Exercícios de Revisão

Criptografia Aplicada

Essas questões referem-se ao RA2

Hash, Assinaturas, Certificados Digitais e TLS

Q1: Suponha que um usuário fez o download de um programa em um site espelho da Microsoft. O site original da Microsoft mostra o valor do HASH do programa. Se o HASH calculado localmente for igual ao do site da Microsoft, que tipo de segurança o HASH fornece ao usuário? Indique todas que aplicarem

A. O HASH garante que o arquivo não foi contaminado por vírus no site espelho.

B. O HASH garante que o arquivo veio do site Microsoft.

C. O HASH detecta erros causados pela perda de dados que possam ocorrer durante o download.

D. O HASH protege contra ataques do tipo Man-In-The-Middle, que interceptem e alterem o arquivo em trânsito.

Q2: Suponha que Alice enviou uma mensagem para Bob, e que no final da mensagem tem um código HASH. Que tipo de segurança esse HASH fornece? Indique todas que aplicarem.

A. O HASH garante que o arquivo veio realmente da Alice.

B. O HASH detecta erros causados pela perda de dados que possam ocorrer durante a transmissão.

C. O HASH protege contra ataques do tipo Man-In-The-Middle, que interceptem e alterem a mensagem em trânsito.

D. O HASH garante que apenas Bob irá receber a mensagem.

Q3: Suponha que Alice enviou uma mensagem para Bob, e que no final da mensagem tem uma assinatura HMAC. Que tipo de segurança esse HMAC fornece? Indique todas que aplicarem.

A. O HMAC garante que o arquivo veio realmente da Alice.

B. O HMAC detecta erros causados pela perda de dados que possam ocorrer durante a transmissão.

C. O HMAC protege contra ataques do tipo Man-In-The-Middle, que interceptem e alterem a mensagem em trânsito.

D. O HMAC garante que apenas Bob irá receber a mensagem.

Q4. Em relação aos modelos de distribuição de chave pública, relacione as colunas.

A. Permite transmitir a chave pública de forma confiável.

B. Usado para proteger o HTTP na Web.

C. É centralizado, isto é, depende de entidades oficiais que intermediam a transferência da chave pública.

D. É distribuído, isto é, a troca de chaves públicas pode ser feita diretamente pelos usuários.

I. Web Of Trust

II. PKI com TLS

III. PKI

IV. Ambos

Q5: Suponha que Bob quer enviar uma mensagem protegida por PGP para Alice. Ordene a sequencia de eventos que devem acontecer nessa comunicação.

A. Bob criptografa a chave de sessão com a chave pública da Alice.

B. Bob obtém a chave pública da Alice de forma segura.

C. Bob envia a mensagem criptografada com a chave de sessão e a chave de sessão criptografada com a chave pública da Alice.

D. Alice descriptografa a mensagem com a chave de sessão criada por Bob.

E. Alice descritografa a chave de sessão enviada por Bom com sua chave privada.

Q6: Suponha que Bob não tem a chave pública da Alice, mas ele confia na Carol. Carol por sua confia na Alice. É possível Bob enviar uma mensagem criptografada para Alice usando Web of Trust? Lembre-se que confiar significa ter a chave pública armazenada localmente.

A. Não, pois Alice precisa também confiar em Carol.

B. Sim, pois Carol pode enviar a chave pública de Alice para Bob de forma segura.

C. Não, pois isso permite apenas Carol enviar a chave pública de Bob para Alice.

D. Não, pois Carol precisa ter também a chave pública da Alice.

E. Não tem como um terceiro intermediar a transferência da chave pública de outra entidade.

Q7: Indique o que não está contido em um certificado X509.

A. A chave pública do issuer.

B. A assinatura do issuer.

C. O DN do subject.

D. O DN do issuer.

E. A chave pública do subject.

Q8. Como o navegador Web obtém a chave pública da Autoridade Certificadora (CA) Root.

A. A chave pública da CA vem junto com o certificado do Requerente.

B. O navegador Web envia o certificado do Requerente para CA validar, assim não precisa da chave pública da CA .

C. Assim que obtém o certificado, ele consulta a CA para obter sua chave publica.

D. A chave pública da CA precisa estar previamente armazenada no computador

Q9. Em um cenário típico de uso na Web, relacione as colunas identificando as características de cada tipo de certificado.

A. Trusted, isto é, precisa estar armazenado localmente no computador.

B. Pode ser enviado pela rede.

C. Usado para assinar o certificado de entidade final.

D. Usado para assinar o certificado Intermediário.

I. Certificado Root

II. Certificado Intermediário

III. Certificado de Entidade Final

IV. I e II

V. II e II

Q10. Porque os certificados intermediários são usados? Indique todas que aplicarem.

A. Para evitar que o cliente precise ter muitos certificados de CA armazenados localmente.

B. Para diminuir a exposição do certificado Root.

C. Para diminuir o impacto do vazamento da chave privada de uma CA, uma vez que o certificado intermediário pode ser revogado.

D. Para tornar o processo de verificação do certificado feito pelo cliente mais simples.

E. Para diminuir o tamanho das mensagens necessárias para enviar o certificado.

Q11. Indique a alternativa que melhor define o que é TLS/SSL

A. É um algoritmo de criptografia.

B. É um conjunto de algoritmos, que inclui criptografia, assinatura digital e hash.

C. É um protocolo de negociação e de formatação de mensagens.

D. É uma biblioteca implementada em Python que suporta o desenvolvimento de aplicações com segurança.

Q12. Em relação ao HTTPs indique a afirmativa correta.

A. Ambos, servidor e cliente, precisam provar suas identidades enviando certificados.
B. Apenas o envio do certificado do servidor para o cliente é mandatório.
C. O HTTPs pode funcionar sem certificados.
D. Apenas o envio do certificado do cliente para o servidor é mandatório

Q13: Quais arquivos você precisa fornecer para uma aplicação TLS/SSL que funciona como servidor. Considere que o certificado do servidor foi gerado por uma CA. Indique todas que aplicarem.

A. O certificado de entidade final do servidor.
B. A chave privada do servidor.
C. A lista de autoridades certificadoras TRUSTED
D. A chave privada do cliente.
E. O certificado de entidade final do cliente.

Q14: Indique quais dos modos abaixo correspondem a uma autenticação multifator.

A. PIN e Senha.
B. PIN e impressão digital.
C. Smart card e token no celular.
D. Impressão digital e reconhecimento de iris.

Q16: Que tipo de autenticação melhor representa os tokens gerados pelas aplicações em APP de celulares usados em bancos? Considere que o token expira após um tempo.

A. SCRAM.
B. OTP (One Time Password).
C. TOTP (Time-based OTP).
D. HMAC.
E. OTPT (OTP Temporário)

Q15: Sobre o mecanismo SCRAM (Salted Challenge Response Authentication Mechanism), o que significa Challenge-Response?

A. É uma forma de proteção contra ataques do tipo Replay.

B. É uma forma de autenticação mútua.

C. É uma estratégia para que o servidor autentique o cliente sem conhecer sua senha em plaintext.

D. É uma estratégia no qual o usuário responde a um QUIZ para se autenticar.

Q17: Sobre o mecanismo SCRAM (Salted Challenge Response Authentication Mechanism), o que significa Salted?

A. É uma forma de proteção contra ataques do tipo Replay.

B. É uma forma de autenticação mútua.

C. É uma estratégia para que o servidor autentique o cliente sem conhecer sua senha em plaintext.

D. É uma estratégia no qual o usuário responde a um QUIZ para se autenticar.