terça-feira, 25 de outubro de 2022

Lista de Atividades

Nome: Murilo Fuza da Cunha

---

1) Descreva os serviços de segurança necessários (Confidencialidade, Integridade, Autenticidade, Irretratabilidade e/ou Disponibilidade) para as informações identificadas em itálico nos seguintes cenários. Justifique.

a) Enzo quer assistir o episódio de seu seriado favorito, que será exibido pela Internet no site de uma emissora aberta de TV.

R: Disponibilidade, garantindo que o sinal de tv aberta esteja disponível para ser visualizado no site.

b) Luiza quer contar um segredo para Tavarez utilizando a Internet, de forma que somente os dois tenham acesso às informações contidas nas conversas.

R: Confidencialidade e Integridade. De modo que a confidencilidade atue para que apenas eles tenham acesso ao real conteúdo da mensagem e integridade para que a mensagem chegue corretamente ao destino.

c) Daniel quer baixar um jogo novo, porém, quer ter certeza que nenhum dado foi perdido na transmissão e que a imagem recebida é validada pela empresa que o desenvolve.

R: Integridade e Autenticidade. Daniel poderá verificar se todos os dados que deveriam ser baixados, foram de fato entregues na sua máquina e autenticidade para garantir que todos os pacotes recebidos, pertencem a empresa que ele requisitou o jogo.

d) Amanda aceitou comprar um produto de Tiago, porém, ela gostaria de utilizar um contrato que ele não pudesse voltar atrás quanto sua assinatura e autoria.

R: Irretratabilidade e Autenticidade. Amanda utilizará da irritabilidade para que possa ser firmado o contrato sem que possa ser “desmentida" a compra, garantindo que Tiago não voltara atrás com sua palavra. Autenticidade para garantir que o contrato foi realmente assinado por Tiago.

2) Dentre os algoritmos abaixo, qual (ou quais) você usaria em cada um dos casos da Questão 1 para prover estes serviços?

- Cifras: RC4, DES, 3DES, AES.
- Funções de hash: MD5, SHA-1, SHA-2, SHA-3.

- Código de Autenticação de Mensagens (MAC): CMAC, HMAC.
- Algoritmos assimétricos: Protocolo Diffie-Helmann, assinatura RSA.
- Outros...

A) Serviço: Disponibilidade Algoritmo: Como não possui algoritmo, é interessante utilizar de redundâncias, para que mesmo que algum problema ocorra no provedor, sendo ele elétrico ou de infraestrutura, o serviço se mantenha disponível para visualização.

B) Serviço: Confidencialidade e Integridade. Algoritmo: Para integridade o Argon2 e para confidencialidade o HMAC.

C) Serviço: Integridade e Autenticidade Algoritmo: Para a integridade o Argon2 e para autenticidade o HMAC.

D) Serviço: Irretratabilidade e Autenticidade Algoritmo: Para a Irretratabilidade o algoritmo DSA de assinatura digital e para autenticidade o HMAC.

3) Quais são as principais formas de autenticação de usuários? Como proteger a forma de autenticação mais difundida na atualidade contra ataques cibernéticos?

R: As principais formas são: Biometria, Reconhecimento Facial, Token de Autenticação, chave eletrônica, padrão e pin.

Sendo a autenticação por senha a mais difundida e utilizada atualmente, uma forma de proteger seria com a pré comunicação entre servidor e usuário para que seja estabelecido um canal único de comunicação e gere assim um token de autenticidade e hash para que ao enviar uma senha com um esquema segura de hashing ele possa ser verificado com tal token aleatório que foi gerado anteriormente.

4) Qual a diferença entre um MAC e uma função Hash?

R: A principal diferença é a necessidade de uma chave de texto simples para que o MAC funcione, diferentemente do hash (argon2) que gera uma chave após o processo de hashing.

5) Qual a diferença entre um MAC e algoritmos de cifragem?

R: A diferença está na utilização da chave, onde o MAC envia a mensagem as claras e pois verifica sua autenticidade e integridade com o processo de hashing no recebimento, já a cifragem envia a mensagem cifrada (não entendível) para que possa ser desfeita tal cifra com a chave que foi enviada,

6) Elenque protocolos/algoritmos criptograficamente seguros para as funções abaixo:

- Cifra de fluxo

  R: RC4

- Cifra de bloco

  R: DES e AES

- Hash

  SHA256, SHA512, Whirlpool e RIPEMD.

- Esquema de hash de senhas

  Argon2, Scrypt e Bcrypt.

  Autenticação de mensagens (MAC)

  R: HMAC e CMAC