Segurança da Informação: Autenticidade

Prof. Renato da Costa

Autenticação X Autorização

Autenticação: garantia de que a pessoa é realmente quem diz ser, prova de identidade.

Autorização: garantia de que as pessoas não executarão qualquer ação que não possuam permissão. A autorização determina as capacidades reais de um usuário.

Disponibilidade: garantir que um recurso esteja disponível sempre que necessário.

As definições numeradas de I a V correspondem, respectivamente, a:

a) Integridade; Autenticação; Autorização; Acessabilidade; Não repúdio.

b) Identificação; Raio de Ação; Autorização; Acessabilidade; Negação.

c) Autenticação; Autorização; Integridade; Confidencialidade; Não repúdio.

d) Autenticação; Raio de Ação; Integridade; Confidencialidade; Identificação.

e) Integridade; Confidencialidade; Autenticação; Autorização; Negação.

Sefaz RS - 2019

Para o estabelecimento de padrões de segurança, um dos princípios críticos é a necessidade de se verificar a legitimidade de uma comunicação, de uma transação ou de um acesso a algum serviço. Esse princípio refere-se à

a)confidencialidade.
b)autenticidade.
c)integridade.
d)conformidade.
e)disponibilidade.

Autenticar é confirmar a identidade de uma entidade visando, por exemplo, garantir que a entidade é quem ela diz ser. As técnicas para autenticação podem basear-se na verificação de informações como, por exemplo, senhas.

( )CERTA ( )ERRADA

Uso de Senhas

Uma senha se tornará frágil, ou será fácil de ser descoberta, caso na sua elaboração utilize

(A) um código, que seja trocado regularmente.
(B) pelo menos 8 caracteres entre letras, números e símbolos.
(C) nomes próprios ou palavras contidas em dicionários.
(D) um código fácil de ser lembrado.
(E) um código simples de digitar.

Assinale, entre as senhas apresentadas nas opções a seguir, a que é considerada mais segura, segundo as regras e os cuidados especiais pertinentes.

A) 2210Carlos, de Carlos Silva que faz aniversário em 22 de outubro

B) 139002, de um usuário cuja conta é 13900-2

C) Acvnd12d03, a partir da frase “A conta venceu no dia 12 de março”

D) Flamengo2009

E) 1122334455

A segurança digital visa proteger dados e documentos pessoais. Pensando nisso, foi criado o conceito de senha. Uma senha ou palavra-chave (por vezes, referida no inglês password) é uma palavra ou uma ação secreta, previamente convencionada entre duas partes como forma de reconhecimento. Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema. Qual alternativa abaixo NÃO deve ser utilizada como senha por não ser segura?

a) Palavras com pontuação e letras maiúsculas e minúsculas.
b) Letras com símbolos.
c) Iniciais de uma frase ou poema.
d) Letras e números.
e) Palavras do dicionário.

http://cartilha.cert.br/senhas/

Reutilizar as senhas: usar a mesma senha para acessar diferentes contas pode ser bastante arriscado, pois basta ao atacante conseguir a senha de uma conta para conseguir acessar as demais contas onde esta mesma senha foi usada.

- *procure não usar a mesma senha para assuntos pessoais e profissionais;*
- *jamais reutilize senhas que envolvam o acesso a dados sensíveis, como as usadas em Internet Banking ou e-mail.*

Das opções abaixo, o método MENOS aconselhável a ser utilizado como forma de gerenciamento de senhas pessoais é

a) anotar as contas e senhas em um papel e guardá-lo em um local seguro, como um cofre ou gaveta trancada.

b) usar um programa gerenciador de senhas que permite armazenar senhas em um único arquivo acessível por meio de uma chave mestra.

c)usar opções como "Lembre-se de mim" e "Continuar conectado" em sites da web.

d) gravar suas contas e senhas em um arquivo criptografado no computador e manter um backup deste arquivo em outro computador.

e)criar grupos de senhas de complexidade diferente, de acordo com o risco envolvido.

Uma senha serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na internet devido, principalmente, à simplicidade que possui. São consideradas boas práticas de segurança para protegê-la, EXCETO:

a) Criar uma senha forte e utilizá-la para assuntos pessoais e profissionais.

b) Certificar-se de encerrar uma sessão ao acessar sites que requeiram uso de senhas.

c) Certificar-se do uso de serviços criptografados quando o acesso a um site envolver fornecimento de senha.

d) Utilizar a verificação em duas etapas, pois adiciona uma segunda camada de proteção no acesso a uma conta.

Das opções abaixo, o método MENOS aconselhável a ser utilizado como forma de gerenciamento de senhas pessoais é

a) anotar as contas e senhas em um papel e guardá-lo em um local seguro, como um cofre ou gaveta trancada.

b) usar um programa gerenciador de senhas que permite armazenar senhas em um único arquivo acessível por meio de uma chave mestra.

c)usar opções como "Lembre-se de mim" e "Continuar conectado" em sites da web.

d) gravar suas contas e senhas em um arquivo criptografado no computador e manter um backup deste arquivo em outro computador.

e)criar grupos de senhas de complexidade diferente, de acordo com o risco envolvido.

Maria está trabalhando na definição de uma política de senhas para um site. Já está estabelecido que as senhas devem conter quatro caracteres; que será considerado um alfabeto com 26 letras; e que os caracteres especiais serão limitados à lista abaixo.

!@#$%&*=+

A partir disso, Maria imaginou três alternativas, cada uma com distintos requisitos mínimos obrigatórios que devem ser observados na criação de uma senha, a saber:

I. pelo menos uma letra maiúscula, pelo menos um caractere especial;
II. pelo menos uma letra minúscula, pelo menos um dígito numérico;
III. pelo menos uma letra maiúscula, pelo menos uma letra minúscula.

...

...

Considerando que os usuários escolham suas senhas aleatoriamente, a ordem das políticas, da mais forte para a mais fraca, é:

A) I, II, III;
B) I, III, II;
C) II, I, III;
D) II, III, I;
E) III, II, I.

...

Considerando que os usuários escolham suas senhas aleatoriamente, a ordem das políticas, da mais forte para a mais fraca, é:

A) I, II, III;

B) I, III, II;

C) II, I, III;

D) II, III, I;

E) III, II, I.

Biometria

Informática
Prof. Renato da Costa

Ministério da Saúde

O controle de acesso, que é uma das formas de assegurar que somente pessoas autorizadas acessem determinada informação, pode ser realizado mediante o uso de dados biométricos.
( )CERTA ( )ERRADA

Embasa

Em um sistema de controle de acesso, os usuários podem ser autenticados usando-se biometria, que necessariamente consiste em fazer a digitalização e o reconhecimento de impressões digitais e é considerada uma das formas mais precisas e efetivas de autenticação.
( )CERTA ( )ERRADA

- Fatores de Autenticação
- Autenticação Forte
- Autenticação em duas etapas

Os controles de acesso ~~biométricos~~ são usados considerando- se algumas características principais sobre os usuários, que são:
(A) função, onde trabalha e identificação.
(B) o que sabe, o que é e o que tem.
(C) o que sabe, o que faz e o que tem.
(D) o que sabe, o que conhece e onde trabalha.
(E) o que tem, o que sabe e o que pode fazer

Fatores de Autenticação

- Algo que você tem
- Algo que você sabe
- Algo que você é

Observe o seguinte diálogo:

João: Sr. Gerente, sou usuário iniciante de computadores. Estou aprendendo a realizar transações bancárias pela Internet, mas estou com muito receio em relação à segurança do site do banco. Poderia me ajudar?

Gerente do Banco: Claro, Sr. João. Para confirmar a realização de uma transação, você deve utilizar uma senha, definida por você mesmo, e usar um cartão de segurança, com códigos previamente definidos, emitido pelo banco.

...

...

A forma de autenticação que combina uma senha pessoal e um cartão de segurança oferecida pelo Gerente do Banco de João é:

(A) Single sign-on;
(B) Senha forte;
(C) Certificado digital;
(D) Verificação em duas etapas;
(E) Token.

BNDES

Qual opção apresenta um conjunto de métodos que caracteriza uma autenticação forte?

(A) Utilização de senha, dados pessoais aleatórios e PIN.

(B) Reconhecimento de retina e impressão digital.

(C) Uso de crachá magnético, chave física e crachá com código de barras.

(D) Reconhecimento facial e de íris.

(E) Reconhecimento de padrão de voz e utilização de senha.

Polícia Federal - 2018

Na autenticação em dois fatores, necessariamente, o primeiro fator de autenticação será algo que o usuário possui — por exemplo, um token gerador de senhas — e o segundo, alguma informação biométrica, como, por exemplo, impressão digital ou geometria da face reconhecida.

( ) CERTA ( ) ERRADA

Obrigado

Prof. Renato da Costa
@prof.renatodacosta