INE5680 – Prova 1 – 11/05/2012 - Solução das Provas 1a e 1b (Bosco)

Questões (Verdade/Falso) valem 0,25 (total 1,25) e a questão sobre criptografia de chave pública vale 3,75.

Prova 1a: máximo (1,25)

(Verdade/Falso) Vulnerabilidade é uma falha de segurança em um sistema de software que pode ser explorada para efeito de obter a segurança de um sistema.

Vulnerabilidade é uma falha de segurança em um sistema de software que pode ser explorada para efeito de burlar a segurança de um sistema.

(Verdade/Falso) Ameaça: Potencial para violação da segurança quando há capacidade que pode quebrar a segurança e causar danos. É um possível perigo que pode explorar uma vulnerabilidade.

(Verdade/Falso) Um email recebido portando um link suspeito, mas que é deletado, constitui uma ameaça. Por isso, você deletou, para que o ataque, via intrusão por software, não se concretizasse.

(Verdade/Falso) Risco: É a probabilidade da ocorrência de uma vulnerabilidade.
É a probabilidade da ocorrência de uma vulnerabilidade uma ameaça.

(Verdade/Falso) Ataque: É uma tentativa deliberada, especialmente no sentido de uma técnica de burlar os serviços de segurança e violar a política de segurança de um sistema. Se o ataque for bem sucedido, ele é uma intrusão/invasão. O ataque pode ser detectado, por um sistema como se fosse um alarme, conhecido por sistema de detecção de intrusão.

Prova 1b máximo (1,25)

1.(Verdade/Falso) Vulnerabilidade é uma falha de segurança em um sistema de software que pode ser explorada para efeito de obter/burlar a segurança de um sistema.

2. (Verdade/Falso) Ameaça: Potencial para violação da segurança quando há capacidade que pode quebrar a segurança e causar danos. Não é um possível perigo que pode explorar uma vulnerabilidade.

Será que Não é mesmo ??? É um possível perigo que pode explorar uma vulnerabilidade.

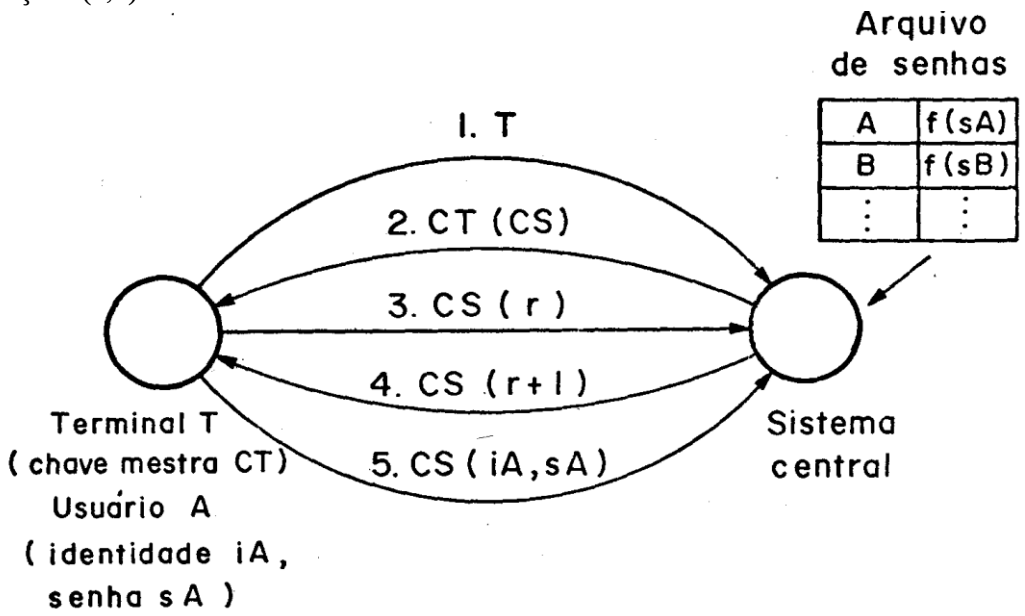
3. (Verdade/Falso) Um email recebido portando um link suspeito, mas que é deletado, constitui uma ameaça. Por isso, você deletou, para que o ataque, via intrusão por software, não se concretizasse.

4. (Verdade/Falso) Risco: Não é a probabilidade da ocorrência de uma vulnerabilidade.
É a probabilidade da ocorrência de uma ameaça.

5. (Verdade/Falso) Ataque: É uma tentativa deliberada, especialmente no sentido de uma técnica de burlar os serviços de segurança e violar a política de segurança de um sistema.

Se o ataque for bem sucedido, ele é uma intrusão/invasão. O ataque pode ser detectado, por um sistema como se fosse um alarme, conhecido por sistema de detecção de intrusão.

6. Altere o protocolo da figura abaixo, desenhado com criptografia simétrica, para mostrar como se pode implementar um protocolo de autenticação com criptografia de chave pública. Suponha que o terminal é uma entidade T e o sistema central uma entidade S. Considere para o terminal o par *(PU_T, PR_T) e o par (PU_S, PR_S)* de chave pública e chave privada para o sistema de autenticação. (1,0)



0. Considere que o sistema central conheça as chaves públicas dos vários terminais *T* (PU_T). E que esses conheçam a chaves pública do sistema central.

1. O protocolo se inicia quando o terminal envia sua identificação *T* para o sistema central. Alguém está querendo usar o terminal.

2. Pelo protocolo da figura, o sistema central deve enviar uma chave de sessão *CS* para o terminal *T* poder criptografar os dados do usuário (usando criptografia simétrica com a chave de sessão *CS*), através da chave mestra *CT*, a qual não é necessário mais e será substituída pela chave pública de T (PU_T).

3. Mas, para se usar criptografia de chave pública, o sistema central, agora, se utilizará da chave pública do terminal T (PU_T), enviando uma chave de sessão *CS* criptografada por (PU_T), para *T*. Com sua chave privada (PR_T), o terminal *T* decifra a chave de sessão *CS*.

4. O passo 3 da figura continua. Com *CS*, o terminal *T* pode cifrar os números *r*, supostamente aleatório gerado por *T*, e enviá-los ao sistema central.

5. De posso do número *r*, o sistema central modifica esse número *r*, adicionando 1, cifrando-o com *CS* e enviando para *T*. Lembrem que os números *r* e *r+1* são

usados apenas uma vez, para evitar ataques de repetição no procedimento de autenticação de um usuário do terminal *T*. Daí o termo *nonce*, em inglês, para denominar esses números.

6. O terminal envia sua identificação *iA* e a senha *sA* para o sistema central poder autenticar usando o arquivo de senhas, contendo os valores *hash* das senhas dos usuários do sistema.

Observações:

a) A **criptografia de chave pública** substitui a *CT* (chave mestra de *T*).

b) A **criptografia simétrica**, com uma chave de sessão *CS* é usada no procedimento de autenticação.

c) *Uma chave de sessão CS de criptografia simétrica, quando cifrada por uma chave pública (PU_T) e decifrada por uma chave privada (PR_T), tem-se os uso da criptografia simétrica para cifrar a comunicação, e usa a chave pública (PU_T) para cifrar e repassar a chave de sessão (CS). Esta chave de sessão (CS) é temporária, só serve para aquela sessão de um usuário, e deve ser descartada ao término de cada sessão. Sessão, aqui, é com dois `s´, pois tem a conotação de tempo.*