Authentication

1. Các khái niệm cơ bản.

- Authentication là qua trình xác định người và thực thể truy cập vào hệ thống máy tính có thực sự là người mà họ tuyên bố hay không → hệ thống sẽ được ra cho bạn được phép hoặc không truy cập.
- Authorization là là qua trình mà thực thể xác đinh quyền vào nội dung hoạt động sau khi quá trình authentication kết thúc.
- Việc xác thực được thực hiện ở bất kì đâu khi cần phân quyền.

2. Hoạt động.

3. yếu tố xác thực.

- có 3 yếu tố chính để xác thực:

    - yếu tố kiến thức : là nhưng thứ người dùng biết sử dụng để xác thực.(mật khẩu, mã pin, câu hỏi,….)
    - yếu tố sở hữu : là yếu tố người dùng có như căn cước, khoá bảo mật, sim số, bằng lái xe….)
    - yếu tố vốn có : là yếu tối mà ai sinh ra cũng có như vân tay, võng mạc, khuôn mặt….)

- các xác thực như 2FA và 3FA là xác thực 1 trong những yếu tố trên nhằm đảm bảo rằng người sử dụng là chính chủ sở hữu.

4. Các loại xác thực.

- các loại xác thực nhằm chính xác thực với tài khoản.

- xác thực mã thông báo : thường sử dụng qua SMS hoặc các nền tảng nhắn tin nhằn cung cấp thông tin xác thực như OTP, reset password….
- xác thực mật khẩu : là yêu cầu người dung nhập mật khẩu và nhập mật khẩu mới khi đăng nhập.
- xác thực sinh trắc học : dây là yếu tố vốn có như vân tay, võng mạc…Nhằm thực hiện xác thực qua các yêu tố đó.
- xác thực dựa trên chứng chỉ : hoạt động bằng cách sử dụng chứng chỉ số (digital certificate) được lưu trữ trên thiết bị của người dùng cùng với khóa

riêng (private key). Khi người dùng hoặc thiết bị yêu cầu truy cập, chứng chỉ số sẽ được trình bày để máy chủ xác minh.

- MFA :là sự kết hợp 1 hoặc nhiều loại xác thực ở trên.
- Xác thực không cần mật khẩu : là loại xác thực cung cấp thông tin bằng chứng để chứng minh cho 1 số chướng ngại vật để xác thực.
- SSO : cho phép người dùng xác thực nhiều tài khoản bằng 1 bộ xác thực thông tin xác thực.(như google, apple, Facebook…)

5. Phương pháp xác thực API.

- xác thực HTTP cơ bản : thực hiện xác thực qua các http header khi người dùng cung cấp account vào trong yêu cầu.

- API keys : là 1 khoá định danh để cho thấy ai dang sử dụng account đó bằng API key.Khi người dùng đăng nhập lại sử dụng key duy nhất để để chứng minh rằng đó là chính chủ.

- Oauth 2.0 : sử dụng account của mình do của bên thứ 3 để xác minh.1

6. Giao thức xác thực.

- Kerberos : sử dụng mật mã khoá đối xứng và 1 trung tâm phân phối khoá (key Distribution Center - KDC).

- LDAP : là 1 giao thức ứng dụng mở , tập trung cung cấp lưu trữ người dùng , mật khẩu, địa chỉ email, , kết nối máy in và dữ liệu tĩnh khác trong thư mục nhằm duy trì dữ liệu và truy cập.

- Oauth2.0(open authentication): là việc mà xác thực qua bên thứ 3 và uỷ quyền mà không lấy các thông tin đăng nhập của người dùng

- Remote authentication dial-in user services (RADIUS) :

- SAML : Giao thức dựa trên XML này trao đổi dữ liệu xác thực giữa IdP và nhà cung cấp dịch vụ.

- giao thực xác thức bắt tay thử thách (CHAP) : thực hiện như bắt tay 3 bước gửi yêu cầu xác thực và trả về để xác thực thực và trả lại kết quả.

- DIAMETER :

- giao thức xác thực mở rộng (EAP) : sử dụng nhiều ở mạng không dây và kết nối point to point.

- giao thức xác thực mật khẩu (PAP) : xác thực bằng những yếu tố kiến thức nhưng không được mã hoá như CHAP.

- TACACS : thực hiện xác thực dữa trên IP trên hệ thống.