

autenticação

↳ "Quem é você?"

Uma entidade faz a prova de identidade para responder

FATORES DE AUTENTICAÇÃO DE USUÁRIOS

- * **CONHECIMENTO**: senha e PIN (...)
- * **POSSE**: token, certificado e chave de segurança (...)
- * **BIOMETRIA**: impressão digital e reconhecimento facial (...)
- * **outros fatores são**: endereço IP, padrão de digitação, ...

⇒ **MFA**: utiliza 2 ou mais fatores de autenticação.

ENTROPIA DE SENHAS

$$E = \log_2 (K^L)$$

↓
K: número de caracteres possíveis

↗ L: tamanho da senha

PRINCIPAIS ATAQUES A SENHAS

- * Força bruta e ataque de dicionário
- * Tabelas arco-íris → PALAVRAS NO DICIONÁRIO
BASE DE SENHAS VAZADAS
- * Keyloggers e screenloggers
- * Password sniffing
- * Engenharia social (phishing, MITM, ...)

⇒ **TABELAS DE HASH PRÉ-COMPUTADAS**

SENHA DE USO ÚNICO (OTP)

- 2 tipos:
- * **HOTP** → senha válida por X eventos
 - * **TOTP** → senha válida por X tempo

PASSKEYS

- ↳ 2FA
- ↳ sem senha
- ↳ sem nome de usuário.

Autenticação entre serviços

- ↳ JSON, JWT, ...