Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Como evitar?

A melhor proteção contra esse ataque é ter um mecanismo de bloqueio da conta do usuário após uma determinada quantidade de tentativas de autenticação mal sucedidas.

Combinações de senhas conforme comprimento e complexidade

Formação da senha	6 caracteres	8 caracteres	12 caracteres

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Como evitar?

A melhor proteção contra esse ataque é ter um mecanismo de bloqueio da conta do usuário após uma determinada quantidade de tentativas de autenticação mal sucedidas.

Combinações de senhas conforme comprimento e complexidade

Formação da senha	6 caracteres	8 caracteres	12 caracteres
Minúsculas e maiúsculas	19 bilhões	53 trilhões	390 quintilhões

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Como evitar?

A melhor proteção contra esse ataque é ter um mecanismo de bloqueio da conta do usuário após uma determinada quantidade de tentativas de autenticação mal sucedidas.

Combinações de senhas conforme comprimento e complexidade

Formação da senha	6 caracteres	8 caracteres	12 caracteres
Minúsculas e maiúsculas	19 bilhões	53 trilhões	390 quintilhões
Minúsculas, maiúsculas e números	56 bilhões	218 trilhões	3 sextilhões

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Como evitar?

A melhor proteção contra esse ataque é ter um mecanismo de bloqueio da conta do usuário após uma determinada quantidade de tentativas de autenticação mal sucedidas.

Combinações de senhas conforme comprimento e complexidade

Formação da senha	6 caracteres	8 caracteres	12 caracteres
Minúsculas e maiúsculas	19 bilhões	53 trilhões	390 quintilhões
Minúsculas, maiúsculas e números	56 bilhões	218 trilhões	3 sextilhões
Minúsculas, maiúsculas, números e caracteres especiais	646 bilhões	5 quadrilhões	418 sextilhões

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário

Ataque de força bruta

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Já há alguns anos existem soluções de baixo custo para criar sistemas poderosos para quebrar senhas. Atualmente placas de vídeo são otimizadas para quebrar senhas em alta velocidade. Com o uso dessas placas já foi construído um computador doméstico que consegue calcular até 350 bilhões de senhas por segundo.

Tempo para quebrar uma senha conforme comprimento e complexidade

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Já há alguns anos existem soluções de baixo custo para criar sistemas poderosos para quebrar senhas. Atualmente placas de vídeo são otimizadas para quebrar senhas em alta velocidade. Com o uso dessas placas já foi construído um computador doméstico que consegue calcular até 350 bilhões de senhas por segundo.

Tempo para quebrar uma senha conforme comprimento e complexidade

Formação da senha	6 caracteres	8 caracteres	12 caracteres

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Já há alguns anos existem soluções de baixo custo para criar sistemas poderosos para quebrar senhas. Atualmente placas de vídeo são otimizadas para quebrar senhas em alta velocidade. Com o uso dessas placas já foi construído um computador doméstico que consegue calcular até 350 bilhões de senhas por segundo.

Tempo para quebrar uma senha conforme comprimento e complexidade

Formação da senha	6 caracteres	8 caracteres	12 caracteres
Minúsculas e maiúsculas	Menos de 1 segundo	2 minutos	35 anos

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Já há alguns anos existem soluções de baixo custo para criar sistemas poderosos para quebrar senhas. Atualmente placas de vídeo são otimizadas para quebrar senhas em alta velocidade. Com o uso dessas placas já foi construído um computador doméstico que consegue calcular até 350 bilhões de senhas por segundo.

Tempo para quebrar uma senha conforme comprimento e complexidade

Formação da senha	6 caracteres	8 caracteres	12 caracteres
Minúsculas e maiúsculas	Menos de 1 segundo	2 minutos	35 anos
Minúsculas, maiúsculas e números	Menos de 1 segundo	10 minutos	292 anos

Segurança nos sistemas de autenticação

Adivinhar a senha do usuário
Ataque de força bruta

Já há alguns anos existem soluções de baixo custo para criar sistemas poderosos para quebrar senhas. Atualmente placas de vídeo são otimizadas para quebrar senhas em alta velocidade. Com o uso dessas placas já foi construído um computador doméstico que consegue calcular até 350 bilhões de senhas por segundo.

Tempo para quebrar uma senha conforme comprimento e complexidade

Formação da senha	6 caracteres	8 caracteres	12 caracteres
Minúsculas e maiúsculas	Menos de 1 segundo	2 minutos	35 anos
Minúsculas, maiúsculas e números	Menos de 1 segundo	10 minutos	292 anos
Minúsculas, maiúsculas, números e caracteres especiais	2 segundos	4 horas	37924 anos

Segurança nos sistemas de autenticação

Acessar o repositório onde as senhas estão armazenadas

Segurança nos sistemas de autenticação

Acessar o repositório onde as senhas estão armazenadas

Acessar o arquivo de senhas e roubar todas as senhas de um sistema é um dos ataques mais bem sucedidos que pode ser feito. Sabendo disso, os sistemas geralmente possuem restrição de acesso para o arquivo onde as senhas são armazenadas. A maioria dos sistemas também utiliza algum tipo de codificação nas senhas (hash) para dificultar que a senha original seja descoberta caso algum usuário não autorizado tenha acesso ao arquivo com as senhas.

Segurança nos sistemas de autenticação

Acessar o repositório onde as senhas estão armazenadas

Acessar o arquivo de senhas e roubar todas as senhas de um sistema é um dos ataques mais bem sucedidos que pode ser feito. Sabendo disso, os sistemas geralmente possuem restrição de acesso para o arquivo onde as senhas são armazenadas. A maioria dos sistemas também utiliza algum tipo de codificação nas senhas (hash) para dificultar que a senha original seja descoberta caso algum usuário não autorizado tenha acesso ao arquivo com as senhas.

Este tipo de ataque pode ser explorado de diversas formas: encontrar falhas no controle de acesso ao arquivo de senhas; conseguir acesso como um usuário com alto privilégio e acessar o arquivo de senhas de forma não autorizada; encontrar sistemas que não armazenam as senhas codificadas ou que utilizam codificação fraca; efetuar criptoanálise nas senhas criptografadas, entre outros.

Segurança nos sistemas de autenticação

Acessar o repositório onde as senhas estão armazenadas

Caso o ataque tenha sucesso e seja possível acessar o arquivo com as senhas codificadas, pode- se tentar quebrar as senhas com um computador local, ou utilizar recursos online.

Segurança nos sistemas de autenticação

Acessar o repositório onde as senhas estão armazenadas

Caso o ataque tenha sucesso e seja possível acessar o arquivo com as senhas codificadas, pode- se tentar quebrar as senhas com um computador local, ou utilizar recursos online.

http://www.md5online.org/

http://www.md5crack.com/

http://crackhash.com/

https://www.cloudcracker.com/

Segurança nos sistemas de autenticação

Acessar o repositório onde as senhas estão armazenadas

Caso o ataque tenha sucesso e seja possível acessar o arquivo com as senhas codificadas, pode- se tentar quebrar as senhas com um computador local, ou utilizar recursos online.

http://www.md5online.org/

http://www.md5crack.com/

http://crackhash.com/

https://www.cloudcracker.com/

Como evitar?

A melhor proteção contra esse ataque é ter um mecanismo efetivo de segurança no sistema operacional, ou no banco de dados, para impedir acessos indevidos ao repositório de senhas.

Segurança nos sistemas de autenticação

Capturar a senha digitada pelo usuário

Nesse caso o recurso utilizado é infectar ou invadir o computador de um usuário e instalar um software para capturar tudo que o usuário digitar, inclusive as senhas para acesso ao equipamento ou sistema que se deseja atacar.

Segurança nos sistemas de autenticação

Capturar a senha digitada pelo usuário

Nesse caso o recurso utilizado é infectar ou invadir o computador de um usuário e instalar um software para capturar tudo que o usuário digitar, inclusive as senhas para acesso ao equipamento ou sistema que se deseja atacar.

Diversos ataques para descobrir as senhas muitas vezes não atacam diretamente o sistema de autenticação, e sim outras partes do sistema para ter acesso a senha do usuário, como um keylogger (programa utilizado para capturar as senhas digitadas no teclado), mouselogger (programa utilizado para capturar os movimentos e cliques no mouse) e screenlogger (programa utilizado para capturar a tela do usuário quando, por exemplo, ele estiver digitando a senha em um teclado virtual). É importante ressaltar que keylogger, mouselogger e screenlogger existem também para os dispositivos móveis como celular, smartphone e tablets.

Segurança nos sistemas de autenticação

Capturar a senha digitada pelo usuário

Segurança nos sistemas de autenticação

Capturar a senha digitada pelo usuário

Pessoas ou câmeras observando o usuário quando ele digita sua senha;

Segurança nos sistemas de autenticação

Capturar a senha digitada pelo usuário

Pessoas ou câmeras observando o usuário quando ele digita sua senha;

Pessoas ouvindo quando alguém fala sua senha ao telefone;

Segurança nos sistemas de autenticação

Capturar a senha digitada pelo usuário

Pessoas ou câmeras observando o usuário quando ele digita sua senha;

Pessoas ouvindo quando alguém fala sua senha ao telefone;

Usuários que deixam suas senhas anotadas em algum lugar visível;

Segurança nos sistemas de autenticação

Capturar a senha digitada pelo usuário

Pessoas ou câmeras observando o usuário quando ele digita sua senha;

Pessoas ouvindo quando alguém fala sua senha ao telefone;

Usuários que deixam suas senhas anotadas em algum lugar visível;

Usuários que compartilham suas senhas com pessoas "confiáveis" e essas senhas acabam repassando as senhas para pessoas "não confiáveis";

Segurança nos sistemas de autenticação

Capturar a senha digitada pelo usuário

Pessoas ou câmeras observando o usuário quando ele digita sua senha;

Pessoas ouvindo quando alguém fala sua senha ao telefone;

Usuários que deixam suas senhas anotadas em algum lugar visível;

Usuários que compartilham suas senhas com pessoas "confiáveis" e essas senhas acabam repassando as senhas para pessoas "não confiáveis";

Equipamentos que capturam senhas não criptografadas na rede;

Segurança nos sistemas de autenticação

Capturar a senha digitada pelo usuário

Pessoas ou câmeras observando o usuário quando ele digita sua senha;

Pessoas ouvindo quando alguém fala sua senha ao telefone;

Usuários que deixam suas senhas anotadas em algum lugar visível;

Usuários que compartilham suas senhas com pessoas "confiáveis" e essas senhas acabam repassando as senhas para pessoas "não confiáveis";

Equipamentos que capturam senhas não criptografadas na rede;

Usuários que são vítimas de ataque de engenharia social e fornecem suas senhas ou informações pessoais para o atacante.

Segurança nos sistemas de autenticação

Impedir o acesso de usuários legítimos

Um usuário mal intencionado, quando deseja impedir que um usuário legítimo faça sua autenticação, executa o ataque contra esse usuário e realiza diversas tentativas de autenticação mal sucedidas com a conta do usuário até bloquear o seu acesso, impedindo assim que o usuário legítimo acesse o sistema.

Segurança nos sistemas de autenticação

Burlar o mecanismo de recuperação de senha

Seja pelo envio de emails, URLs especiais, senhas temporárias, perguntas de caráter pessoal, recuperação da senha já existente, ou resetar a senha pra um novo valor, a maioria dos sistemas tem algum tipo de falha na implementação ou dependem de uma informação pouco confiável para permitir a recuperação de senhas.

Segurança nos sistemas de autenticação

Burlar o mecanismo de recuperação de senha

Seja pelo envio de emails, URLs especiais, senhas temporárias, perguntas de caráter pessoal, recuperação da senha já existente, ou resetar a senha pra um novo valor, a maioria dos sistemas tem algum tipo de falha na implementação ou dependem de uma informação pouco confiável para permitir a recuperação de senhas.

É recomendado que o mecanismo de recuperação de senhas utilize um conjunto de informações tanto de cunho pessoal, como configuradas pelo usuário, para ser considerado mais seguro.

Segurança nos sistemas de autenticação

Roubar sessões/credenciais válidas

Os ataques que visam roubar sessões válidas geralmente capturam pacotes não criptografados em uma rede com o auxílio de um sniffer. Ou então, usam de e-mails, mensagens ou sites falsos, como o Phishing ou a Engenharia Social.

Segurança nos sistemas de autenticação

Ferramentas de ataque

John The Ripper. **http://www.openwall.com/john/**

Crack. **http://www.users.dircon.co.uk/~crypto/index.html**

Brutus. **http://www.hoobie.net/brutus/**

Slurpie. **http://www.ussrback.com/distributed.htm**

Cain and Abel. **http://www.oxid.it/cain.html**

THC Hydra. **http://www.thc.org/thc-hydra/**

L0pht Crack. **http://www.l0phtcrack.com/**

Rainbow Crack. **http://project-rainbowcrack.com/**

Segurança nos sistemas de autenticação

Recomendações para criação de senhas fortes

Segurança nos sistemas de autenticação

Recomendações para criação de senhas fortes

Uma senha forte não deve ser baseada em informações pessoais como: nome do usuário, nome da empresa, número de identidade, data de aniversário, número do telefone, etc. Um atacante determinado pode encontrar uma grande quantidade de informações pessoais sobre qualquer indivíduo nas redes sociais e na área de recursos humanos da empresa onde se trabalha.

Segurança nos sistemas de autenticação

Recomendações para criação de senhas fortes

Uma senha forte não deve ser baseada em informações pessoais como: nome do usuário, nome da empresa, número de identidade, data de aniversário, número do telefone, etc. Um atacante determinado pode encontrar uma grande quantidade de informações pessoais sobre qualquer indivíduo nas redes sociais e na área de recursos humanos da empresa onde se trabalha.

Não devem ser criadas senhas que possuam só um tipo de caractere, como senhas que tem somente números, ou senhas que tenham somente letras. Não devem ser utilizadas palavras comuns que podem ser encontradas em qualquer dicionário, por exemplo, a palavra “voluntario”. A substituição de letras por números, como por exemplo “v0lunt4r10”, não ajuda muito pois ferramentas de quebra de senha também testam essa técnica de substituição em suas tentativas de ataque.

Segurança nos sistemas de autenticação

Recomendações para criação de senhas fortes

Uma senha forte não deve ser baseada em informações pessoais como: nome do usuário, nome da empresa, número de identidade, data de aniversário, número do telefone, etc. Um atacante determinado pode encontrar uma grande quantidade de informações pessoais sobre qualquer indivíduo nas redes sociais e na área de recursos humanos da empresa onde se trabalha.

Não devem ser criadas senhas que possuam só um tipo de caractere, como senhas que tem somente números, ou senhas que tenham somente letras. Não devem ser utilizadas palavras comuns que podem ser encontradas em qualquer dicionário, por exemplo, a palavra “voluntario”. A substituição de letras por números, como por exemplo “v0lunt4r10”, não ajuda muito pois ferramentas de quebra de senha também testam essa técnica de substituição em suas tentativas de ataque.

Uma senha forte é uma senha única, com comprimento de 8 ou mais posições, ela deve ser criativa, difícil de ser descoberta por outra pessoa, mas que seja fácil de ser lembrada por parte do usuário. Uma prática comum para criar senhas fortes é a de utilizar as primeiras letras de uma frase em conjunto com alguns caracteres especiais.