AUTENTICAÇÃO

AUTENTICAÇÃO DE USUÁRIO

Segundo a RFC 4949 (*Internet Security Glossary, Version* 2), autenticação de usuário é:

- O processo de verificação de uma identidade alegada por ou para uma entidade do sistema.

Obs.: Esse processo é conceituado como autenticação de usuário.

Consiste em duas etapas:

- **Identificação**

É o meio pelo qual um usuário provê uma identidade alegada ao sistema.

- **Autenticação**

É o meio para estabelecer a validade da alegação.

Meios de Autenticação

Há três meios de autenticação de usuário (usados isolados ou combinados)

- Sabe (Conhecimento) Ex.: senhas, etc.

5m

Ex.: Resposta a uma pergunta que foi previamente cadastrada.

- Tem (Objeto) Ex.: tokens, smart card, etc.

Ex.: Smart card – cartão inteligente utilizado para autenticar e liberar o acesso do indivíduo a um sistema ou a um local físico.

- É (Características) Ex.: biometria
  - Biometria estática – impressão digital, face, etc.
  - Biometria dinâmica – padrão de voz, ritmo de digitação, etc.

I – Autenticação baseada em senha

- Funciona a partir da identificação do usuário (ID) e sua senha associada.
- Autenticação baseada na comparação da senha informada com a senha previamente armazenada para o ID do usuário informado.

Obs.: O sistema irá comparar se a senha apresentada para um determinado ID corresponde a mesma senha que foi previamente cadastrada.

- Mantida em um arquivo de senhas do sistema.

O ID provê as seguintes formas de segurança:

- Determina se o usuário está autorizado a obter acesso ao sistema.
- Determina os privilégios concedidos ao usuário.

Obs.: O ID cadastrado faz referência ao que o indivíduo pode acessar no sistema.

- Usado no controle discricionário.

Vulnerabilidades de Senhas

Ataques e Contramedidas

10m

- Ataque a senha popular:
  - Teste de senha para os IDs.

Ex.: A matrícula de um usuário é: 3527.

No ataque à senha popular, o indivíduo irá colocar a matrícula do usuário e tentar várias senhas diferentes para tentar acessar o sistema.

Nesse caso, geralmente serão testadas senhas populares, ou seja, palavras que existem no dicionário, datas de nascimento, etc.

- Contramedidas: políticas para inibir a inclusão de senhas comuns.

- Exploração de Erros do Usuário:
  - Anotar a senha em post-its ou compartilhamento.
  - Contramedidas: treinamento do usuário.

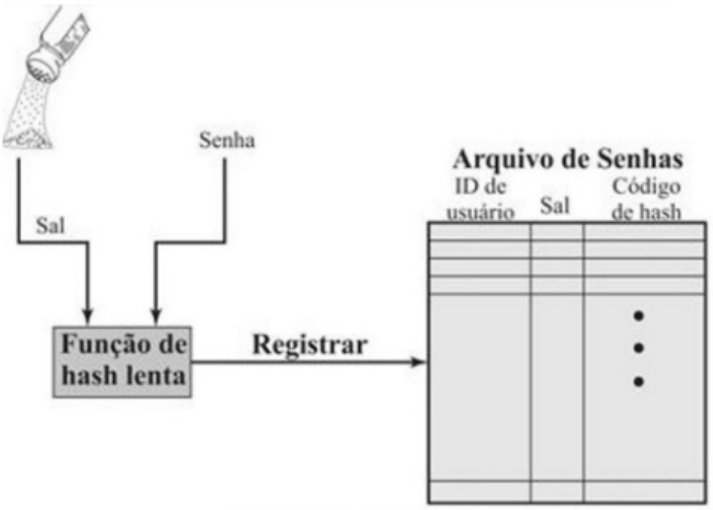
ANOTAÇÕES

- Sequestro de estação de trabalho:
  - Atacante aguarda que o usuário deixe a estação logada.
  - Contramedidas: bloqueio automático da estação de trabalho por inatividade.

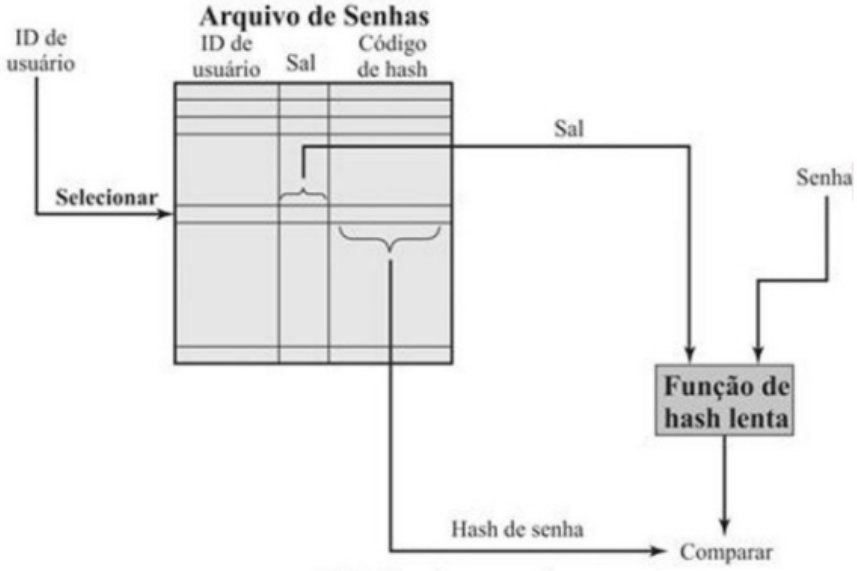
15m

Hash de Senhas

- Consiste no armazenamento dos hash de senhas para evitar ataques de criptoanálise.
- Aplica-se uma senha juntamente com um valor de salt (valor aleatório, não secreto) como entrada para um algoritmo de hash.
- Onde um valor de hash é produzido (execução lenta*).
- O hash de senha é armazenado juntamente com uma cópia em texto as claras do sal, no arquivo de senhas para o ID do usuário.



(a) Registrando nova senha



(b) Verificando uma senha

Obs.: Observa-se que o sal e a senha serão aplicados novamente na função hash, para que o resultado gerado seja comparado ao código de hash armazenado.

Tem três finalidades:

- Impedir a percepção de senhas duplicadas no arquivo de senhas.
- Dificultar ataques de dicionários off-line.
- Impossibilitar o descobrimento de usuários que utilizam a mesma senha em mais de um sistema.

20m

II – Autenticação Baseada em Token

Os objetos utilizados pelos usuários com a finalidade de autenticação são conhecidos por tokens.

São exemplos de tokens:

- Cartões de memória
- Smart Cards

III – Autenticação Biométrica

Baseada nas características físicas do usuário.

Comumente temos:

- Características faciais
- Impressões digitais
- Geometria da mão

Ex.: O Banco do Brasil utilizou por um tempo a autenticação baseada na geometria da mão.

- Padrão da retina
- Assinatura
- Voz

ANOTAÇÕES

IV – Autenticação Biométrica Dinâmica

- Baseada em um desafio gerado pelo sistema.
- A sequência de desafio consiste em uma sequência de números, caracteres ou palavras.
- Onde o usuário deverá falar, digitar ou escrever essa sequência, gerando um sinal biométrico.

Obs.: O sinal biométrico será cifrado e enviado como parâmetro para autenticação.

- Esse sinal é cifrado e enviado como parâmetro na autenticação.

EXERCÍCIOS DE FIXAÇÃO

1. (2019/IADES/AL/GO/Segurança da Informação)
Metodologias de autenticação envolvem três fatores básicos para autenticar um usuário, que são algo que o usuário
a. sabe; algo que o usuário tem; e algo que o usuário é.
b. quer; algo que o usuário tem; e algo que o usuário é.
c. sabe; algo que o usuário quer; e algo que o usuário é.
d. sabe; algo que o usuário tem; e algo que o usuário quer.
e. não sabe; algo que o usuário tem; e algo que o usuário quer.

COMENTÁRIO

25m

As metodologias de autenticação envolvem três fatores básicos para autenticar um usuário, que são algo que o usuário sabe, tem ou é.

Obs.: 2FA = faz referência ao uso de dois fatores de autenticação.

MFA = faz referência ao uso de múltiplos fatores de autenticação.

ANOTAÇÕES

2. (2020/CESPE/CEBRASPE/SEFAZ/AL/Auditor de Finanças e Controle de Arrecadação da Fazenda Estadual)

Julgue o próximo item, relativo à segurança da informação.

Identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades, como pré-requisito para permitir o acesso desses usuários ao sistema.

( ) Certo
( ) Errado

COMENTÁRIO

Identificação – usuário alega uma identidade
Autenticação – meio pelo qual essa identificação alegada é verificada.
A identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades para permitir o acesso desses usuários ao sistema.

GABARITO

1. a
2. C

ANOTAÇÕES