tích hợp được nhiều hệ thống	Bảo mật mạnh (mutual auth, chống replay), dùng trong AD/SSO	Rất bảo mật, chi tiết (log từng lệnh), tách biệt AAA	Dữ liệu dạng cây, tối ưu cho đọc/search, chuẩn mở
Nhược điểm	Bảo mật gốc yếu (MD5), dựa trên UDP (mất gói)	Phức tạp, cần đồng bộ clock, KDC là SPOF	Cisco proprietary, chủ yếu dùng trong Cisco ecosystem	Không phải AAA, chỉ cung cấp directory info, cần kết hợp với RADIUS/Kerberos
Ví dụ thực tế	Wi-Fi WPA2-Enterprise, VPN client auth	Windows Active Directory login, MIT Kerberos	Cisco ISE/ACS để quản lý admin login router	OpenLDAP, Microsoft AD, Email servers
Tóm tắt	dùng cho **end-user network access** (Wi-Fi, VPN, ISP).	dùng cho **domain login & SSO**, đặc biệt trong **Windows AD**.	dùng cho **admin login & command authorization trên network devices**.	là **directory service**, nơi lưu user info, group, policy; thường tích hợp với RADIUS/Kerberos.

Authorization

- Xác định quyền dựa trên **trust level** và **need-to-know**.
- **Subject**: Entity yêu cầu truy cập.
- **Object**: Tài nguyên bị bảo vệ.
- **Access Rights**: Read, Write, Execute, Delete, Create, Search.

Mô hình Access Control

Mô hình	Đặc điểm	Ưu điểm	Nhược điểm
MAC – Mandatory Access Control	Quyền do **central authority** quy định; người dùng không thay đổi được	Bảo mật cao, chuẩn hóa	Thiếu linh hoạt, phức tạp

DAC – Discretionary Access Control	Chủ sở hữu toàn quyền cấp/quản lý quyền	Linh hoạt, dễ quản lý	Dễ sai sót, nguy cơ lộ dữ liệu
RBAC – Role-Based Access Control	Quyền dựa trên vai trò trong tổ chức	Quản lý tập trung, dễ mở rộng	Cần quản trị role cẩn thận
Rule-Based AC	Quyền dựa trên luật điều kiện (thời gian, vị trí)	Rất linh hoạt, phù hợp chính sách động	Quản trị phức tạp
ABAC – Attribute-Based AC	Quyền dựa trên thuộc tính của Subject, Object, Environment	Linh hoạt cao, phù hợp hệ thống lớn	Độ phức tạp và chi phí cao

Triển khai Access Control

- **Principle of Least Privilege**: Chỉ cấp quyền tối thiểu cần thiết.
- **Access Control Matrix**:
    - **ACL (Access Control List)** – gắn với object. - ai có thể truy cập
    - **Capability List** – gắn với subject. - có thể truy cập vào đâu

Identity, Credential & Access Management

- **Identity Management**: Quản lý vòng đời định danh số (tạo, phân phối, thu hồi).
- **Credential Manager**: Quản lý vòng đời chứng thực (PIN reset, revoke, reissue).
- **Access Manager**: Quản lý tài nguyên, quyền và chính sách.
- **Identity Federation**: Tin tưởng định danh giữa các tổ chức (SSO, federated login).

Các yếu tố nâng cao

- **User Provisioning**: Tự động cấp quyền theo vai trò.
- **Password Synchronization**: Đồng bộ mật khẩu giữa nhiều hệ thống.
- **Centralized Auditing**: Theo dõi và báo cáo tập trung.
- **Regulatory Compliance**: Đáp ứng tiêu chuẩn (ISO 27001, HIPAA, PCI DSS).

Liên hệ thực tế & Best Practices

- **Chính sách mật khẩu mạnh** + **MFA** cho tài khoản quan trọng.
- **RBAC** cho môi trường doanh nghiệp vừa & nhỏ; **ABAC** cho tập đoàn lớn.
- Tích hợp **SSO** nhưng phải có cơ chế **session timeout** và **conditional access**.
- Audit định kỳ, đặc biệt là **quyền admin/root**.
- Khi cấp quyền mới → áp dụng **Just-In-Time Access** để hạn chế quyền tồn tại lâu.