SEGURANÇA DA INFORMAÇÃO

Mecanismos de Autenticação

ROTEIRO

- Conceitos básicos
- Usuários e grupos
- Estratégias de autenticação
- Técnicas biométricas
- Estruturas de autenticação

CONCEITOS BÁSICOS

A autenticação prova a identidade de diversas entidades do sistema computacional

Objetivos

- Identificar usuários para o sistema
- Identificar sistema para os usuários
- Identificar sistemas para outros sistemas
- Garantir a origem de uma aplicação etc.

CONCEITOS BÁSICOS

Etapas de autenticação em um servidor

Autenticação no servidor

- Login (inicia a sessão do usuário)
- Autenticação do cliente
- Criação de processos
- Utilizar os sistemas criados pelos processos
- Finalizar a sessão do usuário (Logout)

CONCEITOS BÁSICOS

No Linux, os Ids do usuários (UID) ficam registrados em */etc/passwd*

Utilizamos o ID para rotular

- Entidades
  - Processos, threads etc.
- Recursos
  - Impressoras, arquivos etc.

CONCEITOS BÁSICOS

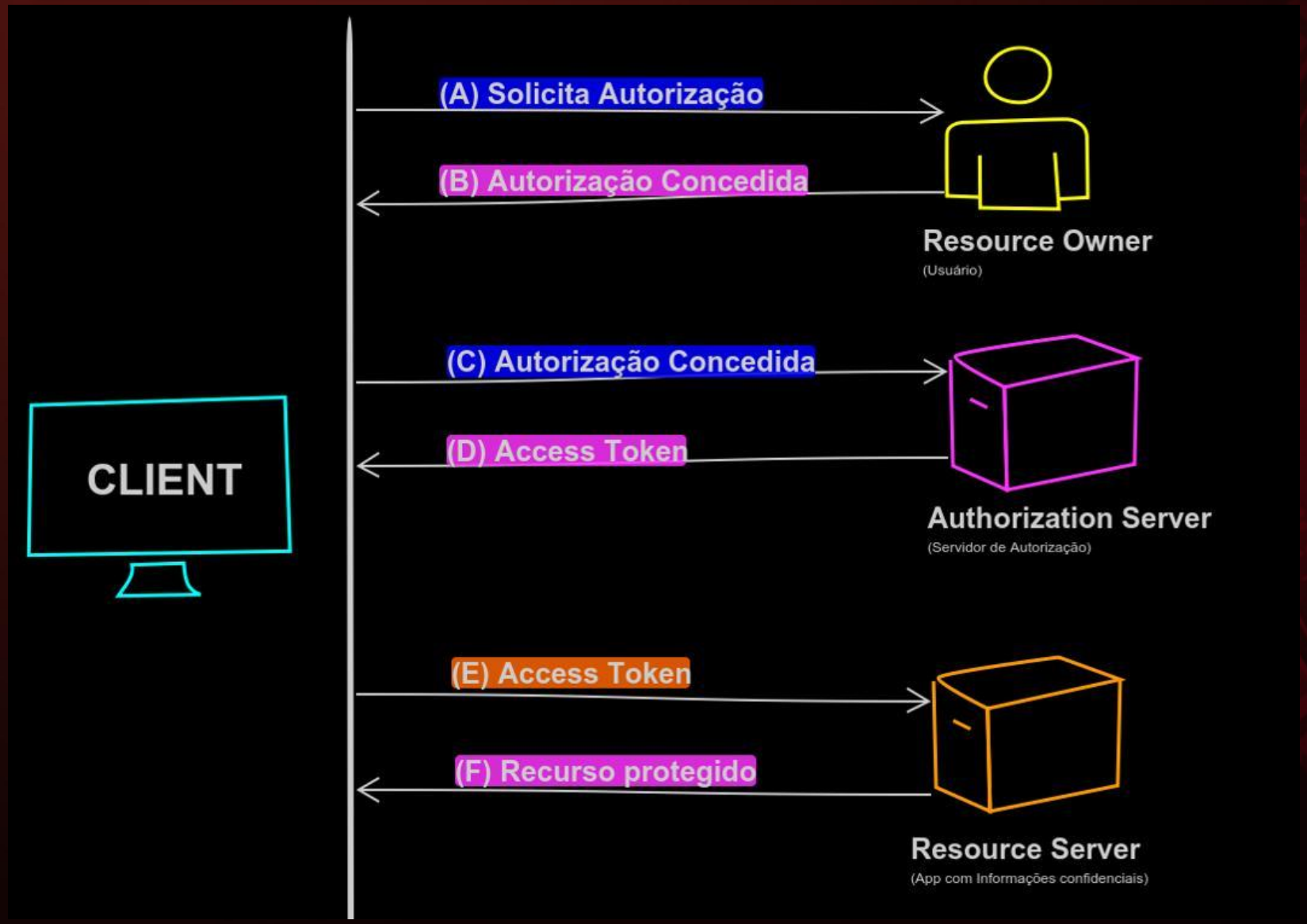
Usuários também podem ser organizados em grupos

GID (*Group Identifier*)

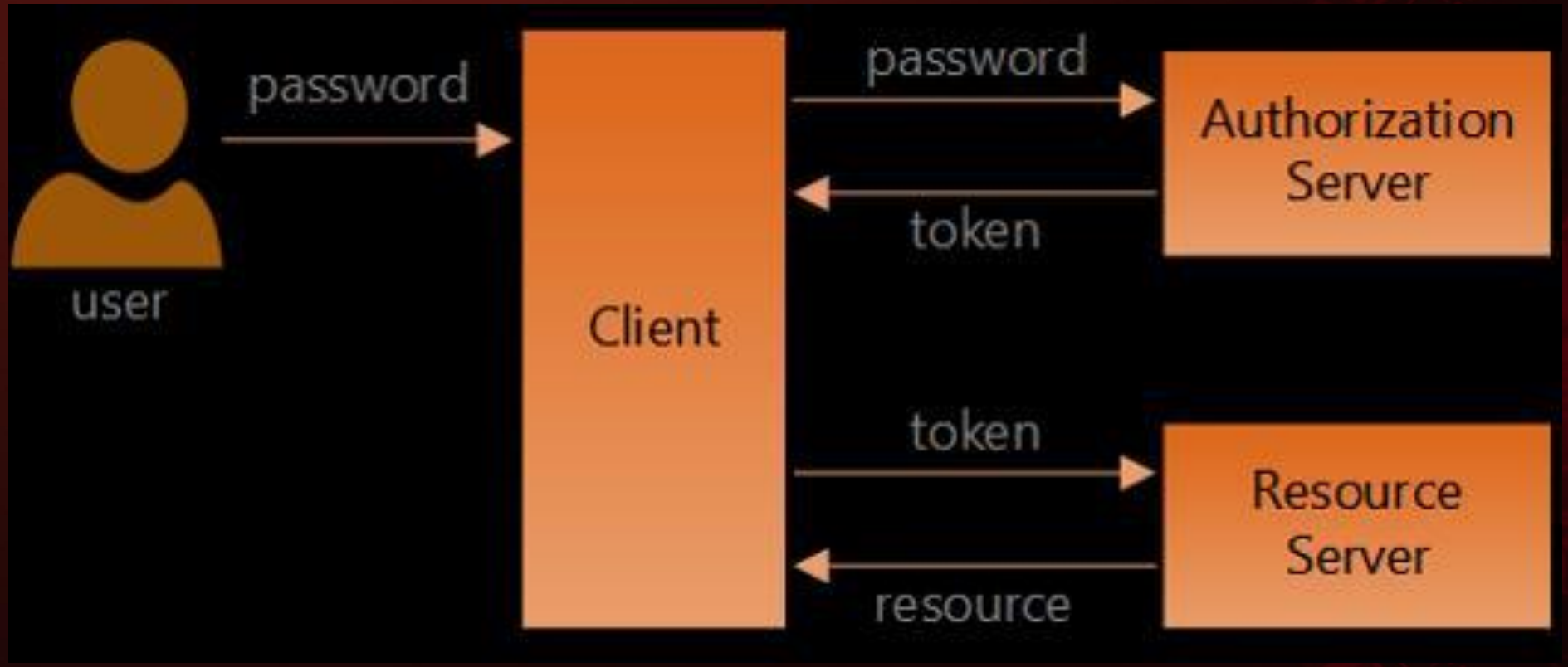
- **/etc/group**

Um usuário pode pertencer a mais de um grupo

FLUXO GERAL


(A) Solicita Autorização
(B) Autorização Concedida
Resource Owner
(Usuário)
(C) Autorização Concedida
CLIENT
(D) Access Token
Authorization Server
(Servidor de Autorização)
(E) Access Token
(F) Recurso protegido
Resource Server
(App com Informações confidenciais)

FLUXO GERAL


password
user
Client
password
token
Authorization Server
token
resource
Resource Server

ESTRATÉGIAS DE AUTENTICAÇÃO

As estratégias de autenticação envolvem

Aquilo que você conhece	Aquilo que você tem	Aquilo que você é

ESTRATÉGIAS DE AUTENTICAÇÃO

AQUILO QUE VOCÊ CONHECE

O que é conhecido pelo usuário

Fácil de memorizar

É uma técnica de autenticação fraca, o que permite a informação ser roubada ou facilmente transferida

- Exemplo
  - Login/senha
  - PIN

ESTRATÉGIAS DE AUTENTICAÇÃO

AQUILO QUE VOCÊ TEM:

Informação mais complexa ou um dispositivo

Melhor que a técnica anterior

Problema
Um dispositivo material (cartão) pode ser roubado

- Exemplo:
  - Cartões, *tokens*
  - Chaves criptográficas
  - Certificados digitais

ESTRATÉGIAS DE AUTENTICAÇÃO

AQUILO QUE VOCÊ É:

Características intrínsecas do usuário

Biometria:

- Técnica mais complexa de implementar
- Considerada mais robusta que as anteriores

- Exemplo:
  - Dados biométricos

ESTRATÉGIAS DE AUTENTICAÇÃO

AUTENTICAÇÃO MULTIFATOR

Utilizar em conjunto as estratégias anteriores

Banco: senha + cartão

- Deve ser utilizado de forma racional

Muito utilizada em aplicações disponíveis na Internet

TÉCNICAS BIOMÉTRICAS

Utiliza as características biométricas, físicas ou comportamentais de um usuário para sua identificação única perante o sistema

FÍSICAS

- Impressão digital
- Padrão da Iris
- Geometria das mãos
- DNA

COMPORTAMENTAIS

- Som
- Padrão de voz

TÉCNICAS BIOMÉTRICAS

Alguns requisitos:

UNIVERSAL: deve estar presente em todos os indivíduos

SINGULAR (unicidade): dois usuários devem apresentar valores diferentes para a característica

PERMANÊNCIA: não deve mudar drasticamente no tempo

TÉCNICAS BIOMÉTRICAS

Alguns requisitos:

MENSURABILIDADE: deve ser mensurável

COLETA: pode ser medida por um dispositivo

ACEITAÇÃO: coleta bem aceita pelos indivíduos

SISTEMA BIOMÉTRICO

Sistema que utiliza a biometria para:

- Identificar um usuário
- Autenticar para comprovar sua identidade

É composto por:

SENSOR: captura os dados biométricos

EXTRATOR: extrai o que é relevante (características) dos dados coletados

COMPARADOR: compara as características coletadas com os dados armazenados

BANCO DE DADOS: registrar as informações biométricas

ESTRUTURA DE AUTENTICAÇÃO

OBJETIVO:

- Unificar bases de dados de usuários
- Modularizar os métodos de autenticação
- Tornar mais simples construir aplicações que requerem autenticação

FRAMEWORKS

- Faz com que as técnicas de autenticação sejam unificadas
  - Com os mesmos algoritmos e oferece uma interface de programação padronizada (homogênea)

ESTRUTURA DE AUTENTICAÇÃO

Exemplos de estruturas de autenticação

LOCAL

- PAM – *Pluggable Authentication Modules*
- XSSO – *X/Open Single Sign-On* (similar ao PAM)
- BSD Auth – usada no OpenBSD

EM REDE

- CHAP – *Challenge-Handshake Authentication Protocol*
- EAP – *Extensible Authentication Protocol*
- RADIUS – *Remote Authentication Dial In User Service*
- LDAP – *Lightweight Directory Access Protocol*

ESTRUTURA DE AUTENTICAÇÃO

NA INTERNET:

- **X.509**
- Open ID
- Kerberos
- SAML
- OATH

ESTRUTURA DE AUTENTICAÇÃO

NA INTERNET:

- Kerberos
  - Proposto nos anos 80 (MIT)
  - Centraliza a autenticação de serviços
    - Compartilhamento, login, etc.
    - Linux, Windows, Mac
  - Tickets são obtidos pelos usuários para:
    - Acessar serviços da rede
    - São cifrados com DES, 3DES, AES

REFERÊNCIAS

1. https://www.brunobrito.net.br/oauth2/
2. https://docs.microsoft.com/pt-br/aspnet/web-api/overview/security/individual-accounts-in-web-api
3. Criptografia e Segurança de Redes: Princípios e Práticas - Willian Stallings
4. https://pemtajo.github.io/a_autenticacao_de_dois_fatores_e_segura/