APRESENTAÇÃO

Segurança da Informação

Mecanismos de Autenticação

Prof. MSc. Jhonatan Geremias
jhonatan.geremias@pucpr.br

Autenticação

- Para a maioria dos contextos de segurança, a **Autenticação** é o mecanismo **essencial** utilizado como **defesa primária**.

Definição (RFC 2828→ RFC4949 pag 26)

- É o processo de **verificação** de uma **identidade alegada** por (ou para) uma entidade do sistema;
- É composta de duas etapas:
  - **Identificação**: Apresentação (alegação) de uma identidade ao sistema;
  - **Verificação**: Certificação da validade da alegação de identidade.

Norma ISO 27002 - identificação e autenticação

- A norma ISO 27002 fornece algumas diretrizes para orientar o processo de identificação e autenticação:
  - Todos os usuários devem ter um identificador único de uso pessoal e exclusivo, convém que uma técnica adequada de autenticação seja selecionada para validar a identidade dos usuários;
  - O controle de autenticação deve ser aplicado para todos os tipos de usuários, inclusive administradores do sistema e diretoria;
  - Os identificadores dos usuários devem ser utilizados para rastrear as atividades dos indivíduos. Como boas práticas as atividades regulares dos usuários não devem ser realizadas por meio de contas privilegiadas;

Norma ISO 27002 - identificação e autenticação

- Convém documentar qualquer tipo de circunstância excepcional que exija a utilização de identificador de usuário compartilhado por um grupo de pessoas;
  - Controles adicionais podem ser necessários para manter as responsabilidades dos indivíduos que vão utilizar este identificador;
- Identificadores genéricos para uso de um indivíduo só devem ser autorizados onde as ações executadas pelo usuário não precisam ser rastreadas, ou quando existem outros controles implementados para tal;
- Onde existe a necessidade de uma autenticação mais robusta métodos adicionais de autenticação são necessários;
  - Meios criptográficos, smart cards, tokens e mecanismos para autenticação biométrica.

Norma ISO 27002 - identificação e autenticação

- Convém que a força dos processos de identificação e autenticação sejam proporcionais a sensibilidade da informação que deve ser acessada.
  - Ideal que as senhas sejam protegidas utilizando meios criptográficos e protocolos de autenticação;
- Objetos como tokens podem ser utilizados para identificação e autenticação;
- Tecnologias de autenticação biométricas que usam características únicas de um indivíduo podem ser utilizadas para autenticar a identidade de um usuário;
- A combinação de diferentes tecnologias e mecanismos de segurança resultam em uma autenticação mais forte.

Implementação típica

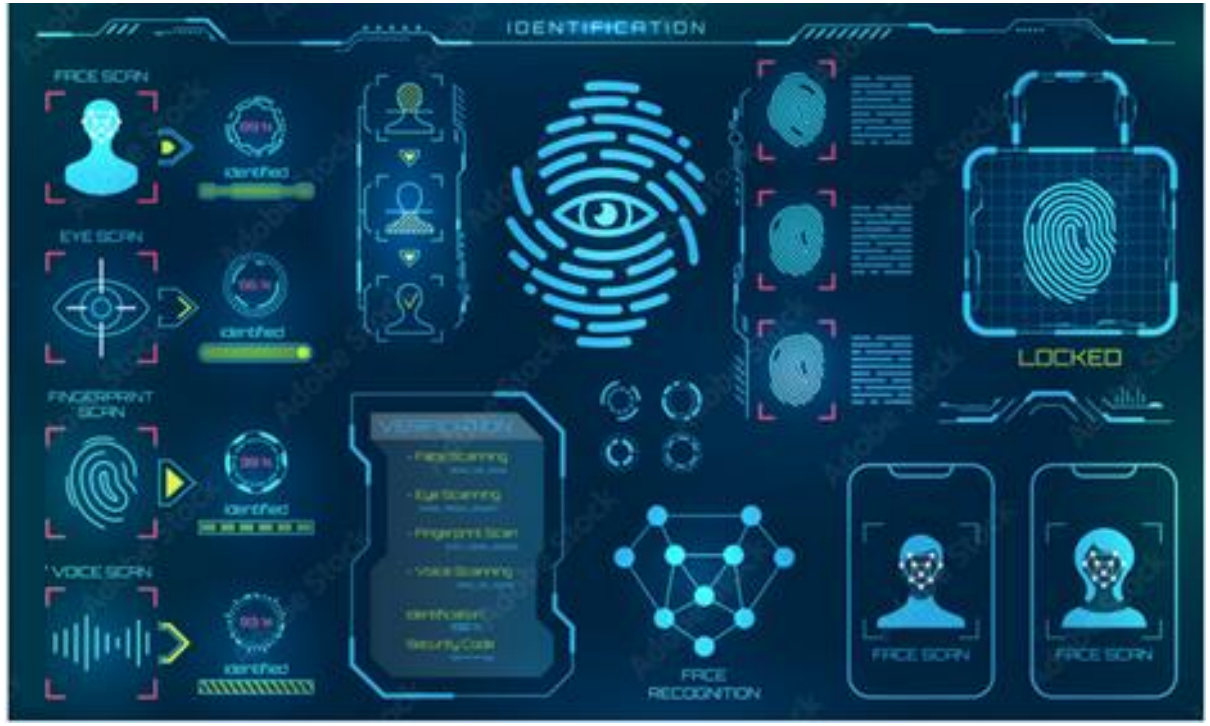
- Login + Senha
- Técnica **amplamente** utilizada quando se exige que um usuário não apresente apenas o seu identificador;
- Requer um ID único e uma senha associada;
- O sistema **compara** a senha **fornecida** com uma senha **previamente armazenada (ou hash)**, vinculada ao ID.

Exercício 01

- Desenvolva um programa que realize a autenticação de usuário.
- O programa deve armazenar previamente os ID de usuário e as senhas desses usuários.
  - O usuário deve entrar com o login e senha no programa
  - O programa deverá:
    - Imprimir na tela: “Bem vindo, usuário”, caso as credenciais estejam corretas.
    - Imprimir na tela: “Login ou senha incorreto, tente novamente mais tarde.”, caso as credenciais estejam incorretas.

Fatores de Autenticação

- Existem **quatro principais fatores** para autenticar a identidade de um usuário, que podem ser usados **isolados** ou **combinados**.



Fatores de Autenticação

1) **Algo que o indivíduo sabe**: baseado em algo que o usuário tem conhecimento;
   - Senhas;
   - Número de identificação pessoal (PIN);
   - Respostas a um conjunto de perguntas previamente arranjadas;
   - Desenhos e imagens;
2) **Algo que o indivíduo possui**: baseado em algo que o usuário tenha posse;
   - Cartões eletrônicos;
   - Smart Cards;
   - Chaves físicas;
   - Normalmente chamados de tokens;
   - Senhas descartável (OTP), por e-mail ou SMS.

Fatores de Autenticação

3. **Algo que o indivíduo é (biometria estática):** características físicas do indivíduo;
   - Impressão digital;
   - Leitura da Retina e Iris;
   - Reconhecimento Facial;
   - Geometria da palma da mão;
4. **Algo que o indivíduo é (biometria mecânica):** características comportamentais;
   - Padrão de voz;
   - Características de escrita;
   - Ritmo de digitação.

Novas técnicas de autenticação

- **Localização geográfica**: o usuário estar geograficamente em determinada localização, pode ser utilizado como fator de autenticação;
- **Proximidade**: cartões crédito e débito utilizando a tecnologia NFC;
  - *NFC - Near Field Communication:* comunicação por campo de proximidade;
  - Permite realizar o pagamento e troca de informações sem a necessidade de inserir o cartão e digitar a senha;
- **SQRL *(Secure, Quick, Reliable Login*) *:*** utiliza um QR code e um APP para autenticar a identidade de um usuário em sites remotos.

Problemas dos FA

- **Algo que o indivíduo sabe**:
  - Roubo, adivinhação, sequestro.
- **Algo que o indivíduo possui**:
  - Roubo ou falsificação.
- **Algo que o indivíduo é**:
  - Falso positivo/negativo, alto custo, conveniência.

Ataques contra o mecanismo de autenticação

- A autenticação é alvo frequente de ataques
- Entre os mais comuns:
  - Ataques de dicionário;
  - Ataque à conta específica;
  - Ataque à senha popular;
  - Adivinhação de senha contra usuário único;
  - Exploração de erros do usuário;
  - Monitoração eletrônica;
  - Exploração da reutilização de senhas.

Vulnerabilidades de senhas

- **Ataque de dicionário off-line**: Acesso ao arquivo de senha / hashs;
- **Contramedidas**:
  - Controles de acessos robustos;
  - Sistemas de detecção de intrusão;
  - Remissão de senhas (caso o arquivo seja comprometido);
  - Criptografia.

Vulnerabilidades de senhas

- **Ataque a uma conta específica**: Adversário visa uma conta específica e apresenta adivinhações de senhas até descobrir a correta;
- **Contramedida**:
  - Mecanismo de trava: bloqueia o acesso à conta depois de certa quantidade de tentativas malsucedidas (5 x, por exemplo).

Exercício 2

- Faça uma atualização no programa que realiza a autenticação do usuário com ID e Senha.
- Caso o usuário erre a senha por mais de 5 x, o programa deve bloquear o acesso do usuário ao sistema.

Vulnerabilidades de senhas

- **Ataque a senha popular**: Selecionar uma senha popular e testá-la em várias IDs;
- **Contramedida**: Inibir a definição de senhas comuns, monitorar IP em busca de padrões de pedido de autenticação.

Vulnerabilidades de senhas

- **Adivinhação de senha contra usuário único**: Adversário utiliza informações do detentor da conta e as políticas de senhas do sistema para adivinhar a senha;
- **Contramedidas**:
  - Políticas de senhas que determinem um comprimento mínimo e conjunto de caracteres;
  - Proibir a utilização de identificadores;
  - Estabelecer uma vida útil curta.

Vulnerabilidades de senhas

- **Sequestro de estação de trabalho**: Adversário espera até que uma estação na qual um usuário se autenticou fique desassistida;
- **Contramedidas**:
  - Bloqueio do acesso automático após um breve período de inatividade
  - Esquemas de detecção de intrusão baseados no comportamento do usuário.

Vulnerabilidades de senhas

- **Explorar erros do usuário**:
  - Se o sistema gerar a senha, é provável que o usuário anote;
  - Usuário compartilha a senha;
  - Técnicas de engenharia social (simular que é o gerente da conta bancária);
  - Sistemas com senhas padrões ou *default*;
- **Contramedidas**:
  - Política de segurança com responsabilização;
  - Capacitação do usuário.

Vulnerabilidades de senhas

- **Explorar reutilização de senhas**: Diferentes dispositivos compartilham a mesma senha ou uma senha semelhante;
- **Contramedida**: Políticas que proíbam a utilizam de senhas iguais ou semelhantes.

Vulnerabilidades de senhas

- **Monitoração Eletrônica**: Se uma senha for comunicada por meio da rede, ela pode ser interceptada;
- **Contramedidas**:
  - Criptografia;
  - Capacitação do usuário.

Abordagem para quebrar a senha

- Uso de um **grande dicionário** de senhas possíveis, incluindo grafia de palavras de **trás para frente**, **números** ou **caracteres especiais**;
- O adversário procura encontrar uma **correspondência**, testando cada um dos valores.

Escolha de senha pelo usuário

- Alguns usuários, quando podem escolher sua própria senha, escolhem uma senha **absurdamente curta**;
- Os resultados realizados na *Purdue University* mostram que 3% dos usuários escolheram uma senha com **três ou menos** caracteres de comprimento.

Escolha de senha pelo usuário

Comprimento	Número	Fração do total
1	55	0,004
2	87	0,006
3	212	0,02
4	449	0,03
5	1.260	0,09
6	3.035	0,22
7	2.917	0,21
8	5.772	0,42
Total	13.787	1,0

Escolha de senha pelo usuário

- O comprimento da senha é apenas parte do problema;
- Alguns usuários escolhem uma senha **muito fácil**, como o próprio nome, nome da rua, palavras comuns do dicionário;
- **Facilita** a quebra de senha, como mostra o estudo de Klei em uma base de **14 mil** senhas.

Escolha de senha pelo usuário

Tipo de senha	Tamanho da busca	Número de correspondências	Porcentagem de senhas correspondentes
Nome de usuário/conta	130	368	2,7%
Sequências de caracteres	866	22	0,2%
Números	427	9	0,1%
Em chinês	392	56	0,4%
Nomes de lugares	628	82	0,6%
Nomes comuns	2.239		4,0%
Nomes de mulher	4.280		1,2%
Nomes de homem	2.866		1,0%
Nomes incomuns	4.955		0,9%
Mitos e lendas	1.246	66	0,5%
Shakespearianas	473	11	0,1%
Termos de esporte	238	32	0,2%
Ficção científica	691	59	0,4%
Filmes e atores	99	12	0,1%
Desenhos animados	92	9	0,1%
Pessoas famosas	290	55	0,4%
Frases e padrões	933	253	1,8%
Sobrenomes	33	9	0,1%

24% de sucesso

Estratégia de seleção de senha

- Em resumo, se não forem obrigados, muitos usuários escolhem uma senha **curta ou fácil**;
- Se o sistema gerar uma senha composta de 8 **caracteres aleatórios**, a quebra de *hash* será praticamente **impossível**;
- Mas também será quase impossível o usuário **lembrar** da senha sem anotá-la;
- Como **eliminar** senhas fáceis e permitir que o usuário tenha uma senha **memorizável**?

Requisitos para seleção de senha

- Definição de políticas de senhas avaliando os requisitos de complexidade ;
  - Letras maiúsculas (A à Z);
  - Letras minúsculas (a à z);
  - Dígitos (0 a 9);
  - Caracteres especiais (caracteres não alfanuméricos): (~! @ #$%^&*_-+='|\() {} []:;"' <>,.? /);
- Definição de senha com no mínimo 8 caracteres:
  - Garante que existam cerca de 218.340.105.584.896 possibilidades diferentes;
  - Dificulta bastante um ataque de força bruta.

Estratégia de seleção de senha (cont.)

- Existem quatro técnicas:
  - Educação do usuário;
  - Senhas geradas por computador;
  - Verificação reativa da senha;
  - Verificação proativa da senha.

Educação do Usuário

- Informar o usuário da **importância** de usar senhas difíceis de adivinhar e dar-lhe diretrizes para selecionar senhas fortes;
  - Não é bem sucedida: muitos usuários **ignoram** as **diretrizes** ou não sabem julgar o que é uma senha **forte**;
- **Exemplo de técnica**: Usar a primeira letra de cada palavra em uma frase;
  - **Frase**: Segurança é a melhor disciplina do curso;
  - **Senha**: Seamddc.

Senha gerada por computador

- Baixa aceitação pelos usuários;
- O algoritmo **FIPS PUB 181** define um dos mais bem projetados geradores de senhas automatizados;
  - Gera **silabas pronunciáveis**, concatenando-as para formar uma palavra.

Verificação reativa de senha

- Sistema verifica **periodicamente** a si próprio, tentando quebrar as senhas fáceis de adivinhar;
- Quando consegue sucesso, **bloqueia o acesso** e **notifica** o usuário;
- Problemas:
  - Alto consumo de recursos;
  - Senha fácil fica vulnerável até o sistema detectar.

Verificação proativa de senha

- Permite que o usuário **defina a própria senha**, entretanto o sistema verifica se a senha é aceitável ou não;
- Segue a filosofia: com orientação suficiente, o usuário pode **selecionar** a senha **memorizável** seguindo alguns **critérios**;
- Objetivo é um **equilíbrio** entre a aceitabilidade pelo usuário e a força da senha.

Autenticação Multifator

- A autenticação multifator é uma técnica onde o sistema pode implementar mais de um fator de autenticação para certificar as credenciais dos usuários;
- A combinação de diferentes tecnologias permite obter um mecanismo de autenticação mais robusto;
  - Para fortalecer o procedimento de autenticação podemos associar mais de um fator de autenticação.
  - Baseado nos quatro fatores básicos de autenticação:
    - O que o indivíduo sabe;
    - O que ele possui;
    - Características físicas;
    - Características comportamentais.

Obrigado!

Jhonatan Geremias (elaboração)

Jhonatan.geremias@pucpr.br

Gonzaga (revisão / atualização)

luis.gonzaga@pucpr.br

SCIENTIA, VITA ET FIDES

PUCPR

GRUPO MARISTA