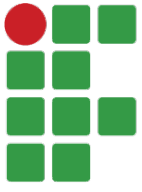
Fatores de Autenticação

Segurança Computacional

Ricardo de la Rocha Ladeira
{ricardo.ladeira@ifc.edu.br}



INSTITUTO FEDERAL
Catarinense
Campus Blumenau

Introdução

- Entrar em uma sala para fazer o ENEM.
- Acessar a conta de e-mail.
- Acessar a conta de uma rede social.
- Realizar operações bancárias, tais como imprimir extrato e transferir valores.

- O que todas essas ações têm em comum?

Introdução

- Entrar em uma sala para fazer o ENEM.
- Acessar a conta de e-mail.
- Acessar a conta de uma rede social.
- Realizar operações bancárias, tais como imprimir extrato e transferir valores.

- O que todas essas ações têm em comum?

- Em todas elas é necessário que ocorra antes uma verificação de identidade seguida de uma autorização.

Fatores de Autenticação

- Esta verificação de identidade é realizada a partir do fornecimento de alguma informação.

- A informação utilizada para isso faz parte de alguma categoria de credenciais utilizadas para conceder a permissão de acesso a algum recurso. Essas categorias são ditas **fatores de autenticação**.

- O que o usuário **sabe**: PIN, senha, pergunta secreta.
- O que o usuário **tem**: documento, token, cartão inteligente.
- O que o usuário **é**: retina, íris, rosto, caminhar, digital, forma de digitar (TypingDNA).

Fatores de Autenticação

- Também podem ser encontrados na literatura como fatores de
  - **conhecimento**
  - **posse**
  - **inerência**

Fatores de Autenticação

- Quanto mais fatores de autenticação utilizados, melhor!
- Que fatores de autenticação são utilizados fora do meio virtual? Pense, por exemplo, no ENEM. Que permissões o candidato precisa? Como ele se autentica?

Fatores de Autenticação

- Quanto mais fatores de autenticação utilizados, melhor!
- Bancos exigem o uso do cartão e do escaneamento da digital no leitor biométrico.
  - Neste caso, combinam dois fatores de autenticação. Quais?

Fatores de Autenticação

- Quanto mais fatores de autenticação utilizados, melhor!
- Bancos exigem o uso do cartão e do escaneamento da digital no leitor biométrico.
  - Neste caso, combinam dois fatores de autenticação. Quais?
  - O que o usuário tem e o que o usuário é!
- Os terminais automáticos que ainda não têm leitor biométrico utilizam a senha e o cartão. Adicionalmente podem utilizar perguntas pessoais (nome da mãe, dígitos do CPF...)
  - Neste caso, que fatores de autenticação estão presentes?

Fatores de Autenticação

- Quanto mais fatores de autenticação utilizados, melhor!

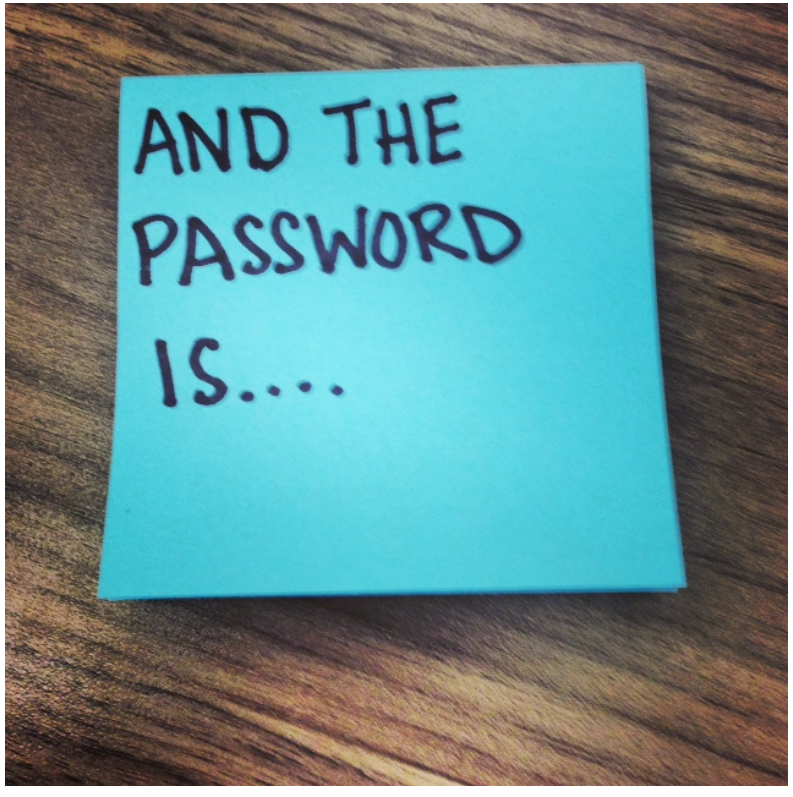
- Em *smartphones*, por exemplo, para ativação da autenticação por dois fatores[1], recomenda-se algum serviço de autenticação baseada em token (exemplo: **Google Authenticator**) ou outra forma disponível (biometria, reconhecimento facial etc) que **não seja o SMS**.
- O objetivo é evitar o golpe de **Chip Swap** (troca de chip), em que o golpista consegue acesso à linha do chip do celular da vítima e obtém acesso a serviços, inclusive com autenticação de dois fatores, via SMS.
  - Utilizar a opção por SMS em último caso (é melhor que não usar).
  - Em caso de comprometimento da linha, entrar em contato com a operadora e fazer Boletim de Ocorrência.

[1] A autenticação de 2 fatores também é conhecida como **2FA — Two Factor Authentication.**

Senhas

- E por que uma aula específica sobre senhas?

Senhas



Senhas

- Senha é todo código pré-definido que possibilita o reconhecimento do usuário para acesso a algum recurso.
- Exemplifica o fator de autenticação *"o que o usuário sabe"*.
- Tipicamente são classificadas em **fortes** e **fracas** em função da complexidade do seu descobrimento.

Senhas

Senha Fraca

- Senha fraca é a senha considerada óbvia.
- É aquela que pode ser adivinhada em poucas tentativas.
- Senhas óbvias (algumas):
  - seu nome
  - sua data de nascimento
  - número do seu telefone celular
  - nome de alguém ligado a você
  - seu ídolo
  - sequências numéricas
  - suas preferências (banda, estilo de música, filme, cor, time)...
  - combinações ingênuas (nome da mãe + ano de nascimento)

Senhas

Senha Fraca

- Pensando em um dicionário de senhas fracas (por exemplo, só com números)
- Quanto tempo você levaria para fazer um dicionário de
  - 1 dígito?
  - 2 dígitos?
  - 3 dígitos?
  - 4 dígitos?
  - 5 dígitos?
  - 6 dígitos?

Senhas

Senha Fraca

- Pensando em um dicionário de senhas fracas (por exemplo, só com números)
- Quanto tempo você levaria para fazer um dicionário de
  - 1 dígito?
  - 2 dígitos?
  - 3 dígitos?
  - 4 dígitos?
  - 5 dígitos?
  - 6 dígitos?
- `dicionario-de-numeros.sh`
- `dicionario-de-numeros.c`

Senhas

Senha Fraca

übergizmo Search this site Reviews Phones Computers Tutorials Events More

French Central Bank password was 123456 (really)

By Hubert Nguyen on 09/20/2012

A French citizen has unintentionally breached the security of the French central bank (Banque de France) over the phone and was freed by French authorities after being accused of “hacking” the central bank’s and triggering a 48-hours shut down of that particular computer system which handles the consumer indebtedness files (basically people who are flagged as having a very bad credit history).

Senhas

Senha Fraca

- As piores senhas:
- https://www.purevpn.com/blog/worst-password-list/
- https://www.strongpasswordgenerator.org/25-worst-passwords/
- https://www.ravepubs.com/exposing-the-most-vulnerable-passwords-of-2024/

- Boa leitura:
- https://www.csoonline.com/article/3526408/most-common-passwords.html

Senhas

Senha Fraca

- Alguns sistemas já impedem alguns tipos de senhas fracas.
- Mas há sistemas com outras restrições de senhas. Exemplo: máximo de 6 dígitos, todos numéricos.
- Neste caso, o recomendável é não utilizar sequências simples, datas, partes do número do telefone, da matrícula do carro, do CPF...

Senhas

Senha Fraca

- Pense na sua senha de e-mail. Ela pode ser considerada fraca?
- Pense nas suas senhas de redes sociais e cadastros de websites. Elas são fracas? Elas **podem** ser fracas?
- Algum tipo de senha pode ser fraca?

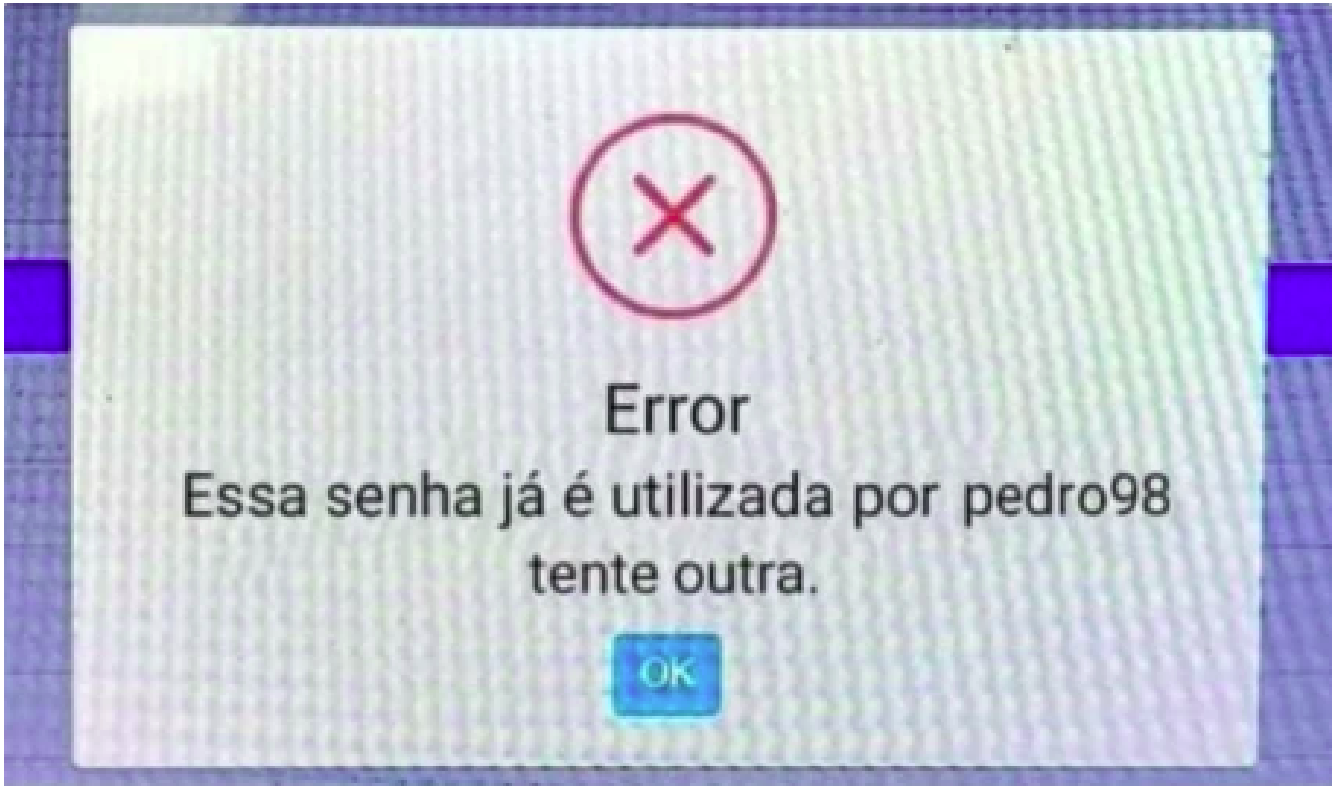
Senhas

Senha Fraca

- Adianta implementar um sistema seguro se os usuários usam senhas como '1234'?
- Você utiliza a mesma senha para acessar mais de um serviço?

Senhas

Senha Fraca

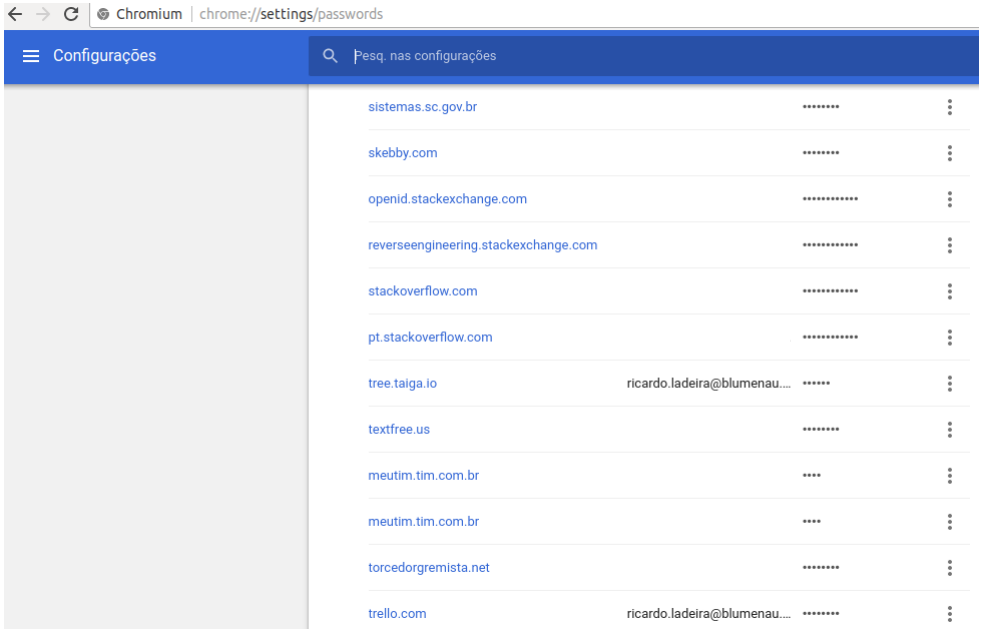


Senhas

Parênteses

- E adianta ter uma senha forte, mas um sistema de proteção fraco?

Figura: Armazenamento de Senhas do Google Chromium.

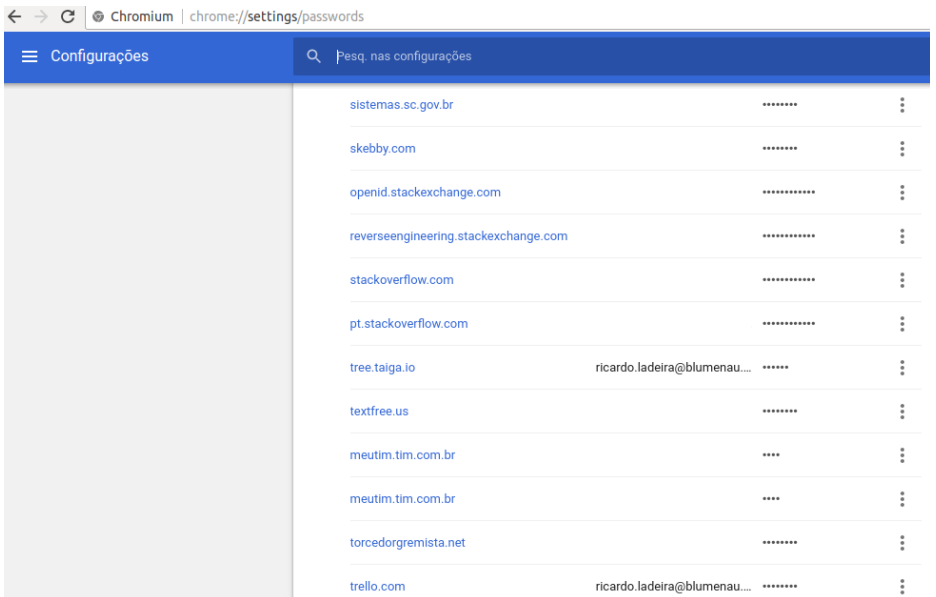


Senhas

Parênteses

- O acesso físico à máquina já compromete as senhas armazenadas no navegador!
  - Bom exemplo: senhas em sistemas Linux, no arquivo `/etc/shadow` (acesso somente com privilégio de administrador – `sudo`).

Figura: Armazenamento de Senhas do Google Chromium.



Senhas

Parênteses

- No Chrome: `chrome://password-manager/passwords`

Figura: Armazenamento de Senhas do Google Chrome.

Senhas

Parênteses

- Outros perigos
  - inspeção de elementos HTML antes de você usar o navegador
  - execução de *scripts* em máquinas públicas com sessão aberta
  - configuração de navegador para armazenamento de senhas
  - keyloggers e screenloggers
  - ...
- Mais motivos para que você não utilize serviços críticos de outros dispositivos além dos seus.
- Utilize navegação anônima em computadores públicos.
- Tenha seu próprio perfil de usuário!

Senhas

Senha Fraca

- Exemplos de senhas fracas:
  - Nirvana
  - 00000000
  - 1234567890
  - 123meunome
  - iloveyou
  - tricolor
  - blumenau
  - 32460000
  - solange1990
  - neymarjunior

Senhas

Senha Fraca

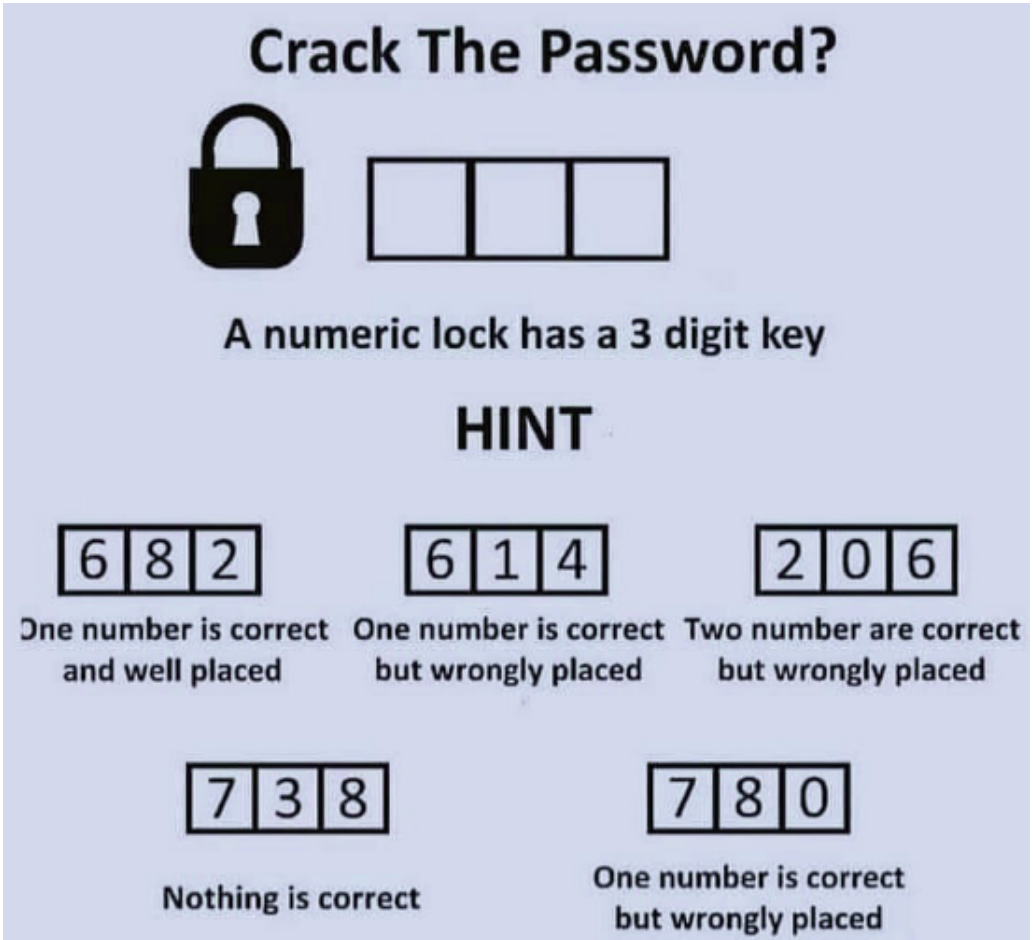


Figura: Qual é a senha?

Senhas

Senha Forte

Senhas

Senha Forte

- Senha considerada mais segura.

1. Deve ter o maior tamanho possível.
2. Deve utilizar, quando possível, uma combinação entre caracteres especiais (!@#%* ...), letras maiúsculas, minúsculas e números.

- Atualmente, considera-se o comprimento da senha mais importante que diversificar os tipos de caracteres. Assim, uma frase seria mais forte que uma senha menor que diversifica os tipos de caracteres. O NIST não exige mais a diversificação de tipos de caracteres.

Senhas

Senha Forte

- Exemplos de senhas com características de senhas fortes:
  -)*T11I#foM3+y)E%T
  - aFZG$9K)J5Vg
  - MpBI%T9LI%r
  - r2d4h6%9fr41
  - opodertendeacorrompereopoderabsolutocorrompeabsolutamente
- `https://www.betterbuys.com/estimating-password-cracking-times/`
- `https://www.useapassphrase.com/`

Senhas

Senha Forte

Figura: Senha forte.

Senhas

Senha Forte – como gerá-la e memorizá-la?

- Exemplo (Retirado da página da Microsoft):
- Crie uma sigla a partir de uma informação fácil de lembrar. Por exemplo, escolha uma frase significativa para você, como "Nascimento do meu filho é 12 de dezembro de 2004". Usando essa frase como guia, você pode usar `Nmfe12/Dez,4` como senha.

Senhas

Senha Forte – como gerá-la e memorizá-la?

- Exemplo (Retirado da página da Microsoft):
- Crie uma sigla a partir de uma informação fácil de lembrar. Por exemplo, escolha uma frase significativa para você, como "Nascimento do meu filho é 12 de dezembro de 2004". Usando essa frase como guia, você pode usar `Nmfe12/Dez,4` como senha.
- Quero utilizar esta senha para o meu e-mail. Ela é forte? Vocês me aconselhariam a fazer isso?

Senhas

Senha Forte – como gerá-la e memorizá-la?

- Substitua números, símbolos e ortografia incorreta por letras ou palavras em uma frase fácil de lembrar. Por exemplo, "Nascimento do meu filho é 12 de dezembro de 2004" pode se tornar `NasMe F1lhOeh 12124` (não é errado usar espaços na senha).
- Associe a senha a um hobby ou esporte predileto. Por exemplo, "Eu amo jogar badminton" pode ser `4m0Jo6arB@dm1nt()n`.

Senhas

Senha Forte

- Links com geradores e verificadores de senhas fortes:
- `http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/01/geradores-online-ajudam-criar-senhas-seguras-para-usar-na-internet.html`
- `https://howsecureismypassword.net/`

Senhas

Senha Forte

- Tenho uma senha forte. Estou protegido?

Senhas

Senha Forte

- Tenho uma senha forte. Estou protegido?

- Não. A senha forte não é garantia de proteção, mas traz mais dificuldade para quem tenta obtê-la.
- Senhas fracas provavelmente estarão em arquivos de dicionário (listas de palavras), muito usados em ataques de força bruta para o descobrimento de senhas.
  - Scripts `palhoca-antigo.php` e `palhoca-1.php`
- Mais fatores de autenticação, além da senha, garantem maior segurança. Exemplo: verificação em duas etapas, disponível para contas Google.

Senhas

Senha Forte

Outras ações:

- Senha diferente para cada serviço
- Gerenciador de senhas
  - zoho
  - keeper
  - LastPass
  - 1Password
  - ...
- Alterar as senhas sempre que (ou somente quando) houver suspeita de vazamento.

Senhas

Senha Forte

- Segundo as mais recentes diretrizes do NIST (2020):
  - Exija que todos usem senhas de 15 ou mais caracteres sem exigir caracteres maiúsculos, minúsculos ou especiais;
  - Exija apenas alterações de senha quando houver um motivo para acreditar que houve comprometimento;
  - Seus administradores de rede devem examinar as senhas de todos em relação às listas de palavras do dicionário e senhas que se sabe terem sido comprometidas;
  - Para ajudar a impedir um ataque de negação de serviço ao seu serviço de e-mail, não bloqueie a conta de um usuário após um número x de tentativas incorretas de login. Dessa forma, mesmo se um adversário inundar sua rede com informações de login propositadamente incorretas, os usuários não serão bloqueados nas contas deles;
  - Não permita "dicas" de senha.

Senhas

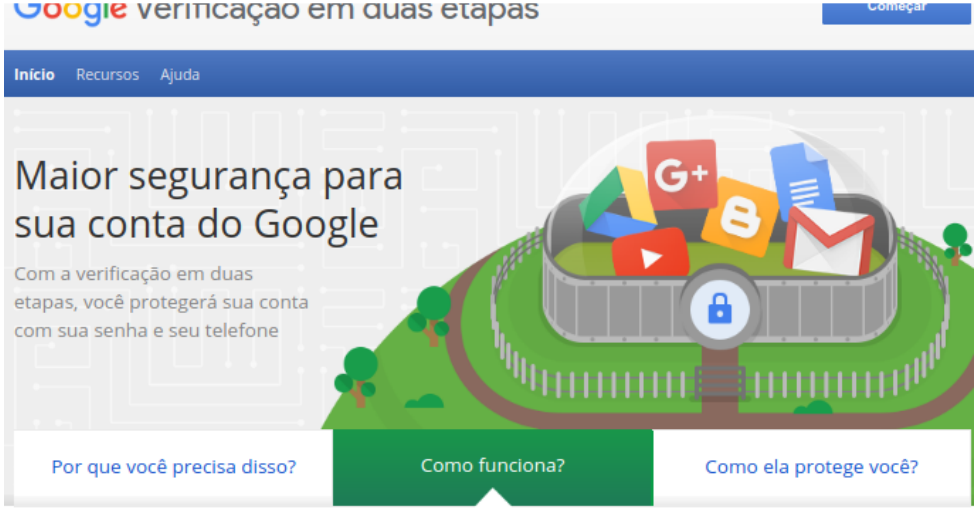
Senha Forte

- A expressão ***password*** (palavra de acesso) tem caído em desuso gradativamente e vem dando lugar à expressão ***passphrase*** (frase de acesso).

- Considerando que as senhas estão ficando cada vez mais longas e parecidas com frases, começa a fazer mais sentido o uso da expressão ***passphrase***.

Senhas

Senha Forte



O login em sua conta será um pouco diferente

1 **Você digita sua senha**
Sempre que fizer login no Google, você digitará sua senha como de costume.

2 **Outra informação é solicitada**
Em seguida, um código é enviado para seu smartphone por meio de mensagem de texto, chamada de voz ou por nosso app para dispositivo móvel. Ou, se você tem uma chave de segurança, pode inseri-la na porta USB do seu computador.

Senhas

Entropia

- **Entropia**, em termos gerais, é uma medida de **imprevisibilidade** de um sistema.
- No contexto da Segurança Computacional, entropia é uma medida de força de senha contra ataques de adivinhação e força bruta.
- O cálculo da entropia procura responder o quão imprevisível é a senha elaborada e envolve o tamanho da senha e o conjunto de caracteres possíveis para formulá-la.

Senhas

Entropia

- A entropia é uma medida calculada em ***bits***.
  - Quando uma senha já é conhecida, sua entropia é 0 *bits*.
  - Quando uma senha precisa, **em média**, de uma tentativa para ser descoberta, diz-se que sua entropia é 1 *bit*[2].
- O cálculo da entropia é feito através do logaritmo de base 2 do total de caracteres possíveis para se utilizar na senha multiplicado pelo tamanho da senha:
  - $L * \log_2(R)$
    - L = Comprimento da senha
    - R = Total de símbolos disponíveis no conjunto utilizado

[2]Para adivinhar o valor deste *bit* temos duas possibilidades: 0 e 1. Na média, acertaremos 50% dos casos em uma tentativa, por isso a resposta é 1 *bit*.

Senhas

Entropia

- $L * \log_2(R)$
  - L = Comprimento da senha
  - R = Total de símbolos disponíveis no conjunto utilizado
- Suponha uma senha de oito dígitos em que os símbolos utilizados são os caracteres que representam letras minúsculas e maiúsculas.
- Neste caso, $L = 8$ e $R = 52$
  - $E = L * \log_2(R)$
  - $E = 8 * \log_2(52)$
  - $E = 8 * 5.70043972$
  - $E = 45.6035178$

Senhas

Entropia

- A quantidade ideal de *bits* depende da sensibilidade das informações que a senha protege. Além disso, as recomendações mínimas de quantidade de *bits* costuma aumentar ao longo dos anos, conforme aumenta também o poder computacional.
- O NIST define desde 2014 o mínimo de 112 *bits* para "segredos criptográficos" do governo e já estipulou a mudança para 128 *bits* a partir de 2030. O valor anterior era 80 *bits*.
  - `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf`

Senhas

Entropia

- Calculadoras de entropia:
  - `https://www.omnicalculator.com/other/password-entropy`
  - `https://apps.cygnius.net/passtest/`

- Note que uma senha com 30 dígitos numéricos apresenta entropia de 99.66 *bits*.
- A senha `Password123456789` apresenta entropia de 101.22 *bits*.

- Não se deve confiar cegamente na entropia. Ela deve servir apenas como um indicador para decidir a senha. A senha deve resistir a ataques de dicionário, portanto, combinações como `Password123456789` ou `12345qwertyQWERTY` não são adequadas.

Ferramentas de Quebra de Senhas

- Hydra
- Brutus
- Advanced rar password
- OPHCRACK
- Aircrack-ng
- John the Ripper
- Rainbow Crack
- WPBrute
- Biblioteca cURL
- ...

- E você pode fazer sua própria ferramenta!

Ferramentas de Quebra de Senhas

Hydra

- Disponível por linha de comando (`hydra`) ou com interface gráfica (`xhydra`).
- Software de força bruta.

Ferramentas de Quebra de Senhas

Hydra

- Exemplo:

- `hydra smtp.live.com smtp -l email@alvo.com -P 'dicionario.txt' -s 465 -S -v -V`

Exercícios

- Qual das senhas abaixo pode ser considerada forte?

a) `carlos1999`
b) `14051989`
c) `bandeira`
d) `321qwerty`
e) `meu!sonho!eh!criar!uma!senha!gigantesca#2021`

Exercícios

- Mas será que agora, após este exercício, esta senha continua forte?

a) `carlos1999`
b) `14051989`
c) `bandeira`
d) `321qwerty`
e) `meu!sonho!eh!criar!uma!senha!gigantesca#2021` ←

Exercícios

- Gere uma senha forte a partir de alguma frase de fácil memorização. Explique passo a passo como chegou na senha.
- Verifique no site https://howsecureismypassword.net/ (ou em https://www.useapassphrase.com/) se o tempo de descoberta da senha é alto o suficiente para que ela seja considerada forte.

Concluindo

- Opte sempre por senhas fortes e de tamanho grande.
- Procure não repetir a mesma senha para recursos diferentes. Se ela for descoberta, todos os recursos estarão vulneráveis.
- Utilize o máximo de caracteres diferentes (números, letras maiúsculas, minúsculas e caracteres especiais) que o sistema permite, desde que isso não interfira negativamente na memorização desta.
- Utilize uma ferramenta confiável de gerenciamento de senhas.

Concluindo

- Sempre que desconfiar que a senha está comprometida, altere-a.
- Lembre-se: quanto mais crítico for o recurso que a senha protege, mais forte ela deve ser.

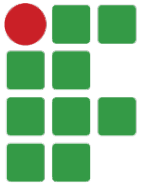
Referências e Sugestões de Leituras

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
- https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-with-passwords
- https://ibsec.com.br/10-ferramentas-de-quebra-de-senha-com-orientacoes-para-cibersegurança/
- http://www.ubergizmo.com/2012/09/french-central-bank-password/
- http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/01/geradores-online-ajudam-criar-senhas-seguras-para-usar-na-internet.html
- https://support.mozilla.org/pt-BR/kb/como-escolher-senhas-seguras

Fatores de Autenticação

Segurança Computacional

Ricardo de la Rocha Ladeira
{ricardo.ladeira@ifc.edu.br}



INSTITUTO FEDERAL
Catarinense
Campus Blumenau