





SEGURANÇA DA INFORMAÇÃO

TÓPICOS ESPECIAIS EM ENGENHARIA
CONTROLE DE ACESSOS

CONTROLE DE ACESSOS

Proteger o que precisa ser protegido com as
tecnologias disponíveis





IDENTIFICAÇÃO



IDENTIFICAÇÃO

- ✗ Métodos para determinar a identidade do sujeito
 - Usuário, Aplicação, Processo
- ✗ Username ou outra informação pública
- ✗ Requisitos:
 - Valor único
 - Padrão de nomeação
 - Não identificar cargos
 - Não ser compartilhado entre usuários

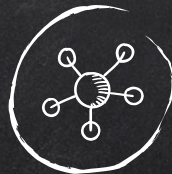


AUTENTICAÇÃO



AUTENTICAÇÃO

- ✕ Forma de provar a identidade
- ✕ Como podemos provar a identidade?
 - Algo que você saiba
 - Algo que você tenha
 - Algo que você seja
- ✕ Senhas, tokens, biometria
- ✕ 2FA (Two Factor Authentication)
 - Fortalece autenticação



ALGO QUE VOCÊ SAIBA

- ✗ Autenticação + tradicional
- ✗ Senhas
 - Cadeia de caracteres (string)
 - Amplamente utilizada
 - Tipos
 - Senhas cognitivas
 - Senhas dinâmicas (uso único)
 - Frase Secreta



SENHAS COGNITIVAS



Baseado em fatos ou opiniões

Perguntas baseadas na
experiência

Fácil de lembrar



SENHAS DINÂMICAS



Uso Único

Dados ou Locais Sensíveis

Dispositivos Token



FRASE SECRETA / PASSPHRASE

Passwords :

samuel123
m0nk3y99
49lakestreet
Y#Cb3\$D6dZYF

Pass-phrases :

I love ice-cream!
Jerry lives in Bugtussle KY
I can see tham, yall.
2 be or not 2 be, that is the ?



ATAQUES CONTRA SENHAS

- ✗ Monitoramento
- ✗ Acessar arquivo de senhas
- ✗ Força bruta
- ✗ Ataques de dicionário
- ✗ Engenharia Social
- ✗ “Espionagem”



ALGO QUE VOCÊ TENHA

- ✗ Requer posse de algo por exemplo, uma chave, smartcard, ou algum dispositivo
- ✗ Exemplos
 - Chave
 - Documentos
 - Dispositivos Token
 - Cartões de Memória
 - Cartões Inteligentes (SmartCard)



DISPOSITIVO TOKEN



Software/Hardware para verificar a identidade no processo de autenticação



DISPOSITIVOS TOKENS – PRÓS/CONTRAS

✗ Prós

- Menos vulnerável a espionagem
 - Escutas
 - Sniffing
- 2FA

✗ Contras

- Erro Humano
- Limitação Bateria
- Próprio Token



TIPOS DE TOKEN

- ✕ Síncrono
 - Tempo ou contador
- ✕ Assíncrono
 - Pergunta/Resposta



CARTÃO DE MEMÓRIA



Armazena informação mas não
processa



SMARTCARD



Armazena e processa informação
Pode ser inutilizado após falhas de login
PIN/Senha desbloqueia cartão

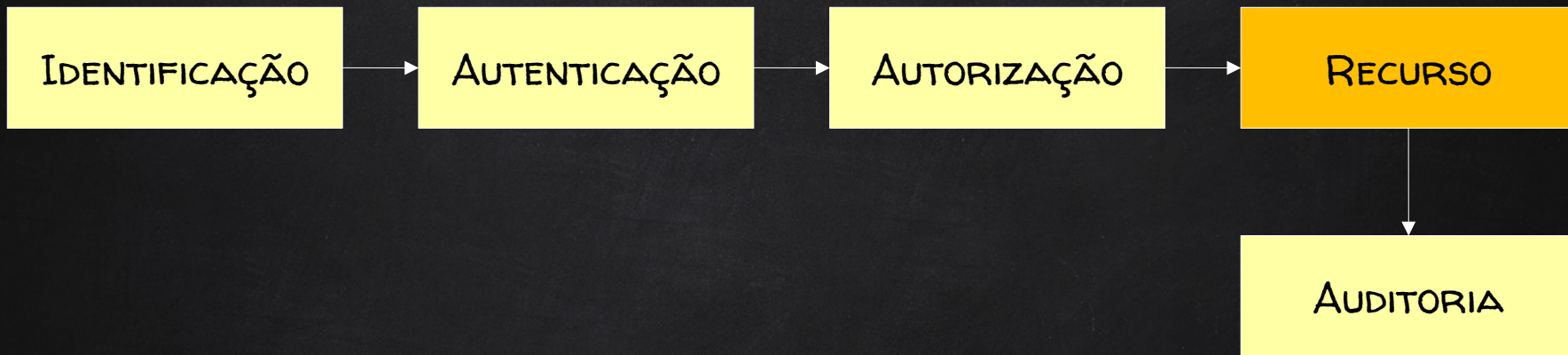


ALGO QUE VOCÊ SEJA

- ✕ Atributo pessoal único é analisado
- ✕ Engloba todas técnicas de biometria
 - Digital
 - Retina
 - Íris
 - Mão
 - Facial



AUTORIZAÇÃO





TIPOS DE CONTROLES DE ACESSO

Administrativos

Papéis,
responsabilidades,
políticas e funções
administrativas.

Técnicos

Hardware/software
para
implementação

Físicos

Garante segurança
e proteção do
ambiente



MODELOS DE CONTROLES DE ACESSO

Discricionário

Discretionary

Access

Control

(DAC)

Mandatório

Mandatory

Access

Control

(MAC)

Baseado em Perfis

Role-Based

Access

Control

(RBAC)



DISCRICIONÁRIO – DAC

- ✗ Permite ao proprietário de recurso especificar quem poderá acessar quais recursos
- ✗ Controle de acesso está no critério do proprietário
- ✗ Define política de control de acesso
 - Restringe acesso a arquivos ou recursos baseado na identidade
- ✗ Pode ser implementado com ACL (Listas de Controle de Acesso)



MATRIZ DE CONTROLE DE ACESSO

Usuário	Arquivo1	Arquivo2	Arquivo3
Jhonny	Leitura	Leitura,Escrita	Leitura
Rosemary	Leitura,Escrita	Sem acesso	Controle Total
Robert	Controle Total	Sem Acesso	Leitura



CAPACIDADE

Usuário	Arquivo1	Arquivo2	Arquivo3
Jhonny	Leitura	Leitura, Escrita	Leitura
Rosemary	Leitura, Escrita	Sem acesso	Controle Total
Robert	Controle Total	Sem Acesso	Leitura



ACL – LISTA DE CONTROLE DE ACESSO

Usuário	Arquivo1	Arquivo2	Arquivo3
Jhonny	Leitura	Leitura, Escrita	Leitura
Rosemary	Leitura, Escrita	Sem acesso	Controle Total
Robert	Controle Total	Sem Acesso	Leitura



MANDATÓRIO – MAC

- ✗ O sistema é quem aplica as políticas de acesso
- ✗ Configurações de privilégio
 - administrador de sistemas
- ✗ Rotulação das informações
 - gestor da informação
- ✗ Todos objetos e indivíduos são rotulados
 - Categoria
 - Classificação (Nível)



MANDATÓRIO – MAC

Usuário	Nível	Categoria
Jhonny	Secreto	Finanças
Robson	Secreto	RH

Recurso	Nível	Categoria
Arquivos contábeis	Secreto	Finanças
Dados de Funcionários	Secreto	RH



BASEADO EM PERFIS – RBAC

- ✗ Privilégios a partir de responsabilidades
- ✗ Papéis e privilégios são gerenciados por admins

Herança

USUÁRIOS

PAPEL

PERMISSÕES



ATIVIDADE!!!

Escrever um comparativo entre duas
biometrias

2-4 páginas

Entrega 06/03/2020

<https://forms.gle/tTRcXNhpj54wSMKj8>



DÚVIDAS?

Não esqueça de enviar sua
maior dúvida pelo link que está
no github.

ezarpelao@unaerp.br

<https://github.com/elizarp/unaerp>

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- ✕ Presentation template by [SlidesCarnival](#)
- ✕ Photographs by [Unsplash](#)