INSTITUTO FEDERAL
PIAUÍ

Autenticação de Usuários

SEGURANÇA DA INFORMAÇÃO

Prof. Silvino Marques
silvinomarques@ifpi.edu.br

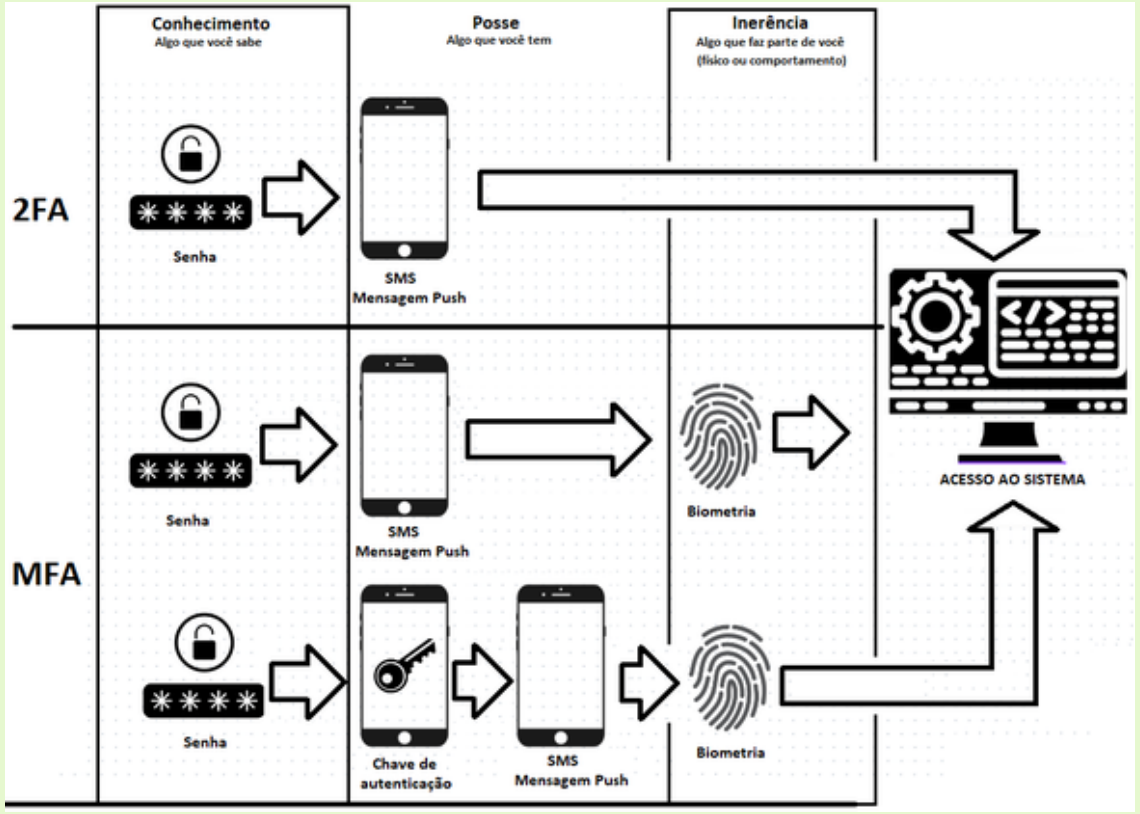
Introdução

- Na maioria dos contextos de segurança de computadores, a autenticação de usuários é a pedra fundamental e a linha de defesa primária.
- A autenticação de usuários é a base para grande parte dos tipos de **controle de acesso** e para a **responsabilização** do usuário.

Meios de Autenticação

- Há quatro meios gerais de autenticar a identidade de um usuário, que podem ser usados sozinhos ou combinados:
  - **Algo que o indivíduo conhece ou sabe:**
    - Entre os exemplos temos uma senha, um número de identificação pessoal (PIN) ou respostas a um conjunto de perguntas previamente arranjado.
  - **Algo que o indivíduo possui:**
    - Exemplos incluem cartões eletrônicos com senhas, *smart cards* e chaves físicas. Esse tipo de autenticador é denominado ***token***.
  - **Algo que o indivíduo é (biometria estática):**
    - Entre os exemplos citamos o reconhecimento por impressão digital, retina e face.
  - **Algo que o indivíduo faz (biometria dinâmica):**
    - Exemplos incluem reconhecimento por padrão de voz, características de escrita e ritmo de digitação.

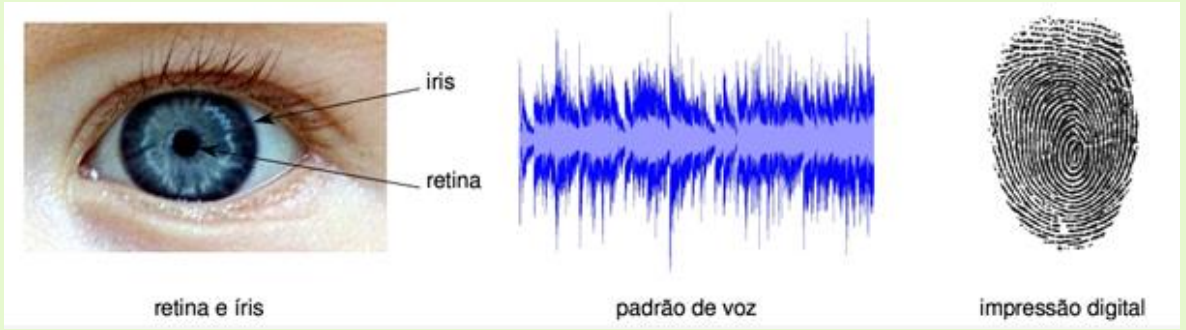
Autenticação Multifator



Segundo relatório de dicas para prevenção de comprometimento de senhas (*OWASP CHEAT SHEET SERIES*, s.d.), **99,9%** dos ataques relacionados a senha cessam com o uso de múltiplos fatores de autenticação.

Biometria

- Uso de características físicas para autenticação
  - Universalidade – Todos usuários devem ter.
  - Singularidade – Dois indivíduos distintos devem sempre ter valores distintos.
  - Permanência – Não pode mudar abruptamente com a passagem do tempo.
  - Mensurabilidade – Deve ser medida em termos quantitativos.
- Características físicas (DNA, Íris, Digital) ou comportamentais (voz, dinâmica de digitação).
- Podem ser autenticadores (usuário se identifica e usa biometria como senha) ou identificadores (pessoa é identificada pela biometria).



Senhas

- A configuração malfeita mais básica que existe são senhas fracas e raramente trocadas (especialmente se for uma senha padrão, como veremos a seguir).
- Não é necessário instalar cavalos de tróia ou explorar falhas em um sistema que é mal configurado.
  - Só esse fator já é suficiente para que ele seja invadido ou tenha seus dados roubados.

Senhas Fáceis

- Nunca devemos deixar uma conta de usuário ou algum outro serviço que dependa de autenticação sem senha. Os invasores podem se aproveitar disso.
- Mas também não adianta colocar senhas fáceis.

Senhas Fáceis

Evite usar:

- dados pessoais
  - nome, sobrenome
  - contas de usuário
  - datas
  - números de documentos, de telefones ou de placas de carros
- dados disponíveis em redes sociais e páginas *Web*
- sequências de teclado
  - “1qaz2wsx”, “QwerTAsdfG”
- palavras presentes em listas publicamente conhecidas
  - músicas, times de futebol
  - personagens de filmes
  - dicionários de diferentes idiomas

Senhas Fáceis

- Algumas pessoas acham que, pelo fato de misturarem essas senhas fracas com um número, estarão mais seguras.
- Vamos pegar o exemplo da senha marcelo. Será que ficaria bem mais seguro se colocássemos marcelo1?
  - O nível de risco é o mesmo, seja qual número for.
- Então, essa é uma prática que deve ser evitada.

Elaboração de senhas

Use:

- números aleatórios
  - quanto mais ao acaso forem os números melhor
    - principalmente em sistemas que aceitem exclusivamente caracteres numéricos
- grande quantidade de caracteres
  - quanto mais longa for a sua senha melhor
- diferentes tipos de caracteres
  - quanto mais “bagunçada” for a sua senha melhor

Elaboração de senhas

Dicas práticas para elaborar boas senhas:

- escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra

  Frase: “O Cravo brigou com a Rosa debaixo de uma sacada”

  Senha: “**?OCbcaRddus**”

- escolha uma frase longa, fácil de ser memorizada e com diferentes tipos de caracteres

  Senha: “**1 dia ainda verei os aneis de Saturno!!!**”

- invente um padrão de substituição próprio

  Padrão: substituir “o” por “0” e duplicar as letras “s” e “r”

  Frase: “Sol, astro-rei do Sistema Solar”

  Senha: “**SS0l, asstrr0-rrei d0 SSisstema SS0larr**”

Elaboração de senhas

- Como devemos então montar a nossa senha?
- Utilizando:
  - Letras maiúsculas e minúsculas;
  - Números;
  - Caracteres estendidos como /*+-*&@#{;
  - Tamanhos de no mínimo 10 caracteres.
- Uma senha segura seria algo como:
  - R7hU@Y*32!

Uso de Senhas

- Não exponha suas senhas;
- Não forneça suas senhas para outras pessoas;
- Use conexões seguras quando o acesso envolver senhas;
- Não use senhas de acesso profissional para acessar assuntos pessoais (e vice-versa);
- Crie grupos de senhas, de acordo com o risco envolvido;
- Armazene suas senhas de forma segura;
- Altere suas senhas (*imediatamente, rapidamente e regularmente*);

Recuperação de senhas

Configure opções de recuperação de senhas:

- um endereço de *e-mail* alternativo
- uma pergunta de segurança
- uma dica de segurança
- um número de telefone celular

Ao usar perguntas de segurança:

- evite escolher questões cujas respostas sejam facilmente adivinhadas
- procure criar suas próprias questões
  - de preferência com respostas falsas

Senha Padrão

- Senha padrão geralmente são encontradas em dispositivos de rede como roteadores, sistemas operacionais e serviços de rede.
- O problema é que essas informações são comumente divulgadas na Internet;
  - Qualquer pessoa que conseguir identificar o seu dispositivo poderá se conectar a ele e ter total acesso.

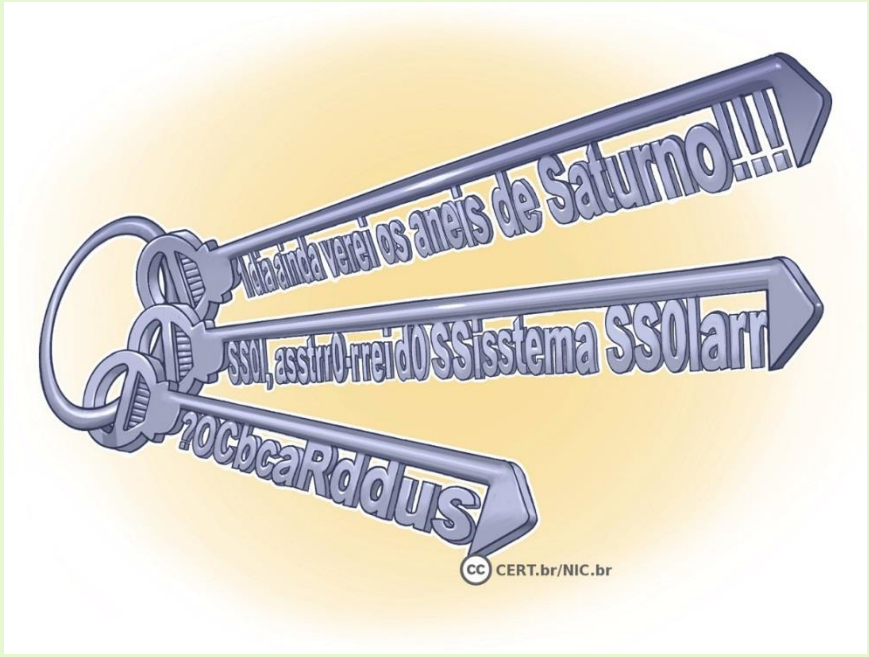
Senha Padrão

Usuário	Senha
admin	senha em branco
admin	admin
admin	1234
Admin	Admin
Admin	senha em branco
usuário em branco	senha em branco

Descobrindo Senhas

Métodos existem diversos, mas vou tentar padronizá-los e dividir por categorias. Você vê, a seguir, alguns tipos:

- Password Guessing: O famoso “chute”.
- Engenharia Social
- Keyloggers
- Força-Bruta
- Ataque de dicionários
- Sniffers
- Man in the middle



Outras Técnicas de Senhas

- Além das tradicionais, existem algumas outras técnicas interessantes para conseguir descobrir ou pelo menos mudar a senha existente nos sistemas.
- Claro que, para funcionarem, você precisa estar localmente no computador ou dispositivo
  - Resetando manualmente;
  - Boot por USB;

Possíveis Soluções

- Configure corretamente o seu sistema. Esteja atento para configurações de senhas, force os usuários a utilizarem senhas com, no mínimo, oito caracteres e misturando letras e números.
- Faça com que o sistema peça a troca dessa senha em, no máximo, seis meses (o ideal é três).
- Também bloqueie a conta do usuário após três tentativas inválidas para evitar os ataques de força-bruta.

Possíveis Soluções

- Evite salvar suas senhas no navegador Web;
- Evite usar opções como: “Lembre-se de mim” e “Continuar Conectado”;
- Evite usar a mesma senha para todos os serviços que você acessa;

Possíveis Soluções

- Utilize serviços criptografados na rede para evitar o sniffing (farejamento).
- Prefira SSH em vez de Telnet, SFTP em vez de FTP comum e por aí vai.
- Não permita que os usuários locais consigam dar boot no sistema por CD. Se isso acontecer, eles poderão facilmente resetar a senha administrativa do sistema.

Referências Bibliográficas

Segurança de computadores : princípios e práticas / William Stallings, Lawrie Brown. 2. ed. - Rio de Janeiro : Elsevier, 2014

Segredos do Hacker Ético - Marcos Flávio Araújo Assunção. São Paulo, SP, Brasil. 2008.

Fascículo Senhas

https://cartilha.cert.br/fasciculos/