Foto por **Rafael Pol** @ **Unsplash**

O QUE É UMA **SENHA FORTE** NA PRÁTICA?

RESUMO

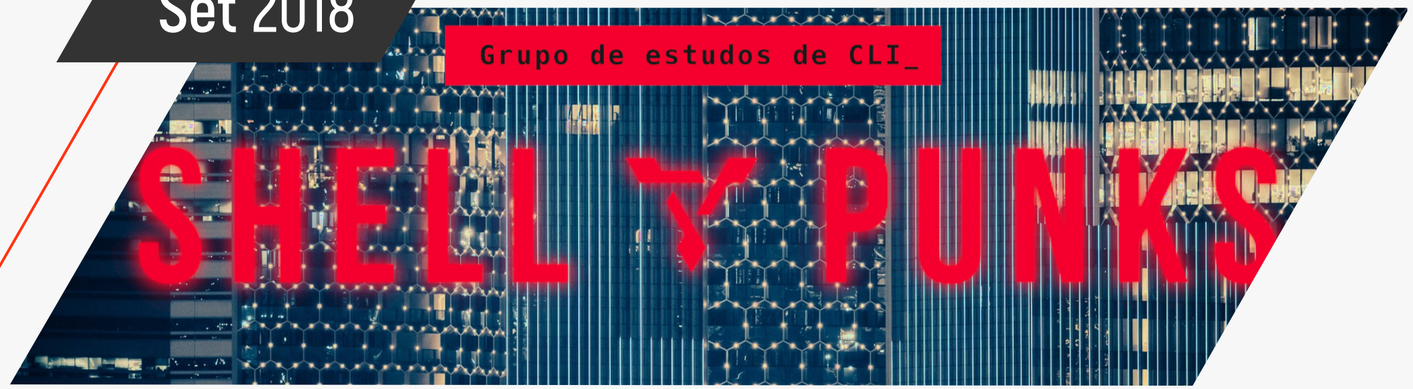
- **Introdução:** Autenticação por senha
- **Leaks:** Onde as senhas vivem
- **Hashes:** Como senhas são armazenadas
- **Cracking:** Como senhas são comprometidas
- **Diceware:** Como podemos nos proteger
- Conclusão
- Dúvidas

PARADIGMA.icu

Um **coletivo hacker** dedicado à pesquisa, desenvolvimento e aplicação de técnicas e tecnologias diversas para o fim de construir uma sociedade mais justa.

Organizamos encontros regulares para nos desenvolvermos no âmbito do software livre e segurança da informação, construindo conhecimento de maneira colaborativa

Set 2018



Nov 2018

AUTENTICAÇÃO POR SENHA

Foto por **Fancycrave @ Unsplash**

ONDE AS SENHAS VIVEM

Foto por **James Tarf** @ **Unsplash**

NÃO REUTILIZE SENHAS

COMO SENHAS SÃO ARMAZENADAS

COMO SENHAS SÃO ARMAZENADAS

- **Função hash:** Uma operação matemática onde um conjunto de informações qualquer é utilizado como referência para derivar uma **sequência de caracteres.** Este é um processo **irreversível.**

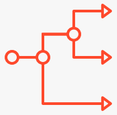
COMO SENHAS SÃO ARMAZENADAS

- **Função hash:** Uma operação matemática onde um conjunto de informações qualquer é utilizado como referência para derivar uma **sequência de caracteres.** Este é um processo **irreversível.**
- Funciona tal como um "código de barras" para verificar se a informação passada corresponde à aquela da qual se tem registro.

COMO SENHAS SÃO COMPROMETIDAS

COMO SENHAS SÃO COMPROMETIDAS

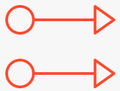
Ataque de dicionário, ou "direto"



Ataque regrado

Ataque combinatório

Ataque de força bruta



Ataque híbrido

COMO PODEMOS NOS PROTEGER?

COMO PODEMOS NOS PROTEGER?

- Diceware

COMO PODEMOS NOS PROTEGER?

- Diceware
- Palácio da Memória

COMO PODEMOS NOS PROTEGER?

- Diceware
- Palácio da Memória
- Quão forte seria esta senha?

COMO PODEMOS NOS PROTEGER?

Consideremos três
possíveis adversários:

Adversário	Hashes por segundo

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões
Jeremi M. Gosley	

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões
Jeremi M. Gosley	18×10^{10} = 180 bilhões

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões
Jeremi M. Gosley	18×10^{10} = 180 bilhões
A NSA	

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões
Jeremi M. Gosley	18×10^{10} = 180 bilhões
A NSA	10^{12} = 1 trilhão

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões
Jeremi M. Gosley	18×10^{10} = 180 bilhões
A NSA	10^{12} = 1 trilhão

Consideremos também:

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões
Jeremi M. Gosley	18×10^{10} = 180 bilhões
A NSA	10^{12} = 1 trilhão

Consideremos também:

- Você é o único alvo do seu adversário neste ataque.

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões
Jeremi M. Gosley	18×10^{10} = 180 bilhões
A NSA	10^{12} = 1 trilhão

Consideremos também:

- Você é o único alvo do seu adversário neste ataque.
- Ele **possui uma cópia do seu "dicionário"**, e portanto, irá utilizá-lo para quebrar sua senha.

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões
Jeremi M. Gosley	18×10^{10} = 180 bilhões
A NSA	10^{12} = 1 trilhão

Consideremos também:

- Você é o único alvo do seu adversário neste ataque.
- Ele **possui uma cópia do seu "dicionário"**, e portanto, irá utilizá-lo para quebrar sua senha.
- Ele sabe que você utilizou, conforme instruído, **exatamente 6 palavras** deste para compor sua senha.

COMO PODEMOS NOS PROTEGER?

Consideremos três possíveis adversários:

Adversário	Hashes por segundo
Eu	22×10^7 = 220 milhões
Jeremi M. Gosley	18×10^{10} = 180 bilhões
A NSA	10^{12} = 1 trilhão

Consideremos também:

- Você é **o único** alvo do seu adversário neste ataque.
- Ele **possui uma cópia do seu "dicionário"**, e portanto, irá utilizá-lo para quebrar sua senha.
- Ele sabe que você utilizou, conforme instruído, **exatamente 6 palavras** deste para compor sua senha.
- **Seus dados não estão viciados** e **seu dicionário não foi adulterado**. Logo, todos os resultados são igualmente possíveis.

COMO PODEMOS NOS PROTEGER?

Tempo estimado para se revelar a senha:

Adversário	Tempo estimado para se revelar a senha*

* 7776^6 ÷ H/s ÷ 2 (média) ÷ 60 (minutos) ÷ 60 (horas) ÷ 24 (dias) ÷ 365 (anos)

COMO PODEMOS NOS PROTEGER?

Tempo estimado para se revelar a senha:

Adversário	Tempo estimado para se revelar a senha*
Eu	

* 7776^6 ÷ H/s ÷ 2 (média) ÷ 60 (minutos) ÷ 60 (horas) ÷ 24 (dias) ÷ 365 (anos)

COMO PODEMOS NOS PROTEGER?

Tempo estimado para se revelar a senha:

Adversário	Tempo estimado para se revelar a senha*
Eu	15 milhões, 982 mil e 585 anos

* 7776^6 ÷ H/s ÷ 2 (média) ÷ 60 (minutos) ÷ 60 (horas) ÷ 24 (dias) ÷ 365 (anos)

COMO PODEMOS NOS PROTEGER?

Tempo estimado para se revelar a senha:

Adversário	Tempo estimado para se revelar a senha*
Eu	15 milhões, 982 mil e 585 anos
Jeremi M. Gosley	

* 7776^6 ÷ H/s ÷ 2 (média) ÷ 60 (minutos) ÷ 60 (horas) ÷ 24 (dias) ÷ 365 (anos)

COMO PODEMOS NOS PROTEGER?

Tempo estimado para se revelar a senha:

Adversário	Tempo estimado para se revelar a senha*
Eu	15 milhões, 982 mil e 585 anos
Jeremi M. Gosley	38 milênios e 945 anos

* 7776^6 ÷ H/s ÷ 2 (média) ÷ 60 (minutos) ÷ 60 (horas) ÷ 24 (dias) ÷ 365 (anos)

COMO PODEMOS NOS PROTEGER?

Tempo estimado para se revelar a senha:

Adversário	Tempo estimado para se revelar a senha*
Eu	15 milhões, 982 mil e 585 anos
Jeremi M. Gosley	38 milênios e 945 anos
A NSA	

* 7776^6 ÷ H/s ÷ 2 (média) ÷ 60 (minutos) ÷ 60 (horas) ÷ 24 (dias) ÷ 365 (anos)

COMO PODEMOS NOS PROTEGER?

Tempo estimado para se revelar a senha:

Adversário	Tempo estimado para se revelar a senha*
Eu	15 milhões, 982 mil e 585 anos
Jeremi M. Gosley	38 milênios e 945 anos
A NSA	3 milênios e meio

* 7776^6 ÷ H/s ÷ 2 (média) ÷ 60 (minutos) ÷ 60 (horas) ÷ 24 (dias) ÷ 365 (anos)

CONCLUSÃO

CONCLUSÃO

1. Como método de autenticação, senhas são prevalentes e ainda serão por mais algum tempo.

CONCLUSÃO

2. Uma maneira eficiente e massiva para um adversário obter senhas é conseguindo acesso a servidores onde diversos usuários possuem contas, e extraindo uma cópia das hashes que correspondem à suas senhas.

CONCLUSÃO

3. Essas hashes são então submetidas à sucessivas adivinhações que, dependendo do poder computacional do adversário, vão de centenas de milhões à trilhões por segundo. Estes ataques são geralmente informados por meio de dicionários a tentar primeiramente as combinações mais relevantes.

CONCLUSÃO

4. Espontâneamente construir uma senha improvável, mesmo quando informado das combinações mais prováveis, é um método limitado em termos da força resultante da senha, e impraticável para proteger um grande número de pessoas.

CONCLUSÃO

5. Em contra partida, Diceware é um método de simples utilização e que gera senhas com **real aleatoriedade**, a senha resultante é tão aleatória que a este tempo desconhecemos computadores que, mesmo informados do método, sequer possuem a capacidade de percorrer um número relevante de possibilidades em um período de tempo razoável.

PARA SABER MAIS

Realizamos encontros regulares para discutir técnicas de autodefesa digital.

t.me/paradigma_icu

paradigma.icu