



Autenticação de Usuário





Objetivos de aprendizado

- › Discutir os quatro meios gerais de autenticar a identidade de um usuário.
- › Explicar o mecanismo de utilização de hashes de senhas para autenticação de usuário.
- › Entender a utilização do filtro de Bloom no gerenciamento de senhas.
- › Apresentar uma visão geral de autenticação de usuário baseada em token.
- › Discutir as questões envolvidas e as abordagens para autenticação de usuário remoto.
- › Resumir algumas das questões principais de segurança para autenticação de usuário



Autenticação de Usuário

- › Bloco fundamental para a construção de sistemas seguros
 - Base para o controle de acesso e responsabilidade/não-repúdio
- › Processo de verificação de uma identidade
- › Possui dois passos:
 - Apresentação da identificação
 - Verificação da identificação
- › Distinta da autenticação de mensagem



Autenticação de Usuário

- › Quatro formas de identificar indivíduos
 - A quarta desdobra da terceira
- › Baseadas em algo que o indivíduo...
 - Sabe – exemplo: senha
 - Possui – exemplo: chave, token, smartcard
 - É (biometria estática) – exemplo: impressão digital, retina
 - Faz (biometria dinâmica) – exemplo: voz, assinatura
- › Podem ser usadas isoladamente ou em conjunto
 - Fator duplo, triplo,...
- › Todas possuem suas limitações....



Autenticação por Senha

- › Método de autenticação amplamente utilizado
 - Usuário provê identificação e senha
 - Sistema compara senha recebida com aquela armazenada para aquela identificação
- › Senha autentica identificação, que por sua vez oferece segurança das seguintes formas
 - determina se o usuário está autorizado a obter acesso a um sistema
 - determina os privilégios concedidos ao usuário
 - é usado no controle de acesso discricionário



Vulnerabilidades da autenticação por senha

- › Ataque de dicionário offline
- › Ataque a conta específica
- › Ataque a senha popular
- › Adivinhação de senha contra usuário único
- › Sequestro de estação de trabalho
- › Explorar erros do usuário
- › Explorar reutilização de senhas
- › Monitoração eletrônica



Contramedidas

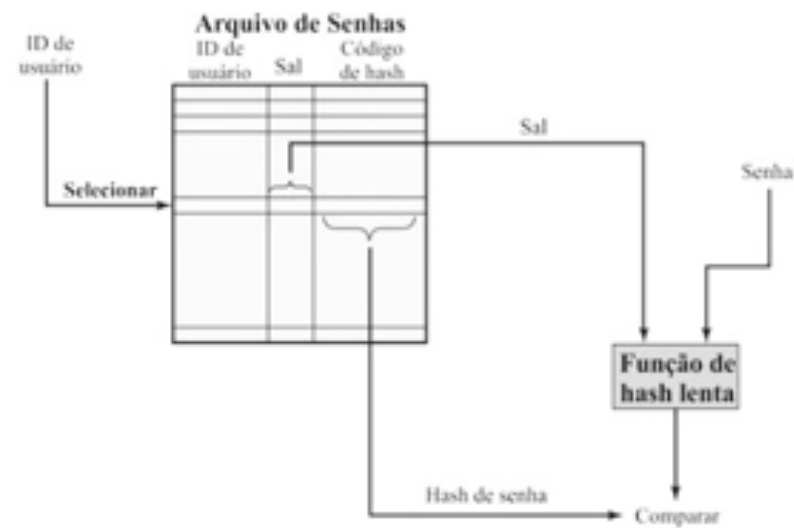
- › Impedir acesso não-autorizado a arquivo de senhas
- › Medidas para detecção de intrusão
- › Mecanismos de desativação de contas
- › Políticas de prevenção ao uso de senhas fracas
- › Políticas de treinamento e conscientização
- › Estratégias de logout automático
- › Criptografia de canais de comunicação



Uso de hashes de senhas



(a) Registrando nova senha



(b) Verificando uma senha



Por que sal?

- › Impede que senhas duplicadas sejam perceptíveis no arquivo de senhas.
- › Aumenta muito a dificuldade de ataques de dicionário off-line.
- › Impede a detecção de senhas reutilizadas





Implementação UNIX

- › Esquema original
 - Senha de 8 caracteres com total de 56-bits
 - Rotina de hash baseada em DES
 - Salt de 12-bits
 - Saída de 11 caracteres
 - 25 iterações
- › Esquema atualmente considerado extremamente inseguro
- › Ainda é usado por questões de compatibilidade e como parâmetro de comparação



Implementações melhoradas

- › Baseadas em melhores algoritmos de hash e maiores tamanhos de senhas e salts
- › Muitos sistemas usam MD5
 - Salt de 48-bits
 - Comprimento de senha ilimitado
 - Loop de 1000 iterações
 - Produz hashes de 128-bits
- › OpenBSD usa Bcrypt – hash baseado na cifra Blowfish
 - Salt de 128-bits para criar hash de 192-bits



Quebra de Senha

› Ataques de dicionário

- Tentar palavras comuns e suas combinações, comparando os hashes contra a tabela de hashes obtida em um arquivo de senhas.

› rainbow table

- Precomputa uma grande tabela de hashes
- Se o salt for pequeno, computa uma tabela por salt
 - › Exemplo dos salts de 12 bits dos antigos sistemas Unix (V7 de 1979)



Escolha de senhas

Tabela 3.1

Comprimentos de senhas observados [SPAF92a]

Comprimento	Número	Fração do total
1	55	0,004
2	87	0,006
3	212	0,02
4	449	0,03
5	1.260	0,09
6	3.035	0,22
7	2.917	0,21
8	5.772	0,42
Total	13.787	1,0

Tabela 3.2

Senhas quebradas de um conjunto de amostra de 13.797 contas [KLEI90]

Tipo de senha	Tamanho da busca	Número de correspondências	Porcentagem de senhas correspondentes	Razão ¹ custo/benefício
Nome de usuário/conta	130	308	2,7%	2,830
Sequências de caracteres	866	22	0,2%	0,025
Números	427	9	0,1%	0,021
Em chinês	392	56	0,4%	0,143
Nomes de lugares	628	82	0,6%	0,131
Nomes comuns	2.239	548	4,0%	0,245
Nomes de mulher	4.280	161	1,2%	0,038
Nomes de homem	2.866	140	1,0%	0,049
Nomes incomuns	4.955	130	0,9%	0,026
Mitos e lendas	1.246	66	0,5%	0,053
Shakespeareanos	473	11	0,1%	0,023
Termos de esporte	238	32	0,2%	0,134
Ficção científica	691	59	0,4%	0,085
Filmes e atores	99	12	0,1%	0,121
Desenhos animados	92	9	0,1%	0,088
Pessoas famosas	290	55	0,4%	0,190
Frases e padrões	933	263	1,8%	0,271
Sobrenomes	33	9	0,1%	0,273
Biologia	58	1	0,0%	0,017
Dicionário de sistema	19.683	1.027	7,4%	0,052
Nomes de máquinas	9.018	132	1,0%	0,015
Memóricos	14	2	0,0%	0,143
Bíblia do rei James	7.525	83	0,6%	0,011
Miscelânea de palavras	3.212	54	0,4%	0,017
Palavras em idíche	56	0	0,0%	0,000
Asteroides	2.407	19	0,1%	0,007
TOTAL	62.727	3.340	24,2%	0,053



Controle de acesso ao arquivo de senhas

- › Possível bloquear a "adivinhação de senhas" ao negar acesso às senhas criptografadas
 - Disponível apenas a usuários privilegiados
 - Frequentemente, se usa um arquivo shadow semarado
- › Ainda existem vulnerabilidades
 - Bug/falha de sistema operacional
 - Permissões de leitura acidentalmente concedidas
 - Reaproveitamento de senhas
 - Acesso a partir de mídia de backup não-protegida
 - Sniffing de senha em redes



Escolha de senhas

- › Usuários tendem a escolher senhas muito simples
- › Senha "ideal": escolhida uniformemente sobre o espaço de senhas possíveis
 - Difícil de lembrar
- › Técnicas:
 - Educação do usuário
 - Senhas geradas por computador / gerenciadores de senhas
 - Verificação reativa de senhas
 - Verificação proativa de senhas
 - Imposição de regras



Proactive Password Checking

- › rule enforcement plus user advice, e.g.
 - 8+ chars, upper/lower/numeric/punctuation
 - may not suffice
- › password cracker
 - time and space issues
- › Markov Model
 - generates guessable passwords
 - hence reject any password it might generate
- › Bloom Filter
 - use to build table based on dictionary using hashes
 - check desired password against this table

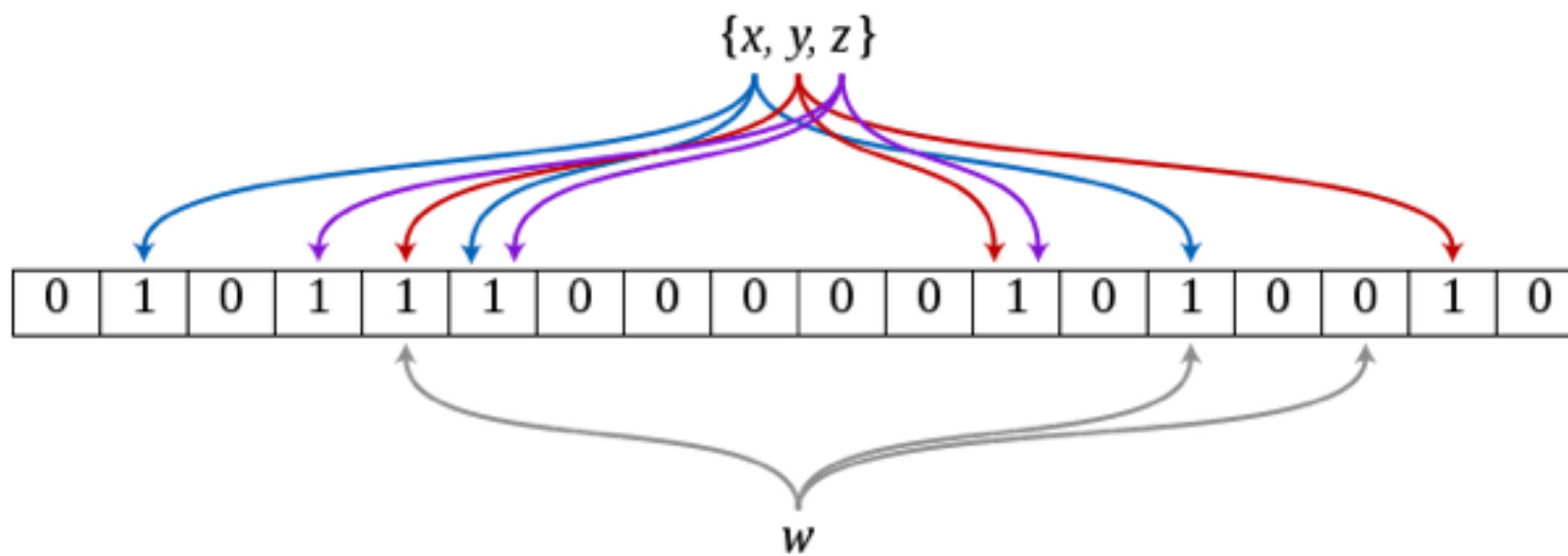


Verificação Proativa de Senhas

- › Regras e conselhos ao usuário – ex.:
 - Pelo menos 8 caracteres, uso de maiúsculas, minúsculas, números e pontuação
 - pode não ser suficiente – usuário não segue ou ”contorna”
- › Uso de crackers de senhas
 - limitações de espaço e, principalmente, tempo
- › Markov Model
 - Otimiza a busca por senhas ”parcialmente conhecidas”
 - Espécie de ”análise de similaridade”
- › Filtro de Bloom
 - Busca rapidamente se ”um elemento está em um conjunto”
 - constrói-se um conjunto de senhas fracas (dicionários)



Filtro de Bloom





Autenticação baseada em Token

Tabela 3.3

Tipos de cartões usados como tokens

Tipo do cartão	Característica distintiva	Exemplo
Gravado em relevo	Somente caracteres em relevo, na frente	Cartão de crédito antigo
Fita magnética	Código de barras magnético atrás, caracteres na frente	Cartão bancário
Memória	Memória eletrônica interna	Cartão telefônico pré-pago
Smart De contato Sem contato	Memória eletrônica e processador internos Contatos elétricos expostos na superfície Antena de rádio sem contato embutida	Cartão de indentificação biométrico



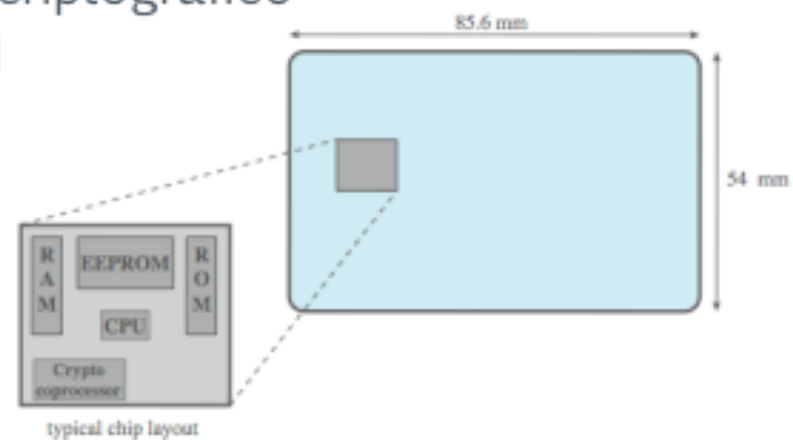
Cartões de Memória

- › Armazenam dados - mas não os processam
- › Pode ser usado como fator único de autenticação ou fator adicional
 - Exemplo de fator único: chave de hotel
 - Exemplos de fator adicional: compra com cartão de crédito; acesso a sistema de informação
- › Potenciais desvantagens:
 - Requer leitora especial
 - Perda do token
 - Clonagem de token*
 - Insatisfação do usuário



Smartcard

- › Estilo "cartão de crédito com chip"
- › Possui processador, memória e portas de entrada e saída
 - acesso por contato ou sem contato
 - pode possuir co-processador criptográfico
 - memórias ROM, EEPROM, RAM





Comunicação com SmartCard



APDU = Unidade de dados do protocolo de aplicação

ATR = Resposta à reinicialização

PTS = Seleção do tipo de protocolo




Estudo de Caso: ICP-Brasil

- › Infraestrutura de Chaves Públicas "oficial" brasileira
- › Usada para dar validade jurídica a assinaturas digitais
- › Equipamentos envolvidos: tokens, smart cards, leitoras de cartão, HSMs
 - Todos esses equipamentos são avaliados por laboratórios e certificados para garantir a proteção dos "parâmetros críticos de segurança"






Estudo de Caso: ICP-Brasil – Smart Cards

 **Infraestrutura de Chaves Públicas Brasileira**

Manual de Condutas Técnicas 1 – Volume I
Requisitos, Materiais e Documentos Técnicos para Homologação de Cartões Criptográficos (Smart Cards) no Âmbito da ICP-Brasil

Versão 4.2

BRASÍLIA, 03 DE AGOSTO DE 2017

 **Infraestrutura de Chaves Públicas Brasileira**

1. Introdução

Este documento descreve os requisitos técnicos a serem observados no processo de homologação de cartões criptográficos (smartcard) ICP no âmbito da Infraestrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Para uma melhor compreensão do disposto neste documento, atenda-se por cartão criptográfico ICP um cartão de circuito integrado (Integrated Circuit Card – ICC) com capacidade de geração e armazenamento de chaves criptográficas assimétricas e processamento criptográfico assimétrico e armazenamento de certificados digitais validados para utilização em uma Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1. Objetivo da homologação

O objetivo do processo de avaliação de conformidade é verificar a interoperabilidade e operação segura de cartões criptográficos ICP-BRASIL por meio da aderência aos requisitos técnicos definidos neste manual.


1.2. Descrição do processo de homologação

O processo de homologação é baseado em um conjunto de requisitos técnicos definidos no presente manual que devem ser atendidos por um cartão criptográfico ICP-BRASIL, para prover interoperabilidade dos cartões através de sua padronização e operação segura de acordo com níveis de segurança previamente definidos, conforme descrito abaixo.

A versão atual deste manual considera dois possíveis níveis de segurança de homologação para cartões criptográficos ICP-Brasil.

Por questão de compatibilidade com as versões anteriores deste manual, optou-se por manter a denominação Nível 1 para o nível de homologação baseado em avaliação funcional e documental e Nível 2 para o nível de homologação baseado na análise das especificações completas e detalhadas do equipamento, inclusive de seu software.

- Nível 1: consiste em uma verificação de aderência através da análise funcional e documental. Este nível adiciona segurança limitada ao cartão, sendo aplicável quando

 **Infraestrutura de Chaves Públicas Brasileira**

versões de sistemas operacionais atualmente disponíveis (tais como, Microsoft Windows, Linux e UNDO).

2.3.2. Estrutura da mensagem de APDU

Uma aplicação necessita enviar um comando para ser processado pelo módulo criptográfico, o qual, por sua vez, retorna a respectiva resposta. Essa correspondência entre um comando enviado e sua respectiva resposta é denominada de "par comando-resposta".

Uma APDU (Application Protocol Data Unit) contém um comando ou uma resposta trocada com o módulo criptográfico.

Uma APDU de comando consiste de duas partes: um cabeçalho obrigatório de 4 bytes e um corpo de tamanho variável. De mesma forma, uma APDU de resposta consiste de duas partes: um corpo de tamanho variável e um anexo obrigatório (trailer) de 2 bytes.

REQUISITO-MC HL1: Um módulo criptográfico deve seguir uma estrutura de comando e resposta APDU (Application Protocol Data Unit) conforme os requisitos e as convenções definidas no padrão ISO/IEC 7816-4:2005.

2.3.3. Conjunto mínimo de comandos

Com o intuito de buscar a interoperabilidade entre provedores de serviços, leitores, módulos criptográficos e aplicações, este documento reconhece a iniciativa do padrão ISO/IEC 7816, e define a obrigatoriedade de atendimento a um conjunto mínimo de comandos.

REQUISITO-MC HL2: Um módulo criptográfico deve suportar, no mínimo, o conjunto de comandos apresentados na Tabela 3.

Manual de Condutas Técnicas 1 – ICP-Brasil | Vol. 1 – versão 4.2



ICP-Brasil: *case* dos Objetos Metrológicos

Instituto Nacional de Tecnologia da Informação
CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA

Área de Imprensa | Glossário | Perguntas frequentes

ÁREA FISCAL - NOTÍCIAS - ÍNDICE DE NOTÍCIAS - CERTIFICADO DIGITAL ICP-BRASIL SERÁ USADO PARA COMBATER FRAUDES NA VENDA DE GASOLINA

ITI
Instituto Nacional de Tecnologia da Informação

Certificado Digital ICP-Brasil será usado para combater fraudes na venda de gasolina

Publicado: São Paulo, 30 de julho de 2018, 13:07 | Última atualização em: Segunda, 30 de julho de 2018, 18:03

Um novo tipo de certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil foi anunciado durante o 16º CentForum - Fórum de Certificação Digital. No painel "Certificado digital nas bombas de gasolina", o assessor técnico da presidência do ITI, Ruy Ramos, explicou que a novidade será destinada a objetos metrológicos aprovados pelo Inmetro.

Inicialmente, o novo certificado digital estará presente nas bombas de gasolina, mas poderá ser aplicado em outros equipamentos, como balanças e relógios medidores de energia elétrica. Alíado de parceria entre as duas entidades, o principal objetivo desse novo certificado é combater fraudes ocorridas na venda de combustíveis.

De acordo com dados da Federação das Indústrias do Estado de São Paulo - Fiesp, o prejuízo pode chegar a R\$ 200 bilhões apenas ao governo do estado de São Paulo por causa das fraudes em diversos setores da economia. Segundo explicou o presidente do Inmetro Carlos Augusto de Azevedo, esta parceria com o ITI representa apenas o início de uso da certificação digital em conjunto com a metrologia neste combate. Azevedo disse que optou-se inicialmente pelas bombas de gasolina por elas serem um dos objetos mais fraudados no país.

Os palestrantes indicaram que a fraude metrológica se torna uma burla fácil, problema grave para todo o país. Eles afirmaram que o papel dos institutos é justamente impedir que esses problemas aconteçam. "Esta união entre a certificação digital e Inmetro é um plano pioneiro do Brasil, ação histórica e projeto de vanguarda no mundo", afirmou o presidente do Inmetro. Este novo modelo de certificado digital para dispositivos ou objetos metrológicos deverá ter validade de 10 anos, resolução assinada por certificado do fabricante, hardware criptográfico certificado pelo Inmetro, entre outras características técnicas.

Reportagem em: Notícias | Índice de notícias

RESOLUÇÃO Nº 139, DE 03 DE JULHO DE 2018.

APROVA A CRIAÇÃO DA POLÍTICA DE CERTIFICADO PARA OBJETOS METROLÓGICOS - OM-BR NO ÂMBITO DA ICP-BRASIL.

O COORDENADOR DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no uso das atribuições que lhe confere o art. 6º, §1º, inc. IV, do Regimento Interno, torna público que o COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no exercício das competências previstas no art. 4º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, em reunião ordinária realizada em 03 de julho de 2018, e

CONSIDERANDO a alteração na Portaria Inmetro nº 559/2016 que, entre outras motivações, visa robustecer o controle metrológico legal das bombas medidoras de combustíveis líquidos com a adoção de certificação digital ICP-Brasil, e

CONSIDERANDO a necessidade da ICP-Brasil avançar em tipos de certificados digitais a fim de fomentar a utilização, em detrimento dos outros, que não possuem validade jurídica, conforme MP nº 2.200-2/2001,

RESOLVEU:

Art. 1º O item 1.1.3, do DOC-ICP-04, versão 6.5, passa a vigorar com a seguinte redação:

"1.1.3. São 12 (doze) os tipos de certificados digitais para usuários finais da ICP-Brasil, sendo 8 (oito) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme o descrito a seguir:

a) Tipos de Certificados de Assinatura Digital:

- I. A1
- II. A2
- III. A3
- IV. A4
- V. T3
- VI. T4
- VII. A CF-e-SAT
- VIII. OM-BR



Autenticação Biométrica

- › Autenticação de usuário com base em características físicas únicas
 - Exemplos: impressão digital, geometria da mão, características faciais e padrões de retina e íris, e características dinâmicas, como registro de voz e assinatura
- › Baseada em reconhecimento de padrões
- › Comparativamente complexa e cara



Características físicas usadas em aplicações biométricas

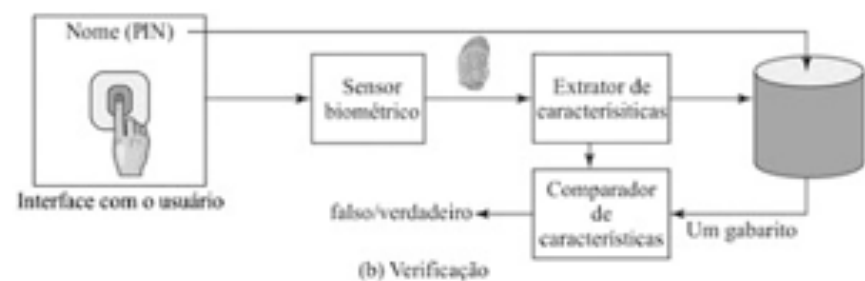
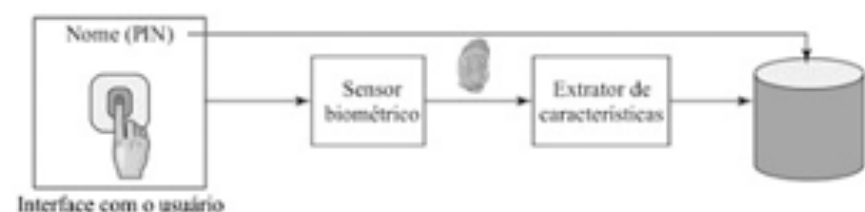
- › Características faciais
- › Impressões digitais
- › Geometria da mão
- › Padrão da retina
- › Íris
- › Assinatura
- › Voz

Custo vs acurácia das características biométricas



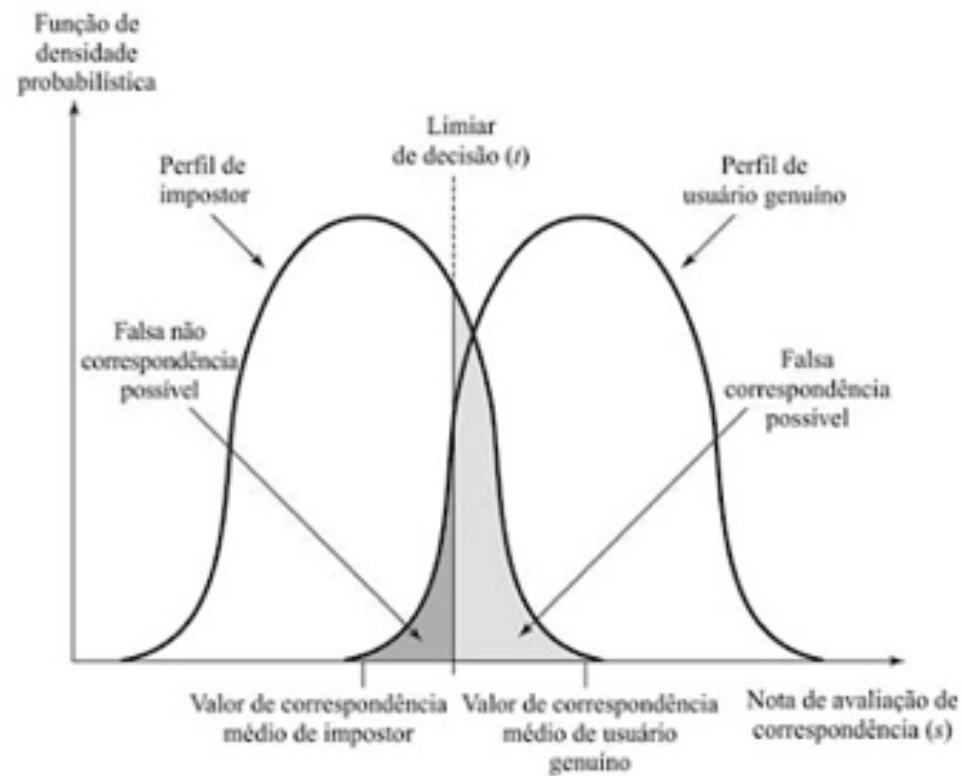


Operação de um sistema de autenticação biométrica



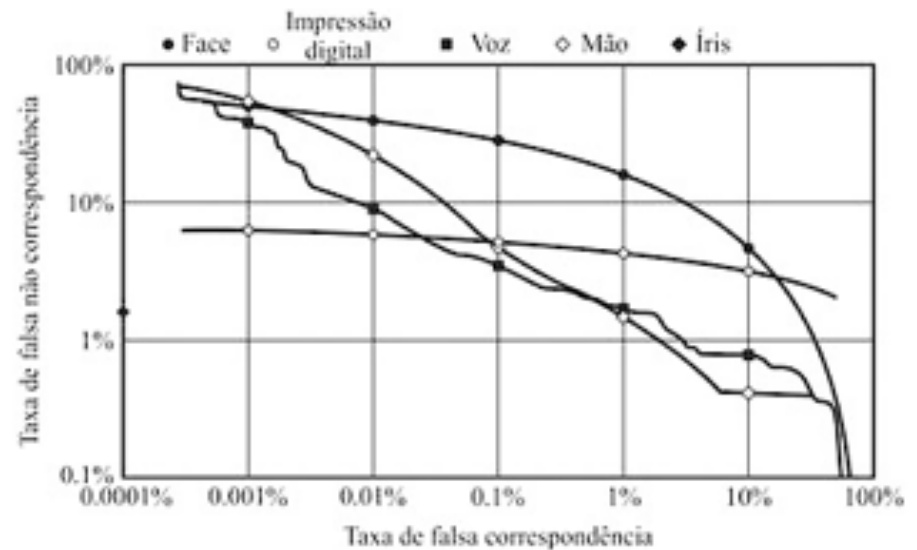
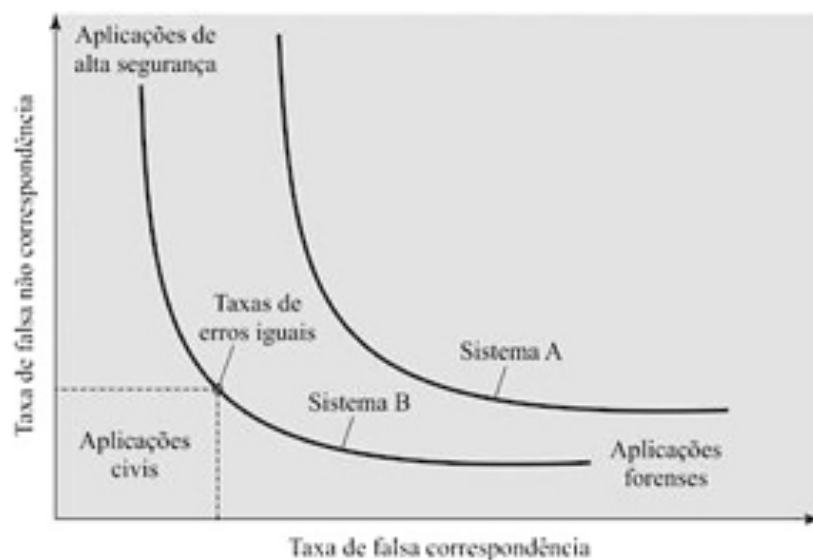


Acurácia Biométrica





Acurácia Biométrica





Autenticação de Usuário Remoto

- › Autenticação a partir de redes é um problema complexo
 - problemas como escuta/monitoramento, reenvio de mensagem etc.
- › Mecanismos geralmente se beneficiam de estratégia desafio-resposta
 - usuário envia identidade
 - sistema retorna número aleatório
 - usuário responde função da senha e do número aleatório
 - sistema calcula função da senha e número aleatório e compara



Protocolos simples de desafio/resposta

Cliente	Transmissão	Sistema
U , usuário	$U \rightarrow$	
	$\leftarrow \{r, h(), f()\}$	número aleatório funções $h(), f()$
senha P' r' , retorno de r	$f(r', h(P')) \rightarrow$	
	\leftarrow sim/não	se $f(r', h(P')) =$ $f(r, h(P(U)))$ então sim senão não

(a) Protocolo para uma senha

Cliente	Transmissão	Sistema
U , usuário	$U \rightarrow$	
	$\leftarrow \{r, h(), f()\}$	r , número aleatório funções $h(), f()$
$P' \rightarrow W'$ senha para código de acesso via token r' , retorno de r	$f(r', h(W')) \rightarrow$	
	\leftarrow sim/não	se $f(r', h(W')) =$ $f(r, h(W(U)))$ então sim senão não

(b) Protocolo para um token

Cliente	Transmissão	Sistema
U , usuário	$U \rightarrow$	
	$\leftarrow \{r, E()\}$	r , número aleatório $E()$, função
biometria $B' \rightarrow BT'$ D' dispositivo biométrico r' retorno de r	$E(r', D', BT') \rightarrow$	$E^{-1}E(r', P', BT') =$ (r', P', BT')
	\leftarrow sim/não	se $r' = r$ e $D' = D$ e $BT' = BT(U)$ então sim senão não

(c) Protocolo para biometria estática

Cliente	Transmissão	Sistema
U , usuário	$U \rightarrow$	
	$\leftarrow \{r, x, E()\}$	r , número aleatório x , desafio na forma de sequência aleatória $E()$, função
$B'; x' \rightarrow BS'(x)$ r' , retorno de r	$E(r', BS'(x)) \rightarrow$	$E^{-1}E(r', BS'(x)) =$ $(r', BS'(x))$ extrair B' de $BS'(x)$
	\leftarrow sim/não	se $r' = r$ e $x' = x$ e $B' = B(U)$ então sim senão não

(d) Protocolo para biometria dinâmica



Questões de segurança de autenticação

Ataques	Autenticadores	Exemplos	Defesas típicas
Ataque a cliente	Senha	Adivinhação, busca exaustiva	Grande entropia; tentativas limitadas
	Token	Busca exaustiva	Grande entropia; tentativas limitadas; roubo de objeto requer presença
Ataque a sistema	Biométrico	Falsa correspondência	Grande entropia; tentativas limitadas
	Senha	Roubo de texto às claras, busca em dicionário, busca exaustiva	Uso de hash; grande entropia; proteção de banco de dados de senhas
	Token	Roubo de código de acesso	Mesmas da senha; código de acesso de uso único
	Biométrico	Roubo de gabarito	Captura de dispositivo de autenticação; desafio/resposta
Escuta, roubo e cópia	Senha	"Olhar sobre os ombros" ("shoulder surfing")	Diligência do usuário para proteger segredo; diligência do administrador para revogar rapidamente senhas comprometidas; autenticação multifator
	Token	Roubo, falsificação de hardware	Autenticação multifator; token resistente ou que evidencia falsificação
	Biométrico	Cópia (spoofing) da biometria	Deteção de cópia no dispositivo de captura e autenticação do dispositivo de captura
Repetição	Senha	Repetição de resposta roubada para senha	Protocolo de desafio/resposta
	Token	Repetição de resposta roubada para código de acesso	Protocolo de desafio/resposta; código de acesso de uso único
	Biométrico	Repetição de resposta roubada para gabarito biométrico	Deteção de cópia no dispositivo de captura e autenticação do dispositivo de captura via protocolo de desafio/resposta
Cavalo de Troia	Senha, token, biometria	Instalação de cliente falso ou dispositivo de captura	Autenticação de cliente ou dispositivo de captura dentro do perímetro de segurança confiável
Negação de service	Senha, token, biometria	Bloqueio após várias autenticações fracassadas	Multifator com token