Questionário de Revisão II

Ary Felipe Farah e Silva

1. **Quais são os critérios considerados para determinar a segurança de uma técnica de criptografia?**

   Os critérios considerados são:

   - Se o Custo para quebrar a cifração foi **maior** que o valor da informação
   - Se o Tempo para quebrar a cifração foi **maior** que a vida útil da informação.

2. **Por que a criptografia simétrica continua sendo amplamente utilizada, mesmo após décadas de existência?**

   Porque a Criptografia Simétrica não está obsoleta. A segurança do método está relacionada com o comprimento da chave e esforço necessário para quebrar uma cifra, não com a sua data de criação. Além disso, possui um mecanismo de distribuição de chaves mais simples.

3. **Explique o conceito de cifragem com chave privada e como ele pode garantir a autenticidade de uma mensagem.**

   A cifragem com chave privada é uma técnica para manter confidencialidade em dados transmitidos/armazenados. Um texto é cifrado com uma chave, e a mesma é utilizada para decifrá-lo. O remetente e destinatário devem possuí-la e mantê-la segura.

4. **Descreva o processo de comunicação entre Alice e Bob por meio de troca de chaves públicas fornecidas por uma Autoridade.**

   a. Bob envia uma mensagem cifrada na **PU***autoridade* para a Autoridade, solicitando a **PU***alice*.

b. Autoridade responde a mensagem cifrada na **PR***autoridade.* A mensagem contém a chave pública de Alice.

c. Bob armazena **PU***alice* e a utiliza para cifrar a mensagem para Alice. A mensagem contém um identificador de Bob.

d. Alice solicita a PU*bob* para a Autoridade, seguindo o mesmo procedimento. (Ambos possuem chaves públicas)

e. Alice gera um *nonce* e encaminha para Bob, cifrando na PU*bob*.

f. Bob responde Alice, executando uma função sobre o nonce recebido, cifrando na PU*alice*.

g. Autoridade responde a mensagem cifrada na **PR***autoridade.* A mensagem contém a chave pública de Alice.

h. Bob armazena **PU***alice* e a utiliza para cifrar a mensagem para Alice. A mensagem contém um identificador de Bob.

i. Alice solicita a PU*bob* para a Autoridade, seguindo o mesmo procedimento. (Ambos possuem chaves públicas)

j. Alice gera um *nonce* e encaminha para Bob, cifrando na PU*bob*.

k. Bob responde Alice, executando uma função sobre o nonce recebido, cifrando na PU*alice*.

5. **Explique as duas abordagens gerais para atacar um esquema de cifração assimétrica e forneça um exemplo de cada uma.**

   Criptoanálise → analisar e explorar amostras dos textos às claras, cifrados e características do algoritmo e tenta deduzir o texto às claras ou a chave usada.

   > **ex**: Ataque de **frequência de letras**. Esse ataque se baseia na ocorrência de letras em um idioma específico. Por exemplo, no Inglês a letra mais comum é o **E**, seguida por **A**, depois por **O**, e assim vai. Cabe ao analista comparar a frequência de letras na mensagem cifrada e no idioma deseja, identificando padrões e deduzindo a chave de criptografia.

   Ataque de Força Bruta → tentar todas as chaves possíveis em um texto cifrado até obter uma tradução inteligível (em média, é necessário tentar

metade de todas as chaves possíveis para obter sucesso)

ex: Um cenário com a **Cifra de César** sendo utilizada. Para descobrir, são usadas 25 chaves diferentes, até que seja possível achar um texto inteligível. (trocar pela próxima letra, trocar por 2 letras a frente, trocar por 3 letras a frente...)

6. **Quais são as premissas que devem ser atendidas para um sistema de criptografia assimétrica ser considerado eficiente?**
   - **Deve ser computacionalmente fácil para:**
     - Uma entidade gerar um par de chaves (pública e privada);
     - Um remetente que conheça a chave cifrar um texto;
     - Um destinatário decifrar um texto para recuperar a mensagem original.
   - **Deve ser computacionalmente inviável que**:
     - Um oponente que conheça a chave pública determinar a chave privada
     - Um oponente que conheça a chave pública e o texto cifrado consiga decifrá-lo
   - Qualquer uma das chaves pode ser utilizada para cifrar, e a outra para decifrar

7. **Explique como as Funções Hash podem ser aplicadas em bancos de dados e estruturas de dados em memória.**
   - Verificam a integridade de dados (hash calculado para um bloco de dados e armazenados para comparar em um futuro acesso)
   - Criar Índices Hash que mapeiam chaves, facilitando na busca de elementos.
   - Evitar a inserção de chaves duplicadas (calcular a posição para ser única)

8. **Qual a importância da integridade de arquivos baixados e como as Funções Hash podem ser utilizadas nesse contexto?**

   A integridade de arquivos baixados oferece:

   - Garantia de autenticidade
   - Evita a corrupção de dados
   - Segurança contra ataques e malware
   - confiança no conteúdo baixado

   As Funções Hash podem verificar a integridade através da comparação do hash que foi fornecido junto com o arquivo com o hash calculado junto com o arquivo baixado. Além disso, existem algorimos que podem calcular esses hashes, como o MD5.

9. **Explique como um ataque em transmissão de mensagem pode ocorrer e como isso afeta a integridade da comunicação.**

   O ataque em transmissão de mensagens pode ocorrer quando um terceiro intercepta a comunicação entre as duas partes. Isso pode afetar a integridade pois possibilita a corrupção de dados e alteração ou falsificação de mensagens, o que pode levar a muitos outros tipos de ataques.

10. **Qual a premissa fundamental de uma Função Hash em relação à segurança da informação?**

    A principal preimssa de uma função hash é que deve ser computacionalmente inviável descobrir o texto às claras a partir do código hash.

11. **Como posso identificar se meu equipamento foi infectado por um código malicioso?**

    Analisando o comportamento do computador, vendo se ele apresenda um desempenho lento, consumo de dados e bateria muito alto, travamentos

recorrentes, programas desconhecidos rodando em segundo plano. Em suspeita de vírus, deve-se rodar um antivírus para escanear o dispositivo na busca de algum malware.

12. **Explique a importância de utilizar apenas programas originais e manter as versões mais recentes dos programas.**

    É importante usar programas originais pois, além da autenticidade e confiança no programa baixados, estes estão sendo atualizados de forma constante, corrigindo patches com vulnerabilidades ou riscos. Cabe ao usuário manter essas versões no seu dispositivo.

13. **Qual a recomendação dada para o uso correto de um antivírus?**

    Instalar o antivírus e configurá-lo para verficar extensões de aquivos, anexos de emails e obtidos na net, discos rígidos e unidades removíveis de forma automática. Além disso, mantê-lo sempre atualizado.

14. **Por que é sugerido criar um disco de emergência do antivírus e manter um firewall pessoal ativo?**

    É recomendado ter um disco de emergência do antivírus para usar quando o antimalware original aparentar estar desabilitado ou comprometido, resultando em um dispositivo com desempenho mais lento ou leitura muito frequente do disco rígido.

    O firewall pessoal tem várias funcionalidades, entre elas o bloqueio de acesso não autorizado, bloqueio de entrada e saída de malware suspeitos, bloqueio de conexões estranhas, prevenção contra ataques de rede, controle de acesso de aplicativos, entre muitos outros.

15. **Quais são os principais meios pelos quais um equipamento pode ser infectado ou comprometido?**

    Os principais meios são: exploração de vulnerabilidades em programas instalados, auto-execução de mídias removíveis infectadas, acesso a páginas web maliciosas via navegadores vulneráveis, ação direta dos atacantes e execução de arquivos previamente infectados, como anexos, links, etc.