Autenticação

Segurança de Dados – MSI

Prof. Daniel Saad Nogueira Nunes

Autenticação

Autenticação

Processo de verificação de uma identidade alegada por ou para uma entidade de sistema.

Autenticação

- Um processo de autenticação consiste de duas etapas:
  - Etapa de identificação.
  - Etapa de verificação.

Autenticação

Etapa de Identificação

- Consiste em apresentar um identificador ao sistema de segurança.
- O identificador deve ser atribuído cuidadosamente, pois identidades autenticadas são a base para outros serviços.

Autenticação

Etapa de Verificação

- Apresenta ou gera informações de autenticação que confirmem a vinculação entre a entidade e o identificador.

Autenticação

Exemplo

- Usuário: Alice Toklas.
- Identificador de usuário: ABTOKLAS
- Esta informação necessita ser armazenada em qualquer máquina que Alice deseja utilizar.

Autenticação

- Senha: segredo privado de Alice e do sistema.
- ID + senha: habilita os administradores a estabelecerem a permissão de acesso e **auditar** a sua atividade.
- Como o ID não é secreto, usuários podem entrar em contato com Alice.
- Como a senha é secreta, ninguém a priori pode fingir ser Alice.

Autenticação

- Identificação: meio pelo qual um usuário provê uma identidade alegada ao sistema.
- Autenticação: meio para estabelecer a validade da alegação.
- OBS: autenticação de usuário $\neq$ autenticação de mensagem.
- Autenticação de mensagem: permite que os pares comunicantes verifiquem se o conteúdo de uma mensagem recebida não foi alterado e se a origem é autêntica.

Meios de Autenticação

- Há em geral quatro meios de autenticar a identidade de usuário.
- Podem ser utilizados sozinhos ou combinados.

Meios de Autenticação

Conhecimento Específico

- Baseia-se em algo que o indivíduo conhece.
- Senhas, PIN, respostas a um conjunto de perguntas, ...

Meios de Autenticação

Possessão

- Baseia-se em algo que o indivíduo possui.
- Cartões, chaves físicas.
- Chamado de *token*.

Meios de Autenticação

Biometria Estática

- Baseia-se no próprio indivíduo.
- Impressão digital, retina, face, ...

Meios de Autenticação

Biometria Dinâmica

- Baseia-se em ações do indivíduo.
- Padrão de voz, características de escrita, ritmo de digitação, ...

Meios de Autenticação

- Cada método tem problema.
- Um adversário pode conseguir adivinhar ou até mesmo roubar uma senha.
- Um adversário pode falsificar ou roubar um *token*.
- Além disto, o próprio usuário pode esquecer a senha ou perder um *token*.
- Custos administrativos para gerenciar as informações de senhas e *tokens* e garantir a segurança.

Meios de Autenticação

- Biometria: falsos negativos e falsos positivos.
- Também sofre com aceitação pelos usuários, custo e conveniência.

Meios de Autenticação

- Exploraremos cada um destes métodos a seguir.

Autenticação Baseada em Senha

- Autenticação por senha é amplamente utilizado.
  - Sistemas multiusuários.
  - Servidores em rede.
  - Sites de comércio eletrônico.
  - Outros serviços que exigem ID + Senha.

Autenticação Baseada em Senha

- O sistema compara a senha fornecida pelo usuário com uma senha armazenada, mantida em um arquivo.
- Senha: autentica o ID do usuário.
- ID provê segurança também:
  - Determina se o usuário está autorizado a obter acesso a um sistema.
  - Determina os privilégios concedidos ao usuário. Ex: Admin, guest, usuário normal, ...
  - Permite que apenas outros usuários tenham acesso a recursos compartilhados, como arquivos.

Vulnerabilidade de Senhas

- Normalmente um sistema que usa autenticação baseada em senha mantém um arquivo de senhas indexado pelos IDs.
- Uma técnica tipicamente utilizada é armazenar não a senha do usuário, mas o resultado da aplicação de uma função de hash de uma via sobre a senha.
- Por que hash?

Vulnerabilidade de Senhas

- Podemos identificar algumas estratégias de ataque e suas contramedidas.
  - Ataque de dicionário off-line.
  - Ataque a uma conta específica.
  - Sequestro de estação de trabalho.
  - Explorar erros de usuário.
  - Explorar reutilização de senhas.

Vulnerabilidade de Senhas

Ataque de Dicionário Off-line

- Se um hacker obtém acesso a base de dados contendo o arquivo de senhas ele pode efetuar um ataque de dicionário off-line.
- Compara os hashes de senha com hashes de senhas frequentemente utilizadas.
- Achando uma correspondência, ele obtém o acesso.
- Contramedidas:
  - Controle para impedir acesso não autorizado ao arquivo de senhas.
  - Detecção de intrusão.
  - Reemissão de senhas.

Vulnerabilidade de Senhas

Ataque a uma Conta Específica

- O atacante visa uma conta específica e aplica "chutes" da senha até descobrir a correta.
- Contramedidas:
  - Mecanismos de travamento.
  - Após uma quantidade determinada de tentativas de acesso, bloquear o acesso à conta.

Vulnerabilidade de Senhas

Sequestro de Estação de Trabalho

- O atacante espera até que uma estação de trabalho na qual um usuário já se autenticou fique desatendida.
- Contramedidas:
  - Bloquear acesso à estação de trabalho após um período de inatividade.
  - Esquemas de detecção de intrusão podem ser utilizados para detectar mudanças no comportamento do usuário.

Vulnerabilidade de Senhas

Explorar Erros do Usuário

- Se o sistema designar uma senha, é provável que o usuário a anote em algum lugar.
- Isto cria uma situação em potencial na qual o adversário pode tentar ler a senha escrita.
- Um usuário leigo também pode compartilhar uma senha intencionalmente para permitir que um colega compartilhe arquivos.
- Através de engenharia social usuários podem ser enganados e disponibilizarem as senhas.

Vulnerabilidade de Senhas

Explorar Erros do Usuário

- Muitos sistemas já vem com senhas pré-configuradas. Se o usuário administrador não a troca, fica fácil adivinhá-las.
- Contramedidas:
  - Treinamento de usuário.
  - Detecção de intrusão.
  - Uso de senhas mais simples combinadas com outro mecanismo de autenticação.

Vulnerabilidade de Senhas

Explorar Reutilização de Senhas

- Ataques podem tornar-se muito mais efetivos ou danosos se diferentes dispositivos de rede compartilharem a mesma senha ou uma senha semelhante para um usuário.
- Contramedida.
  - Proibição de senhas já utilizadas ou senhas semelhantes para determinados dispositivos de rede.

Utilização de Hash de Senhas

- Uma técnica amplamente utilizada é utilizar hash de senhas juntamente com um valor de sal (salt).
- Encontrado em todas as variantes do UNIX.

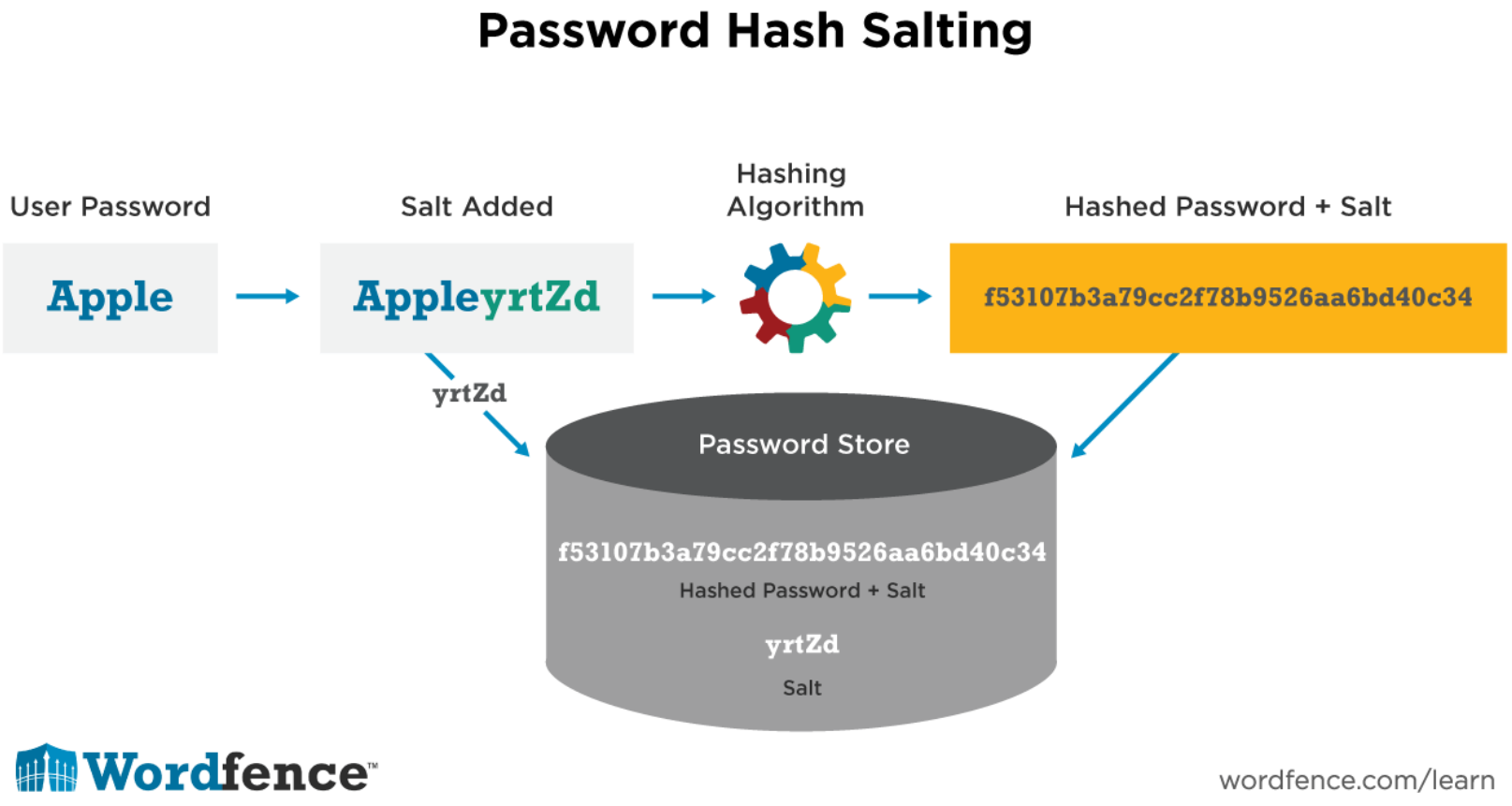
Utilização de Hash de Senhas

- Para registrar uma nova senha, o usuário seleciona uma senha ou uma senha lhe é designada.
- Esta senha é combinada com um valor de sal de comprimento fixo.
- Geralmente o valor de sal é gerado aleatoriamente.

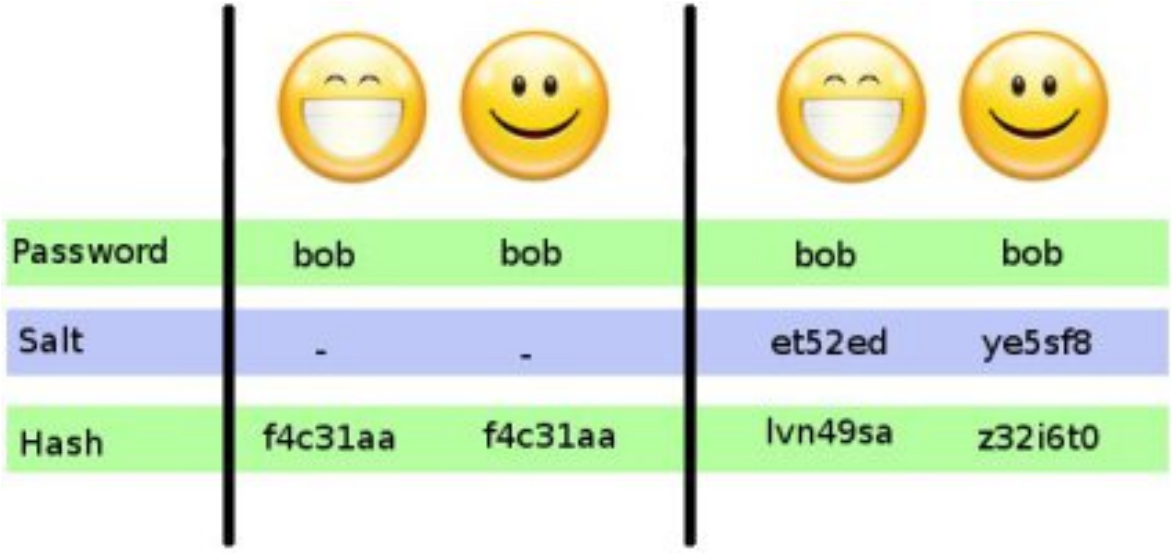
Utilização de Hash de Senhas

- Senha + sal servem de entrada para um algoritmo de hash para produção de um código de tamanho fixo.
- É interessante que o algoritmo de hash tenha execução lenta (mas viável), para frustar ataques força-bruta.
- O hash da senha + sal é armazenado juntamente com uma cópia do sal às claras no arquivo de senhas.
- Mostra-se seguro contra uma variedade de ataques criptoanalíticos e de força-bruta.

Hash + Salt


Password Hash Salting
User Password
Apple
Salt Added
AppleyrtZd
Hashing Algorithm
Hashed Password + Salt
f53107b3a79cc2f78b9526aa6bd40c34
yrtZd
Password Store
f53107b3a79cc2f78b9526aa6bd40c34
Hashed Password + Salt
yrtZd
Salt
Wordfence
wordfence.com/learn

Hash + Salt


Password
bob
bob
bob
bob
Salt
-
-
et52ed
ye5sf8
Hash
f4c31aa
f4c31aa
lvn49sa
z32i6t0

Hash + Sal

- O sal tem como finalidades finalidades:
  - Impede que senhas duplicadas sejam perceptíveis no arquivo de senhas.
    - Mesmo que dois usuários escolham a mesma senha, essas senhas terão diferentes valores de sal a elas designados.
    - Consequentemente os hashes produzidos serão diferentes.
  - Torna-se quase impossível descobrir se uma pessoa que tem senhas em dois ou mais sistemas usa a mesma senha em todos eles.
  - Evitar ataques to tipo rainbow table.

Hash + Sal

- Para entender o segundo ponto, imagine um ataque de dicionário off-line.
- Vamos assumir dois cenários:
  - Não utilizando o sal.
  - Utilizando o sal.

Hash + Sal

Não Utilizando o Sal

- A meta do atacante é adivinhar uma única senha.
- Ele apresenta um grande número de senhas prováveis à função de hash.
- Se qualquer uma das adivinhações corresponder a um dos hashes do arquivo, o atacante encontrou uma senha que está no arquivo.

Hash + Sal

Utilizando o Sal

- Com o sal o atacante deve utilizar a senha + o sal para chegar no mesmo hash.
- Previne contra ataques de *rainbow-table*, em que *hashes* computados são armazenados.

Abordagens de Quebra de Senha

- A abordagem tradicional de adivinhação consiste em desenvolver um grande dicionário possível de senhas e testar cada uma delas com o arquivo de senhas.
- Cada hash de senha deve ser obtido usando cada valor de sal no arquivo de senhas e então comparado com os valores de hash armazenados.

Abordagens de Quebra de Senha

- Se nenhuma correspondência for encontrada, o programa de quebra tenta variações de todas as palavras em seu dicionário de senhas prováveis.
- Tais variações incluem grafias de palavras de trás para frente, números ou caracteres especiais.

Abordagens de Quebra de Senha

- Uma alternativa é adotar um compromisso entre espaço e tempo, computando antecipadamente valores de hash potenciais.
- Para cada senha, o atacante gera os valores de hash associado a cada valor de sal possível.
- Basta consultar se o hash existe na tabela para quebrar uma senha com sal.
- Contramedida: usar sal de comprimento grandes.

Escolhas de Senha de Usuário

- Vários programas de quebra de senha baseiam-se no fato de haver pessoas que escolhem senhas fáceis de adivinhar.
- Alguns usuários escolhem senhas absurdamente curtas.
- Um estudo observou escolhas de trocas de senha em 54 máquinas, representando 7mil usuários e concluiu-se que 3% das senhas tinham três ou menos caracteres.
- Contramedida: rejeitar senhas curtas.

Escolhas de Senha de Usuário

Comprimento	Número	Fração do Total
1	55	0.004
2	87	0.006
3	212	0.002
4	449	0.03
5	1260	0.09
6	3035	0.22
7	2917	0.21
8	5722	0.42
Total	13787	1

Escolhas de Senha de Usuários

- O comprimento da senha é apenas parte do problema.
- Muitas pessoas, quando lhes é permitido escolher sua própria senha escolhem uma fácil como o seu próprio nome, nome da rua em que moram, nome do bicho de estimação, . . .
- O programa de quebra de senhas simplesmente tem de testar o arquivo de senhas contra listas de senhas prováveis.
  - Ataque de dicionário.

Escolhas de Senha de Usuários

- Um estudo coletou vários arquivos de senhas UNIX contendo 14 mil senhas cifradas aproximadamente.
- Utilizando estratégias simples, como tentar usar os nomes dos usuários como senha, ou colocar nomes de lugares famosos, foi o suficiente para quebrar quase 1/4 das senhas.

Escolhas de Senha de Usuários

Tipo de senha	Tamanho da busca	Número de correspondências	Porcentagem de senhas correspondentes	Razão[a] custo/ benefício
Nome de usuário/conta	130	368	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
Shakespearianas	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%	0,098
Pessoas famosas	290	55	0,4%	0,190
Frases e padrões	933	253	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
Mnemônicos	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 iídiche	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 a Arquivo de Senhas

- Um modo de frustrar um ataque a senhas é negar ao oponente acesso ao arquivo de senhas.
- Se a parte do arquivo onde estão os hashes das senhas for acessível somente por um usuário privilegiado, o oponente não pode ler esse arquivo sem saber de antemão a senha do usuário privilegiado.

Controle de Acesso a Arquivo de Senhas

- Muitas das vezes os hashes das senhas são mantidos em um arquivo separado do arquivo de IDs de usuários
- Este arquivo é denominado de arquivos de senha sombra (shadow).

Controle de Acesso a Arquivo de Senhas

- É dada atenção especial à proteção do arquivo de senhas sombra contra acesso não autorizado.
- Embora a proteção de arquivos de senha certamente valha a pena, vulnerabilidades ainda permanecem.

Controle de Acesso a Arquivo de Senhas

Vulnerabilidades

- Muitos sistemas, incluindo o UNIX, são suscetíveis a invasões imprevistas.
- Um hacker pode explorar uma brecha do S.O e obter o arquivo de senhas.
- Alternativamente, ele pode descobrir uma fraqueza no sistema de arquivos ou no SGBD para obter acesso ao arquivo.

Controle de Acesso a Arquivo de Senhas

Vulnerabilidades

- Um acidente de proteção pode deixar o arquivo de senhas legível para outros usuários.

Controle de Acesso a Arquivo de Senhas

Vulnerabilidades

- Alguns dos usuários tem contas em outra máquinas, em outros domínios de proteção e usam a mesma senha.
- Assim, se as senhas puderem ser lidas por qualquer um em uma máquina, uma máquina de outro lugar ficará comprometida.

Controle de Acesso a Arquivo de Senhas

Vulnerabilidades

- A falta de segurança física ou sua fraqueza pode criar oportunidades para um hacker.
- Às vezes há um backup do arquivo de senhas em um disco para reparos de emergência.
- O acesso a este backup permite que o atacante leia o arquivo de senhas.
- Alternativamente, um usuário pode inicializar o sistema a partir de um disco que está sendo executado em outro sistema operacional, como o Linux, e acessar o arquivo a partir desse outro SO.

Controle de Acesso a Arquivo de Senhas

Vulnerabilidades

- Em vez de capturar o arquivo de senhas do sistema, outra abordagem consiste em monitorar o tráfego na rede para colher IDs e senhas de usuários.

Controle de Acesso a Arquivo de Senhas

- Uma política de proteção de senhas deve complementar medidas de controle de acesso com técnicas para forçar os usuários a selecionarem senhas difíceis de adivinhar.

Estratégias de Seleção de Senhas

- Vimos anteriormente que, se os usuários não forem obrigados, eles irão escolher uma senha demasiadamente fácil.
- No outro extremo, se os usuários receberem senhas aleatórias, a quebra de senha será extremamente difícil.
- Mas boa parte dos usuários não irão lembrar destas senhas.
- A meta é eliminar senhas fáceis de adivinhar e ao mesmo tempo permitir que um usuário selecione uma senha que ele consiga memorizar.

Estratégias de Seleção de Senhas

- Quatro técnicas básicas são utilizadas:
  - Educação do usuário.
  - Senhas geradas por computador.
  - Verificação reativa de senha.
  - Verificação proativa de senha.

Estratégias de Seleção de Senhas

Educação do Usuário

- Consiste em informar o usuário a importância de usar senhas difíceis de adivinhar e dar diretrizes para selecionar senhas fortes.
- Provavelmente não será bem sucedida na maior parte das instalações onde haja grande população de usuários ou bastante rotatividade.
- Muitos usuários ignorarão as diretrizes.
- Outros não saberão julgar se uma senha é realmente forte.

Estratégias de Seleção de Senhas

Educação do Usuário

- Uma técnica empregada consiste em pedir para o usuário escolher a primeira letra de cada palavra de uma frase.
- A frase não pode ser bem conhecida.
- O nome do meu primeiro cachorro é Tobias $\Rightarrow$ OndMpceT.
- Estudos mostraram que os usuários podem lembrar tais senhas e que elas não são suscetíveis a ataques de adivinhação de senha baseados em senhas populares.

Estratégias de Seleção de Senhas

Senhas Geradas por Computador

- Senhas gerados por programas também tem problemas.
- Se forem aleatórias, os usuários não se lembrarão.
- Em geral tem aceitação fraca pelo usuário.
- Programas que produzem senhas pronunciáveis a partir de concatenação de símbolos são mais aceitos.

Estratégias de Seleção de Senhas

Verificação Reativa de Senhas

- O sistema executa periodicamente o seu próprio programa de quebra de senhas para identificar senhas fáceis.
- O sistema cancela quaisquer senhas que foram adivinhadas e avisa ao usuário.
- Essa tática tem algumas desvantagens:
  - Intensiva no uso de recursos.
  - Menos eficaz que um adversário que tem tempo e recursos de sobra para serem utilizados somente na tarefa de quebra.

Estratégias de Seleção de Senhas

Verificação Proativa de Senhas

- Permite que o usuário escolha sua própria senha.
- O sistema verifica se a senha é aceitável ou não.
- Se não for, é rejeitada.
- Filosofia: com orientação do sistema, o usuário pode criar e memorizar senhas que provavelmente não serão adivinhadas em um ataque de dicionário.
- Deve-se buscar um equilíbrio entre a aceitabilidade pelo usuário e a força da senha.

Estratégias para Verificação Proativa de Senhas

- Examinaremos agora estratégias para verificação proativa de senhas.

Estratégias para Verificação Proativa de Senhas

Imposição de Regras

- A primeira abordagem é um sistema simples para impor regras.
- Por exemplo:
  - Todas as senhas devem ter no mínimo 8 caracteres.
  - Nos primeiros oito caracteres, as senhas devem incluir no mínimo uma letra maiúscula, uma letra minúscula, dígitos numéricos e sinais de pontuação.

Estratégias para Verificação Proativa de Senhas

Imposição de Regras

- Essas regras poderiam ser acompanhadas de conselhos para o usuário.
- Embora esta abordagem seja superior a simplesmente educar os usuários, ela pode não ser suficiente para impedir programas de quebra de senhas.

Estratégias para Verificação Proativa de Senhas

Dicionário

- Utilizando um dicionário de senhas ruins, o sistema pode avisar o dicionário que uma determinada senha é facilmente quebrada. Desvantagens:
  - Espaço: o dicionário tem que ser grande para ser efetivo.
  - Tempo: é necessário buscar no dicionário a senha que o usuário selecionou para verificar se a mesma é fraca.

Autenticação baseada em token

- Objetos que o usuário possui para a finalidade de autenticação são denominados de tokens.
- Um dos tokens mais comuns são cartões.
- Podem ser de diferentes tipos.

Autenticação baseada em token

Tipo de cartão	Característica distintitva	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	Memória eletrônica e processador interno	Cartão de identificação biométrico

Cartões de memória

- Os cartões de memória podem armazenar, mas não processar dados.
- Mais comum: cartão de banco.
- Possuem uma fita magnética capaz de armazenar um código de segurança simples.
- Cartões mais robustos possuem uma memória interna.

Cartões de memória

- Cartões de memória pode ser utilizados para prover acesso físico.
  - Acesso a quartos de hotel.
- Para prover autenticação é necessário combiná-lo com outro mecanismo, como senhas ou PIN.
  - Caixa eletrônico.

Cartões de memória

- Entre as principais desvantagens estão:
  - Requer leitora especial:

Cartões de memória

- Entre as principais desvantagens estão:
  - Requer leitora especial:
    - Aumenta o custo de utilização do token.

Cartões de memória

- Entre as principais desvantagens estão:
  - Requer leitora especial:
    - Aumenta o custo de utilização do token.
    - Cria o requisito de gerenciar a segurança do hardware e do software da leitora.

Cartões de memória

- Entre as principais desvantagens estão:
  - Requer leitora especial:
    - Aumenta o custo de utilização do token.
    - Cria o requisito de gerenciar a segurança do hardware e do software da leitora.
  - Perda do token:

Cartões de memória

- Entre as principais desvantagens estão:
  - Requer leitora especial:
    - Aumenta o custo de utilização do token.
    - Cria o requisito de gerenciar a segurança do hardware e do software da leitora.
  - Perda do token:
    - Impede o usuário de conseguir acesso ao sistema.

Cartões de memória

- Entre as principais desvantagens estão:
  - Requer leitora especial:
    - Aumenta o custo de utilização do token.
    - Cria o requisito de gerenciar a segurança do hardware e do software da leitora.
  - Perda do token:
    - Impede o usuário de conseguir acesso ao sistema.
    - Custo envolvido na reposição do token.

Cartões de memória

- Entre as principais desvantagens estão:
  - Requer leitora especial:
    - Aumenta o custo de utilização do token.
    - Cria o requisito de gerenciar a segurança do hardware e do software da leitora.
  - Perda do token:
    - Impede o usuário de conseguir acesso ao sistema.
    - Custo envolvido na reposição do token.
    - Um adversário pode adivinhar o PIN e obter acesso não autorizado.

Cartões de memória

- Entre as principais desvantagens estão:
  - Requer leitora especial:
    - Aumenta o custo de utilização do token.
    - Cria o requisito de gerenciar a segurança do hardware e do software da leitora.
  - Perda do token:
    - Impede o usuário de conseguir acesso ao sistema.
    - Custo envolvido na reposição do token.
    - Um adversário pode adivinhar o PIN e obter acesso não autorizado.
  - Insatisfação do usuário:

Cartões de memória

- Entre as principais desvantagens estão:
  - Requer leitora especial:
    - Aumenta o custo de utilização do token.
    - Cria o requisito de gerenciar a segurança do hardware e do software da leitora.
  - Perda do token:
    - Impede o usuário de conseguir acesso ao sistema.
    - Custo envolvido na reposição do token.
    - Um adversário pode adivinhar o PIN e obter acesso não autorizado.
  - Insatisfação do usuário:
    - A utilização de cartões para acesso a computadores pode ser inconveniente para algumas pessoas.

Smart cards

- Uma ampla variedade de dispositivos enquadra-se como smart tokens.
- Podem ser categorizados segundo três critérios, que não são mutuamente exclusivos:
  - Características físicas.
  - Interface.
  - Protocolo de autenticação.

Smart cards

Características Físicas

- Smart tokens incluem um microprocessador embutido.
- Smart tokens parecidos com cartões são denominados smart cards.
- Outros poem ser parecidos com calculadoras, chaves ou outros pequenos objetos portáteis.

Smart cards

Smart cards

Interface

- Interfaces manuais incluem teclado e visor para a interação entre ser humano e token.
- Smart tokens com interface eletrônica comunicam-se com uma leitora/gravadora compatível.

Smart cards

Protocolo de autenticação

- A finalidade de um smart token é prover um meio de autenticação de usuário. O protocolo pode ser enquadrado como:
  - Estático: o usuário autentica-se para com o token e o token autentica o usuário para o computador.
  - Gerador de senha: o token gera uma senha periodicamente, que deve ser digitada no sistema computacional.
    - Requer sincronização do token e do sistema.
  - Desafio/resposta: o sistema computacional gera um desafio e o token gera uma resposta baseada no desafio.
    - Por exemplo, a criptografia de chave pública poderia ser utilizada.

Autenticação biométrica

- Um sistema de autenticação biométrica tenta autenticar o indivíduo baseado em características físicas únicas:
  - Impressões digitais.
  - Geometria da mão.
  - Características faciais e padrões de retina e irias.
  - Características dinâmicas como voz e assinatura.
- Basicamente: reconhecimento de padrões.
- Ainda precisa amadurecer para tornar-se a ferramenta padrão para autenticação de usuários em um sistema.

Características físicas

- Há vários tipos de características físicas diferentes em uso ou em estudo para autenticação.
- Veremos algumas delas.

Características físicas

Características faciais

- Meio mais comum de identificação de seres humanos, é natural considerá-las como método de autenticação.
- Abordagem mais comum: definir características com base na localização relativa e na forma de aspectos faciais.
  - Olhos, sobrancelhas, nariz, lábios, formato do queixo.
- Pode-se também utilizar uma câmera infravermelha para produzir um termograma da face que está correlacionado com o sistema vascular do indivíduo.

Características físicas

Impressões digitais

- Utilizadas como método de autenticação há séculos.
- Informatizada e sistematizada particularmente para finalidades policiais.
- Na prática o sistema de reconhecimento e verificação de impressões extrai diversas características da impressão que são armazenados como números.

Características físicas

Geometria da mão

- Sistemas de geometria da mão identificam aspectos da mão.
- Forma, comprimento e largura dos dedos.

Características físicas

Padrão da retina

- O padrão formado por veias abaixo a superfície da retina é único e, por conseguinte, adequado para identificação.
- Um sistema biométrico de exame de retina obtém uma imagem digital do padrão da retina.
- Utiliza facho de baixa intensidade de luz.

Características físicas

Iris

- Outra característica física é a estrutura da iris.

Características físicas

Assinatura

- Cada indivíduo tem o seu estilo de escrita, e isto é refletido principalmente na assinatura.
- No entanto, várias amostras de um mesmo indivíduo não serão idênticas.
- Isto complica a tarefa de desenvolver uma representação em um computador da assinatura que possa ser comparada com amostras futuras.

Características físicas

Voz

- O estilo da assinatura revela os atributos físicos e hábitos da escrita que a pessoa desenvolveu.
- A voz está basicamente vinculada com características físicas e anatômicas do indivíduo.
- Mesmo assim, ao longo do tempo ainda há uma variação de amostra para o mesmo falante, o que complica a tarefa de reconhecimento biométrico.

Características físicas

- Os métodos apresentados anteriormente podem ser enquadrados em uma curva de custo x acurácia.

Características Físicas

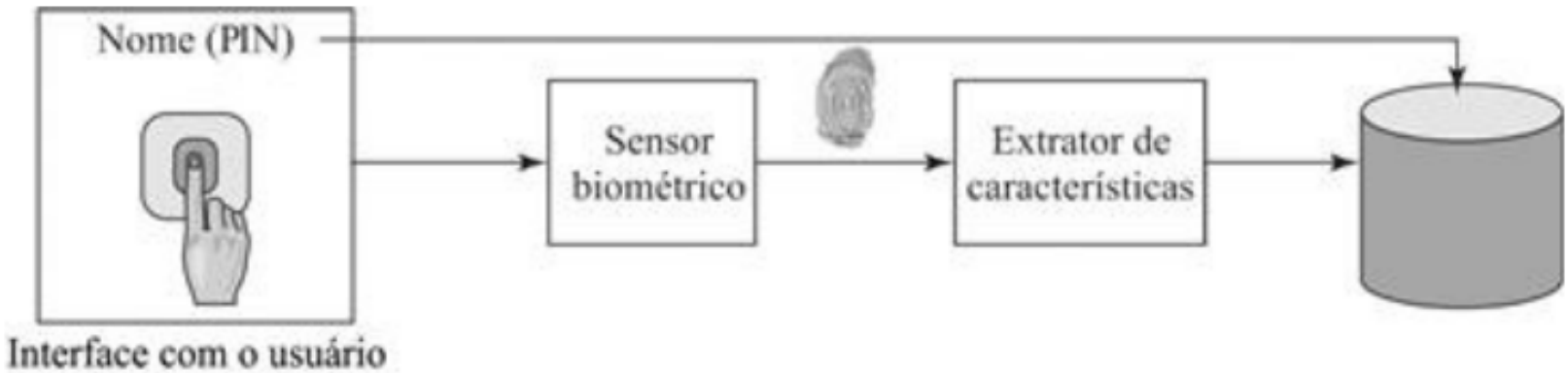
Operação de um sistema de autenticação biométrica

- Cada indivíduo deve ser primeiramente cadastrado em um banco de dados.
- No caso de um sistema biométrico, o usuário apresenta um nome, e normalmente, um PIN ou senha.
- Ao mesmo tempo, o sistema cadastra alguma característica biométrica do usuário de maneira digital.
- Agora o usuário está registrado no sistema, que mantém o nome, possivelmente um PIN ou senha e o valor biométrico.

Operação de um sistema de autenticação biométrica

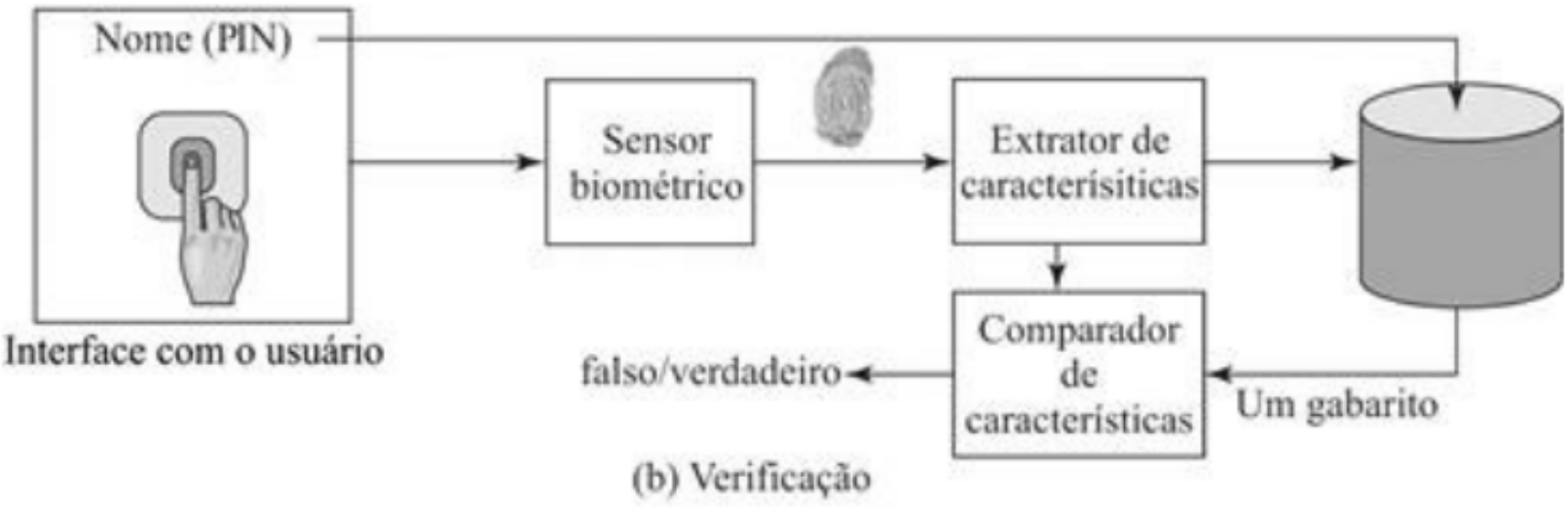
- Dependendo da aplicação, a autenticação do usuário envolve verificação ou identificação.
- Verificação: o sistema extrai a característica do usuário e compara com o gabarito armazenado, em caso de correspondência, o sistema autentica o usuário.
- Identificação: o indivíduo usa o sensor biométrico e não provê nenhuma outra informação adicional. O sistema compara o gabarito apresentado com o conjunto de gabaritos armazenados. Se houver correspondência, o usuário é identificado, caso contrário, ele é rejeitado.

Operação de um sistema de autenticação biométrica



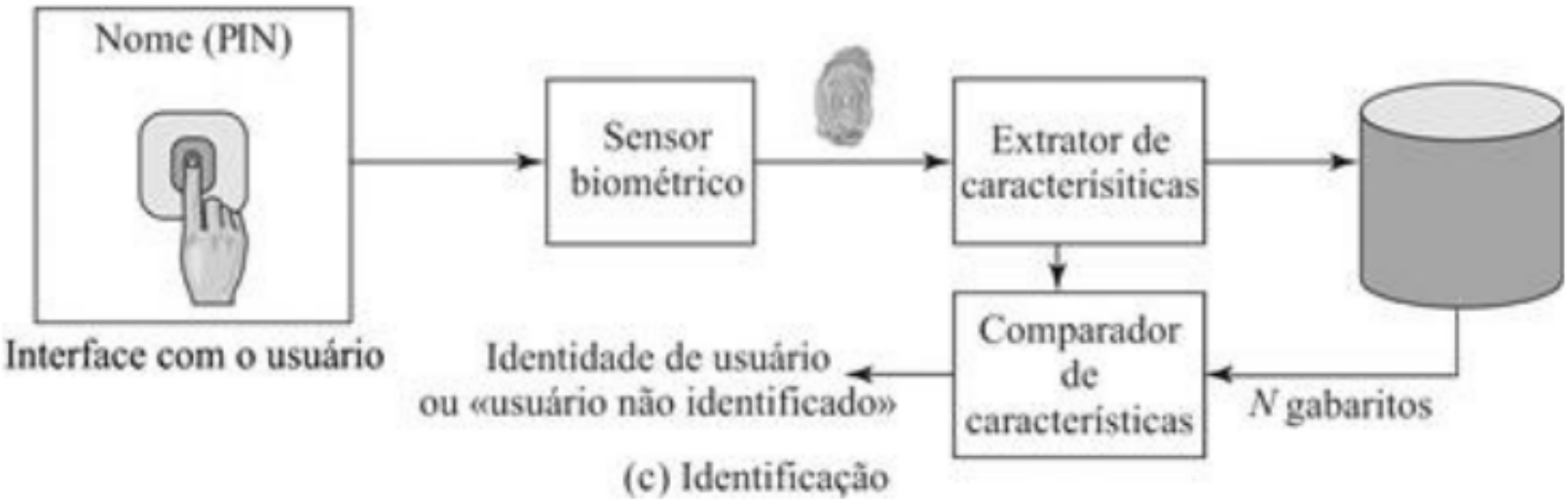
(a) Registro

Operação de um sistema de autenticação biométrica



(b) Verificação

Operação de um sistema de autenticação biométrica



Questões de segurança para autenticação de usuários

- Como qualquer outro serviço, a autenticação de usuários remotos está sujeita a uma variedade de ataques.
- Veremos os principais tipos de ataque.

Questões de segurança para autenticação de usuários

Ataques ao cliente

- Neste tipo de ataque, o adversário tenta ser autenticado com sucesso sem ter acesso ao sistema remoto ou ao caminho de comunicação utilizado.
- Basicamente, o atacante tenta se passar por um usuário legítimo (personificação).
- Para um sistema baseado em senha, o adversário pode tentar adivinhar a senha do usuário.
- No caso extremo, o adversário testa todas as senhas possíveis.

Questões de segurança para autenticação de usuários

Ataques ao cliente: contramedidas

- Seleção de senhas compridas.
- Limite no número de tentativas.
- Tokens podem ser utilizados para gerar códigos de alta entropia a partir de senhas ou PIN de baixa entropia.
- Mesmo conseguindo adivinhar a senha ou o PIN nesta modalidade, o adversário teria que obter o token.

Questões de segurança para autenticação de usuários

Ataques ao sistema

- Ataques a sistema são dirigidos ao arquivo de usuários no sistema onde estão armazenados senhas, códigos de acesso de tokens ou gabaritos biométricos.

Questões de segurança para autenticação de usuários

Ataques ao sistema: contramedidas

- Senhas: já vimos mecanismos anteriormente.
- Tokens: utilizando códigos de acesso de uso único.
- Biometria estática: difícil garantir segurança, pois são atributos físicos.
- Biometria dinâmica: protocolos desafio/resposta.

Questões de segurança para autenticação de usuários

Escuta

- Escuta: refere-se à tentativa do adversário de descobrir a senha ao observar o usuário, procurando e achando uma cópia escrita da senha ou algum ataque que envolva proximidade física entre usuário e adversário.
- Keylogger.
- Roubo do token.
- Cópia de parâmetros biométricos.

Questões de segurança para autenticação de usuários

Escuta: contramedidas

- Keylogger: utilizar senha + outro fator (token ou biometria).
- Roubo do Token: protocolo multifator.
- Biometria estática: autenticação do dispositivo.
- Biometria dinâmica: protocolo desafio/resposta.

Questões de segurança para autenticação de usuários

Trojan

- Uma aplicação ou dispositivo se disfarça como aplicação ou dispositivo autêntico.
- Finalidade: capturar senha, código de acesso ou leitura biométrica.
- Possibilita o adversário personificar o usuário legítimo.
- Ex: chupacabra.

Questões de segurança para autenticação de usuários

Trojan: contramedidas

- Dispositivo de captura dentro do perímetro de segurança confiável.

Questões de segurança para autenticação de usuários

Negação de serviço

- Tenta incapacitar um serviço de autenticação de usuário inundando o serviço com numerosas tentativas de autenticação.

Questões de segurança para autenticação de usuários

Negação de serviço: contramedida

- Autenticação multi-fator que inclui um token frustra este ataque.
- O adversário deve possuir o token para conseguir realizar uma tentativa de autenticação.