Exame 2010

1. Explique a diferença entre uma política de segurança e um mecanismo de segurança. Dê um exemplo envolvendo autenticação de pessoas.
Uma politica de segurança define as restrições no funcionamento das várias entidades do sistema, em suma define o significado de seguro para o sistema em causa. Um mecanismo de segurança é um procedimento que é necessário à segurança do sistema, sem o qual este seria comprometido. Estes meanismos são ditados pela politica de segurança em vigor. Por exemplo, uma politica de autenticação pode definir que os utilizadores utilizam um mecanismo de desafio-resposta para se autenticarem no sistema, e define tambem os parametros de utilização deste mecanismo (o tipo de chave, o tipo de transformação aplicada no desafio, etc).

1 **- Explique em que consiste o conceito de domínio de segurança.**
Conjunto das varias maquinas, redes, utilizadores autorizados e actividades autorizdas e proibidas.

1 - Considere o conceito de ataque por esmagamento da pilha (stack smashing attack). Discuta a sua viabilidade caso existissem duas pilhas, e não apenas uma: uma para guardar parâmetros e variáveis locais, outra para guarder endereços de retorno e endereços de blocos de pilha (stack frames).
É viavel pois elimina a possibilidade de mudar o ponteiro de retorno, mas continua a permitir a modificaçao de valores lidos pela funçao, incluido ponteiros para outras funçoes.

1 - Considere os ataques por esmagamento da pilha (stack smashing attack) usando C. Explique:
a. Qual é a vulnerabilidade da linguagem de programação C que permite tais ataques?
b. Descreva um processo de detecção de tais ataques.
a) O C permite escrever em endereços para alem dos reservados necessitando apenas do endereço base inicial.
b) Canarios – O processo de deteção com canarios escreve um valor bem conhecido para algumas posiçoes de memoria desocupadas. Quando um ataque destes acontece o valor dessas posiçoes é atlterado e o ataque pode ser assim detectado.

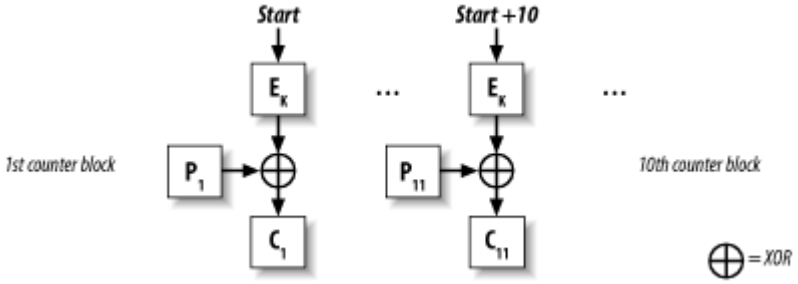
1 - Considere os ataques por esmagamento da pilha (stack smashing attack) usando C. Explique com pormenor como os mesmos podem ser mitigados alterando o endereço base de início da pilha de cada vez que um programa inicia a sua execução.
Como a posiçao dos varios segmentos de memoria é aleatoria, um atacante tem mais difiiculdade em saber precisamente que posiçoes de memoria alterar.

1 - Por que razão podem ocorrer buffer overflows em C e não em Java?
No C o acesso a arrays é feito somando directamente o offset da posiçao desejada ao ponteiro do array mas no java estas operaçoes são verificadas pela maquina virtual assim no C é possivel referencias uma posição fora dos limites do array mas em java nao, é levantada um exceçao.

2 - Considere o conceito de cifra tripla. Explique:
a. O que motiva a sua utilização?
b. Porque razão se usa a cifra tripla com a aproximação EDE?
a) a sua utilizaçao é motivada pelo numero reduzido do comprimento de chaves e porque uma cifra dupla nao tem o acrescimo de segurança esperado(dupla 2^n+1, normal 2^n).
b) No caso do DES é possivel aplicar uma cifra unica se as 3 chaves forem iguais. Por razoes de retrocompactibilidade isso pode ser util.

4. Uma cifra contínua propaga erros na decifra de um criptograma com erros? Justifique a sua resposta.
Não, um erro de transmissão numa cifra continua (stream cipher) apenas corresponde a um erro nos bits do texto a claro produzido.

2 - Explique qual o modelo geral de operação de uma cifra contínua concretizada por uma cifra por blocos em modo contador (Counter, CTR), ilustrando-o com um diagrama.
A cada bloco da mensagem a cifrar é aplicado um XOR com a cifra do indice do bloco somado de um valor inicial. O processo de decifra é igual mas aplica o algoritmo aos blocos da mensagem cifrada.



2 - Considere o circuito lógico conhecido como LFSR (Linear Feedback Shift Register), usado para concretizar cifras contínuas. Explique:

a. Qual é o comprimento máximo do período da sequência de bits que produz?
b. O que significa o facto de possuir um polinómio de realimentação primitivo?

a)2^k-1, com k a ser o numero de bits do SR.
b) Um polinómio primitivo permite gerar todas as combinações possiveis dos n bits do registo (excepto a nula).

3 - O modo contador (Counter, CTR) permite a concretização de uma cifra contínua com acesso aleatório uniforme na cifra/decifra de dados volumosos. Explique:
a. Por que razão o modo CTR possui essa característica?
b. O que torna este modo particularmente interessante para a cifra de conteúdos de ficheiros em sistemas de ficheiros com segurança dos conteúdos.
a) É possivel decifar ou cifrar qualquer bloco desde que seja conhecido o seu indice.
b) Pode-se parelelizar a cifra ou decifra ou fazer transmissao(streaming) atraves de uma rede.
Permite acesso aleatorio ao ficheiro sem necessitar da decifra completa. O overhead está apenas no processo de cifra ou decifra de um bloco.

2. Considere as cifras poli-alfabéticas. Indique:
a. O que é o período de uma cifra poli-alfabética.
b. Uma técnica para descobrir o período (descreva a técnica com algum pormenor).
a) O periodo duma cifra poli alfabetica corresponde ao tamanho da chave usada.
b) Teste de Kasiski:
Analisamos as ocorrencias de blocos identicos do criptograma medindo a distancia entre as ocorrencias do mesmo bloco. Factorizando estas distancias e o maior divisor comum da maioria delas sera o periodo.

3. **Explique o modelo geral de operação de uma cifra contínua.**
existe um gerador pseudo-aleatorio cujo o comportamento é determinado pela chave da cifra. Este gerador produz uma chave continua(keystream) e é misturada com o teste original atraves da operação XOR.

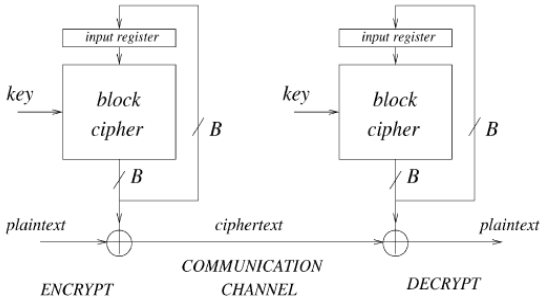
4. Uma cifra contínua é uma aproximação prática à cifra de Vernam, ou one-time pad, a única totalmente segura. Explique:
a. Como funciona a cifra de Vernam.
b. Por que razão em circunstâncias normais não se usa a cifra de Vernam.

a) Uma cifra de vernam é criada a partir de uma chave aleatoria de tamanho maior que o texto a cifrar, misturando os dois através da operação XOR. A chave não pode ser reutilizada para cifrar outro texto.

b) nao é usada porque para decifrar o texto seria necessario transmitir tambem a chave completa, ja que esta nao pode ser gerada.

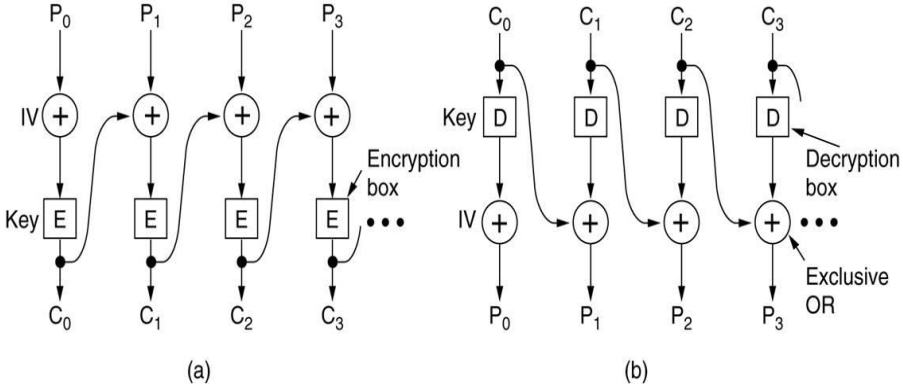
2 - Explique qual o modelo geral de funcionamento de uma cifra contínua concretizada explorando uma cifra por bloco. Ilustre a sua resposta com um diagrama.

É baseada numa funçao de realimentaçao que produz n valores para um registo ri, os n valores deste registo são cifrados e o valor cifrado adicionado ao registo Ro, deste registo são retirados n valores e somados (XOR) ao texto em claro. A decifra é feita do mesmo modo mas utilizando o texto cifrado na operação XOR.



OFB

3 - Explique, ilustrando a sua resposta com um diagrama e com provas matemáticas, por que razão uma cifra por blocos em modo CBC (Cipher Block Chaining) é comparável, em termos de resultado final, a uma cifra polialfabética.



Vi,j i=!j, Pi = Pj e Ci = Cj => Ci-1 = Cj-1

4 - As funções de síntese devem dificultar a descoberta de uma segunda pré-imagem. Explique:
a. Em que consiste essa descoberta?
b. Por que razão tal é crítico no âmbito da validação de assinaturas digitais calculadas sobre valores calculados com funções de síntese?

a) Consiste em descobrir uma mensagem cuja sintese é igual à sintese de uma mensagem já conhecida.

b)The usual attack scenario goes like this:

1.Mallory creates two different documents A and B, that have an identical hash value (collision).

2.Mallory then sends document A to Alice, who agrees to what the document says, signs it and

sends it back to Mallory.
3.Mallory copies the signature sent by Alice from document A to document B.
4.Then she sends document B to Bob, claiming that Alice signed the different document. Because the digital signature matches the document hash, Bob's software is unable to detect the modification.

4 - Explique como opera a cifra assimétrica RSA, ilustrando a sua explicação com as expressões matemáticas da cifra (não precisa de explicar processo de geração das chaves, apenas a sua constituição).
C = p^e mod n
P= C^d mod n

e<n

6 - Quais são os pressupostos matemáticos base em que se baseia a segurança do RSA?

dificuldade na factorização de grandes números e
dificuldade no cálculo de logaritmos discretos de grandes números

3 - A cifra RSA baseia a sua segurança em duas propriedades: dificuldade na factorização de grandes números e dificuldade no cálculo de logaritmos discretos de grandes números. Explique porquê?
C= P^e mod n
P = C^d mod n

Como se pode ver os log é para inverter estas potencias.
Factorizando o valor de "n"em "p" e "q" é possivel determinar "d" apartir de "e".

4 - Explique a aplicabilidade do Paradoxo do Aniversário à resistência à colisão das funções de síntese.
Aplicando o paradoxo do aniversario pode-se establecer uma relaçao entre o numero de bits de uma sintese e a probabilidade de encontrar uma colisao.

5 - Qual é relação entre o Paradoxo do Aniversário e a aferição do limite máximo da robustez de uma função de síntese à descoberta de colisões? Ilustre a sua resposta com um exemplo.
De forma geral, o paradoxo diz que apesar de, num conjunto de objectos, a probabilidade de encontrar uma relação entre um dado objecto fixo e os restantes ser baixa, a probabilidade de encontrar um par com essa relação é bem maior. Isto significa que, apesar de a probabilidade de descobrir um texto cuja sintese seja a mesma que outro texto conhecidos, a probabilidade de encontrar um par de textos que partilhem a sintese é bem maior.

Um exemplo simples é: dado um grupo de 30 pessoas, a probabilidade de uma delas ter nascido num dia escolhido é pequena. No entanto, a probabilidade de existir um par que partilhe a mesma data é bastante maior (> 50%) pois há (30*29)/2 = 435 pares.

5 - Um MAC (Message Authentication Code) é um meio de autenticação de dados. Explique:
a. Qual é o modelo geral de geração e validação de um MAC?
b. Como pode ser concretizado apenas com uma função de cifra?
a)Quando duas entidades querem tranmitir uma mensagem entre si geram um valor MAC sobre a mensagem em questao e uma chave simetrica partilhada, na forma de uma sintese da mensagem. Quando a mensagem é recebida o recetor verifica se a mensagem corresponde á sintese recebida para verificar que o emissor foi a outra entidadade.
b)O CBC-MAC utiliza um conjunto de bits do ultimi bloco do criptograma criado com um cifra por blocos em modo CBC.

6 - Um MAC (Message Authentication Code) é um meio de autenticação de dados. Explique como pode ser usado para garantir uma sequência correta de mensagens enviadas e recebidas (e.g. pacotes UDP) num fluxo de mensagens bidirecional entre duas entidades.

Uma opção é a seguinte: para cada mensagem é calculado o MAC desta forma

MAC = h(K | i | m), onde o K é a chave simétrica secreta, o i o indice da mensagem, e m a mensagem (cifrada ou em claro). Assim, mesmo com a chave correcta, o receptor da mensagem consegue saber que a mensagem recebida não é a esperada, e pode discartar a mesma. Deve ainda existir um mecanismo que assegure o eventual re-envio da mensagem correcta, por exemplo, por sinalização do receptor ao emissor.

5 - Descreva o modelo de execução da construção HMAC, destinada a calcular o MAC (Message Authentication Code) de uma mensagem.

HMAC=H(K + opad | H(K+ipad|msg)), | é a concatenação, + é XOR, opad e ipad são excipientes de tamanho do bloco com os valores 0x36 e 0x5C para cada octeto, respectivamente. H é a função de sintese utilizada, MD5 ou SHA-1.

5 - Explique como funciona o cálculo de um código de autenticação de mensagem (Message Authentication Code, MAC) com recurso a uma cifra por blocos e ao modo de cifra CBC (Cipher Block Chaining).

CBC-MAC utiliza um conjunto de bits do ultimo bloco do criptograma criado com um cifra por blocos em modo CBC.

7. Indique as vantagens e desvantagens de usar ECB (Electronic Code Book) ou CBC (Cipher Block Chaining) na cifra de conteúdos de ficheiros.

ECB: rápido (acesso aleatório), pouco seguro criptograficamente.
CBC: mais seguro, em comparação com ECB, mas só tem acesso aleatório na decifra.

5 - Descreva o modelo genérico de execução das funções de síntese (i.e. como são realizadas).

A funçao de sintese utiliza uma função de compressao que recebe dois valores, o primeiro é um bloco da mensagem e o segundo é o resultado desta função no bloco anterior. Para o primeiro bloco utiliza-se um vector de inicialização. A sintese da mensagem é a sintese do ultimo bloco que depende dos blocos anteriores.

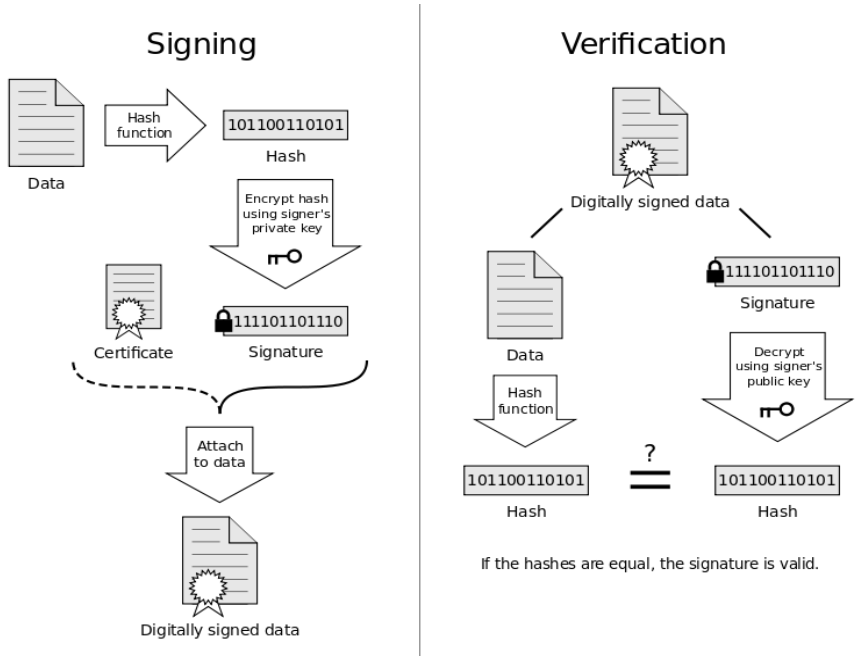
6 - A qualidade de uma função de síntese mede-se segundo três características: (i) resistência à descoberta de um texto, (ii) resistência à descoberta de um segundo texto e (iii) resistência à colisão. Explique em que consiste cada uma destas características.

i) é dificil encontrar o texto original apartir da sintese. Dada uma mensagem é dificil encontrar outra mensagem que produza a mesma sintese
ii) Dada uma mensagem é dificil encontrar outra mensagem que produza a mesma sintese
iii) É dificil encontrar duas mensagens quisquer cuja sintese seja a mesma

6 - Considere o conceito de assinatura digital. Explique:
a. Como é que a mesma é construída? Ilustre com um diagrama.
b. Como é que a mesma é validada? Ilustre com um diagrama.

a) Faz se um hash dos dados, cifra-se a hash com a chave privada do assinante, junta-se ao certificado e isto constitui a assinatura digital.

b) Faz-se uma sintese da mensagem, extrai-se a assinatura da assinatura digital, decifra-se e compara-se com o primeiro hash gerado.



7. As assinaturas digitais são normalmente concretizadas sobre sínteses de documentos e não sobre os mesmos. Explique:
a. Por que razão se usa essa aproximação.
b. Quais das três características de qualidade indicadas na alínea anterior são críticas para se poder usar esta aproximação.

a) Por causa do tamanho do documento.

b) descoberta de um segundo texto porque é possivel modificar uma mensagem mantendo a validade da assinatura mas alterando o conteudo.

6 - Considere o conceito de assinatura digital. Explique o motivo que justifica que na sua construção seja incluída informação adicional (para além do documento a assinar, ou da sua síntese).

É necessario informaçao adicional, tal como data, indentificaçao do assinante, para permitir oter a respectiva chave publica, os algoritmos de sintese e cifra usada. Estas informaçoes são necessarias para fazer a validação da mesma.

7 - Explique, de uma forma o mais completa possível, por que razão os certificados de chaves públicas são vitais para suportar a validação de assinaturas digitais.

O certificado é necessario pois este comprova que uma entidade certificadora confirma a relação entre a chave publica em questão e a entidade referente, assegurando a autenticidade da entidade em questão.

6. Quando se considera a cifra de dados de ficheiros ao nível dos sistemas de ficheiros, há diversos metadados desses ficheiros que não podem ser cifrados, porque precisam de ser analisados por terceiros. Dê 2 exemplos desses metadados e explique porque não podem ser cifrados.

Por exemplo data de criação e o criador do ficheiro. Estes dados são necessários ao funcionamento do sistema de ficheiros, e devem ser acessiveis independentemente do acesso ao ficheiro.

7 - Considere os sistemas de ficheiros com capacidade de cifra de conteúdos de ficheiros. Explique:
a. Por que razão podem não ser suficientes os mecanismos usuais de controlo de acesso aos ficheiros, como as listas de controlo de acesso (Access Control Lists, ACL), para controlar o acesso aos seus conteúdos?
b. Quais as implicações da cifra dos conteúdos na partilha de ficheiros entre vários utentes?

a) Porque pode haver acesso directo ao suporto fisico, administradores pouco eticos.

b) Há mais segurança quando os ficheiros são transferidos entre redes menos seguras, no entanto implica a troca de chaves que, feita de forma incorrecta, pode comprometer a segurança da mesma.

7 - Considere o padrão de facto PKCS #11. Explique:
a. Em que consiste?
b. Porque razão ele não consegue abarcar todas as funcionalidades do Cartão de Cidadão?

a) É uma interface programatica para aceder a tokens criptograficos, por exemplo smartcards.

b)

9 - Considere a gestão de chaves públicas. Explique:
a. O que é uma Entidade Certificadora (Certification Authority, CA)?
b. Como podem os utentes avaliar, em cada momento, a sua confiança numa dada Entidade Certificadora?

a) Os certificados digitais sao documentos com uma estrutura predefinida que possuem, entre outrs elementos uma chave publica de uma dada entidade e uma assinatura digital do certificado feita pela entidade emissora do mesmo, a entidade certificadora.

b) Vericar toda a cadeia de certificação.

8 - Explique, de uma forma o mais completa possível, por que razão se usam certificados de chaves públicas.

Os certificados de chave publicas asseguram a correspondencia entre uma entidade e a sua chave publica e a sua validade é assegurada por uma entidade certificadora.
Isto assegura que uma mensagem assinada digitalmente foi de facto enviada por a entidade certa.

8 - Explique, exemplificando com o Cartão de Cidadão, porque razão os smartcards são úteis para a implantação de infra-estruturas de chave pública (Public Key Infrastructures, PKI).

Porque a chave privada esta dentro do cartao e nao pode ser extraida sem a destruição do mesmo, isto significa que o utilizador pode criar assinaturas digitais facilmente e sem comprometer a segurança.

10. Um smartcard não é um mero circuito de memória, mas possui um processador e inclusive capacidades de execução de funções criptográficas complexas e de geração de valores aleatórios. Explique a utilidade destas duas últimas capacidades.

As funções criptograficas são uteis para cifrar dados e assinar documentos, principalmente interessante porque as chaves necessárias podem estar apenas no cartão, e não ser conhecidas pelo utilizador. O gerador de números aleatorio pode ser utilizado em funções de cifra, sintese ou para protocolos desafio-resposta.

10 - Considere o problema do tempo de vida de um certificado de chave pública. Explique:
a. Como é que o mesmo é controlado?
b. Que mecanismos existem para os utentes verificarem se um certificado ainda não expirou?

a) O proprio certificado contem uma data de validade. Para alem disto pode ser emitir um

certificado de revogação que afirma que uma dada chave publica deixa de ser valida apartir de uma certa data.

b) Ver no proprio certificado se este já expirou e caso contrario aceder à lista de certificados revogados da PKI em que o certificado foi emitido.

8 - Considere o problema da validação de um certificado de chave pública. Explique, com pormenor, quais as vantagens e desvantagens de usar listas de certificados revogados (Certificate Revocation List, CRL) ou serviços OCSP (Online Certificate Status Protocol) pela entidade validadora.

O OCSP é um protocolo que apenas indica o estado de revogaçao de um certificado. Isto tem algumas vantagens nomeadamente: A leitura da lista de revogação não é feita pelo cliente, mas sim pelo servidor OCSP, isto implica menos complexidade para o cliente.
No entanto o OCSP não obriga à encriptação, portanto a informação pode ser interceptada por outros.
A CRL mostra todos os certificados que estao revogados, isto pode ser vantajoso.

8 - Considere o conceito de CRL (Certificate Revocation List). Explique:

a. Quem gere uma CRL?

b. Quem, e quando, se deve usar a sua informação?

a) CA, esta publica a lista de revogação para os seus certificados.
b) Quando uma entidade quer validar um certificado.

9 - Explique, exemplificando, que riscos corre um utilizador caso o seu repositório de certificados seja atacado por um vírus que lhe introduz informação falsa.

Podem ser adicionados certificados nao autorizados, o que dá legitimidade a entidades cuja mesmo não foi comprovada, reciprocamente, podem ser retirados certificados cujas entidades são tidas com fidedignas, para prejuizo das mesmas. Alterando a CRL podem-se obter resultados semelhantes, revogar certificados fidedignos e remover a revogação de certificados que foram préviamente inválididados.

9 - Um certificado de chave pública X.509 certifica, para além de uma chave pública, o fim a que a mesma se destina.

a. Qual é, de entre vários existentes, o interesse primordial da certificação de uma chave pública?

b. Indique três tipos de fins a que se pode destinar uma chave pública certificada (lembre-se do Cartão de Cidadão).

a) garantir a autoria de um documento certificado
b) Assinatura. Autenticação. Certificar

10 - As cadeias de certificação terminam quando se atingem certificados declarados como confiáveis. Explique:
a. Porque terminam nestes certificados?
b. Quem define quem são estes certificados?

a) Porque o proposito da cadeia de certificação é chegar a um certificado confiavel, que valida a entidade da chave publica correspondente. Se na cadeia de certificados nao existe nenhum revogado significa que todos são considerados validos.

b) Estes certificados sao os certificados autocertificados das CA de Topo, suja chave publica se admite estar correcta.

11. Explique de que forma a arquitectura PAM permite a integração de diferentes paradigmas de autenticação de pessoas (com senha, com o Cartão de Cidadão, etc.) com diversas aplicações Unix.

A arquitectura PAM permite que o sistema utilize modulos de autenticação (como os exemplos citados) desenvolvidos independentemente do proprio sistema operativo. Isto possibilita que os protocolos de autenticação dos paradigmas adicionados tem uma interface que o sistema operativo pode consultar, a fim de determinar se o utilizador deve ser autenticado ou não.

11 - Explique como funciona o sistema de cifra de conteúdos de ficheiros do EFS (Extended File System) do Windows.

Cada ficheiro é cifrado com uma chave simetrica(FEK) unica, essa chave é depois cifrada com a chave publica do utlilizador que cifrou o ficheiro e é guardada junto com o mesmo. Para decifrar o sistema usa a chave privada do utilizador para obter a chave simetrica e assim decifrar o ficheiro. Todo este processo é escondido do utilizador, que pode listar e aceder aos ficheiros pela interface normal (wxplorador do windows)

10. O EFS (Encrypted File System) do Windows é uma extensão do NTFS que permite cifra de ficheiros de forma integrada com a sua lista de controlo de acesso. Explique:
a. Como é protegido cada ficheiro através de cifra.
b. De que modo se integra essa cifra (ou decifra) com a lista de controlo de acesso de cada ficheiro.

a) Cada ficheiro é cifrado com uma chave simetrica(FEK) unica, essa chave é depois cifrada com a chave publica do utilizador que cifrou o ficheiro e é guardada junto com o mesmo. Para decifrar o sistema usa a chave privada do utilizador para obter a chave simetrica e assim decifrar o ficheiro.

b)

11. Considere o modelo de operação normal da autenticação Unix. Explique:
a. Como funciona.
b. Por que razão é vulnerável a ataques com dicionários.

a) A chave é transformada por uma função de unidireccional, no caso do Unix, uma hash DES + salt, e este valor é associado ao utilizador num ficheiro do sistema. Quando o utilizador faz a autenticação, a chave inserida é transformada da mesma forma e os valores comparados.
b) Se a chave utilizada é uma palavra comum, e o um atacante a descobrir por ataque de dicionario, este método irá produzir o valor para comparação correcto. É ainda mais grave se o atacante tiver acesso directo ao ficheiro.

12 - Considere a alteração da autenticação local numa máquina Unix para um modelo baseado em chaves assimétricas, por exemplo, usando o Cartão de Cidadão. Indique as vantagens e desvantagens da sua utilização como alternativa à autenticação Unix normal.

Este tipo de autenticação requer o cartao, a chave privada e o pin de acesso no entanto o sistema neste caso Unix só necessita de saber a chave publica do cartao. Desvantagens é a acecibilidade e afins.

12. Um ataque a senhas de acesso com dicionários é um ataque exaustivo? Justifique a sua resposta.
Um ataque por dicionários é também uma abordagem tentativa e erro, mas comparativamente a um ataque brute-force, que percorre todo o dominio da chave possivel, têm um domínio de probabilidade mais reduzido, mas ao contrário do brute-force, este não garante que a chave seja discoberta eventualmente.

11. Considere os protocolos de autenticação com desafio-resposta. Explique:
a. Por que razão o desafio tem de ser um valor nunca antes usado (nonce)?
b. Como podem ser realizados estes protocolos usando o Cartão de Cidadão?

a) Caso um valor de desafio seja repetido um individuo mal intensionado que escutou o canal da transação pode guardar todos os pares(desafio,.resposta) e tentar autenticar-se até lhe ser pedido um desafio cuja resposta já conheça.

b)

11 -Considere os paradigmas de autenticação com apresentação directa de credenciais e com desafio-resposta.
Explique:
a. Qual é a diferença fundamental entre as mesmas?
b. Em que situações pode (deve) ser explorado cada um deles?

a) a apres. Directa de credenciais o utilizador envia os dados para o sistema e este verifica a sua

vericidade. nO desafio resposta sistema envia o desafio ao utilizador, este modifica-o utilizando as suas credencias e envia a resposta.

b) O desafio-resposta deve ser usado sempre que o meio de transmissao possa ser escutado. Este metodo é mais complexo. Quando o meio de transmissao é relativamente seguro a apresentaçao directa de credencias pode ser usado.

12 - Considere os protocolos de autenticação com desafio-resposta. Explique, ilustrando com um diagrama, como pode realizar um protocolo unilateral desse tipo usando as operações de cifra assimétricas do Cartão de Cidadão (do autenticado).

a) Um protocolo deste genero pode ser implementado da seguinte forma:
Depois de o cliente contactar o serviço, este envia-lhe um desafio que o cliente deve cifrar com a sua chave privada e enviar para o servidor. Este vai decifrar o desafio cifrado com a chave publica (que é conhecida) e comparar com o desafio enviado para confirmar a identidade.

13. Considere os protocolos de autenticação com segredo partilhado. Explique:
a. Em que consiste um ataque com dicionário?
b. Por que razão o protocolos do GSM e do RSA SecurID não são vulneráveis a este tipo de ataques?

a) um ataque com dicionario é um ataque que tenta a autenticação percorrendo uma lista de valores provaveis para o segredo.

b) O GSM é do tipo desafio resposta, o securID usa one time password. Como os valores de autenticaçao enviados sao diferentes a cada autenticaçao e para alem disso não sao palavras que possam ser representadas num dicionario de ataque.

12 - Considere o conceito de autenticação com senha única(one time password). Explique:
a. Em que consiste?
b. Quais as suas vantagens e desvantagens?

a) Consiste na utilizaçao de um metodo que gera uma password que só é valida por uma vez. Podem ser geradas baseadas em tempo, ser calculadas a partir da password anterior ou calculadas apartir de um desafio do serviço.

b) Vertigens: Um utilizador malicioso que consiga saber a password introduzida não tera qualquer acesso ao sistema.
Desvitalizaçoes: São dificeis de implementar, requerem software/hardware adicional para computar a pass.

13 -Discuta as diversas vantagens e desvantagens operacionais da autenticação biométrica face aos demais paradigmas de autenticação.

Vantagens: Nao requer memorizaçao ou tokens de segurança, não permite a escolha de pass fracas, até porque nao permite nada.
Desvantages: Pode ser forjado, nao pode ser transferido entre pessoas e nao pode ser feito remotamente.

17. **Descreva três problemas da autenticação biométrica que não se verificam com outros paradigmas de autenticação.**
    Partilha de chaves
    Possibilidade de ser forjado
    A implementação pode ser cara, e dificil.
    Se o sistema for comprometido, a informação biometrica pode ser utilizada para aceder a outros

sistemas (a impressão digital de um sujeito não muda em sistemas diferentes, mas este pode usar palavras passe diferentes)

13 - Considere o modelo de autenticação GSM. Explique:
a. Como funciona?
b. Que riscos podem advir de uma personificação de uma BTS (Base Transceiver Station) por um atacante?

a) É utilizada uma chave pre conhecida que está guardada no SIM(ki) e no HLC, depois o MSC pede um valor aleatorio, o valor de resposta e o valor de encriptaçao(kc) usado como chave para a sessao ao HLC. O MSC envia o valor aleatorio e o cliente devolve o valor de resposta que é o valor aleatorio cifrado com o algoritmo A3, usando como chave o valor ki. O valor kc é calculado no cliente aplicando o algoritmo A8 com a chave ki e o valor aleatoreo.

b) Pode decifrar o trafego...

14. Considere a autenticação em redes GSM. Explique:
a. Como funciona.
b. Como se impede que um operador que forneça acesso em roaming a um subscritor de outro operador obtenha as credenciais de autenticação do subscritor.
a) CIMA
b) As credencias nunca são passadas. Ver a)

15 - Explique como funciona o modelo de autenticação de servidores SSH.

O servidor conhece a chave publica dos clientes que se podem ligar a ele. A autenticaçao é baseada na chave privada e o servidor verifica se o utilizador da chave publica possui tambem a chave privada correspondente.

14 - Quais as vantagens práticas da aplicação do princípio da separação de deveres para a segurança do sistema?

O principio da separaçao de deveres diz que tendo mais que uma pessoa a trabalhar numa mesma tarefa aumenta a prevençao de erros ou fraudes, assim sendo para a segurança de um sistema se existirem mais que uma pessoa para realizar a mesma tarefa a probabilidade de deixarem escapar possiveis falhas é muito mais reduzida.

17 - A gestão de um par de chaves assimétricas envolve a sua geração, a protecção da chave privada, a distribuição da chave pública e o tempo de vida do par. Explique os problemas que importa resolver em cada um destes quatro tópicos.

as chaves devem ser aleatorias mas geradas eficientemente, . - a chave privada nunca pode ser revelada. A chave publica tem de ser fidedigna. A chave nao deve ser valida quando o tempo de vida acabou.

14 - Considere o conceito de monitor de controlos de acesso. Indique:
a.Para que serve?
b. Dê dois exemplos práticos da sua exploração.

a) É um mecanismo usado para limitar as acçoes que um usuario legitimo de um sistema pode realizar, com base nas autorizaçoes aplicaveis ao mesmo. Uma autorizaçao establece o que é permitido ou não realizar, com a determinação dos direitos de acesso de um sujeito a um objecto computacional especifico.
Tem como objectivo prevenir que um sistema entre em um estado inseguro.
A execução de uma acçao nao autorizada pode resultar na violação da confidencialidade ou integridade das informaçoes.

b) - - - Empresa com hierarquias entre utilizasdores.... bala bla bla

- - - - Serviços de distribuição de conteudos.

14. Considere os modelos de controlo de acesso discricionário (Discricionary Access Control, DAC) e obrigatório (Mandatory Access Control, MAC).

a. Explique a diferença entre ambos.
b. Dê exemplos de cada um considerando um sistema operativo como monitor de controlo de acesso.

a)

O mac disponibiliza o acesso baseado em niveis enquato o DAC disponibiliza o acesso baseado em entidades.
O DAC tem uma gestao mais complexa que o MAC e tambem é mais flexivel.
No MAC apenas podem ser modificadas as permissoes por administradores enqueanto que no DAC a acesso pode ser definido por utilizadores.

13 - Considere o conceito de controlo de acessos obrigatório (mandatory). Indique:
a. Como funciona?
b. Dê dois exemplos práticos da sua exploração.

a) Um sistema com MAC implementa o controlo de acessos de uma maneira central, onde apenas um administrador pode definir a politica de segurança sobre os objectos do sistema.

15 - Considere o conceito de matriz de controlo de acesso. Indique:
a. Em que consiste a sua decomposição em Listas de Controlo de Acesso (Access Control Lists, ACLs)?
b. Em que consiste a sua decomposição em capacidades (capabilities)?

a) São listas que relacionam objectos a sujeitos pelo nivel de acesso que o sujeito tem ao objecto.

b) Uma capacidade representa não so um objecto como tambem o seu nivel de acesso. Qualquer sujeito a que o sistema atribua a capacidade pode aceder ao obejceto.

15 - Uma política de controlo de acesso por funções (Role-Based Access Control, RBAC) é diferente de uma política de controlo de acesso com listas de controlo de acesso (Access Control Lists) baseadas em grupos. Explique porquê.

RBAC define as permissoes de acesso de uma função e atribui uma dessas funçoes aos utilizadores. Já a politica com lista de controlo de acessos define as permissoes por objecto e por grupo. Um utilizador so tem uma funçao no esquema RBAC mas pode estar em varios grupos na politica com ACL.

16 - Considere o conceito de controlo de acesso baseado em funções (Role-Based Access Control, RBAC). Explique:
a. Em que consiste?
b. Por que razão não pode ser concretizado com controlos de acesso baseados em grupos, usando um grupo por função?

a) Usa-se o RBAC (controle de acesso baseado em função) para atribuir recursos a usuários. As permissões e os recursos são definidos pelas *funções de gerenciamento*. Uma *função de gerenciamento*, também chamada de *função RBAC* ou simplesmente *função*, define o acesso que uma pessoa possui e as tarefas que pode executar. Ao atribuir uma função a um usuário, o usuário pode executar as tarefas definidas pela função.

b) As roles são aplicadas a sessoes enquanto que os grupos são estaticos...

16 - Explique o princípio geral de operação de uma política de controlo de fluxos de informação.

Aplicam regras de segurança verificando a origem e destino do fluxo. As entidades comunicadoras têm atributos de segurança e a autorização é baseada nestes atributos.

É um mecanismo que previne que as informações fluam por canais secretos e violem a política de segurança ao alcançarem usuários não autorizados. Ele regula a distribuição ou fluxo de informação entre objetos acessíveis. Um fluxo entre o objeto A e o objeto B ocorre quando um programa lê valores de A e escreve valores em B. Os controles de fluxo têm a finalidade de verificar se informações contidas em alguns objetos não fluem explicita ou implicitamente para objetos de menor proteção. Dessa maneira, um usuário não pode obter indiretamente em B aquilo que ele ou ela não puder obter diretamente de A.

17 - Considere os modelos de controlo de fluxo. Explique:
a. Em que consistem?
b. Que informação é usada pelo monitor de controlo de acesso para tomar decisões?

a) aplicam regras de segurança verificando a origem e destino do fluxo. As entidades comunicadoras têm atributos de segurança e a autorização é baseada nestes atributos.

É um mecanismo que previne que as informações fluam por canais secretos e violem a política de segurança ao alcançarem usuários não autorizados. Ele regula a distribuição ou fluxo de informação entre objetos acessíveis. Um fluxo entre o objeto A e o objeto B ocorre quando um programa lê valores de A e escreve valores em B. Os controles de fluxo têm a finalidade de verificar se informações contidas em alguns objetos não fluem explicita ou implicitamente para objetos de menor proteção. Dessa maneira, um usuário não pode obter indiretamente em B aquilo que ele ou ela não puder obter diretamente de A.

b) os atributos das entidades e a origem e destino da comunicação.

17 - Explique o modelo geral de operação da política de controlo de integridade de Biba.

O modelo de Biba define que numa hierarquia de integridade, onde a informação mais importante e fiável está no maior nivel, os produtores de informação só podem criar informação classificada ao seu nivel de integridade ou abaixo do mesmo, e os consumidores só podem receber informação no seu nivel ou a um nivel acima do seu.

15 - Explique os princípios do modelo de controlo de fluxos de Bell-LaPadula.

Um menino com um determinado nivel de segurança só pode ler objectos de um nivel de segurança igual ou inferior ao seu. O mesmo menino só pode escrever objectos num nivel igual ou superior ao seu.

18 - Considere o modelo de controlo de integridade de Clark-Wilson. Explique em que consiste:

a. Um CDI (Constrained Data Item) e um UDI (Unconstrained Data Item)
b. Uma IVP (Integrity Verification Procedure) e uma TP (Transformation Procedure).

Constrained Data Items (CDI) Dados a que se aplica a politica de seguranca, i.e. cobertos por esta ultima.

Unconstrained Data Items (UDI) Dados de entrada para o sistema.

• UDIs tem que ser convertidos em CDIs ou entao sao ignorados.

Transformation Procedures (TP) Programas que operam sobre CDIs.

• CDIs so podem ser modificados por TPs.

Integrity Verification Procedures (IVPs) procedimentos que verificam a integridade dos dados.

1. O sistema tem que manter de forma segura a lista de CDIs que cada TP pode aceder;

2. O sistema tem que manter de forma segura a lista de TPs que cada utilizador pode invocar;

3. O sistema tem que autenticar cada utilizador que invoca uma TP;

4. Apenas um sujeito que pode certificar uma regra de acesso duma TP, pode modificar essa regra. Este sujeito nao deve ter direitos de invocacao da TP.

• Esta restricao e um exemplo da separacao de funcoes.

17 - Explique em que medida o conceito de inferência pode representar um problema de segurança na gestão de uma base de dados.

O conceito de inferencia é definido como a capacidade de derivar ou inferir dados sensiveis apartir de outros dados não sensiveis.

18 - Considere as bases de dados com segurança multi-nível. Explique:

a. Qual é o seu modelo genérico de operação?
b. Como se concretiza a mesma usando a cifra da valores sensíveis.

a)De uma forma geral, os mecanismos de controle de acesso obrigatório impõem segurança multinível, pois exigem a classificação de usuários e de valores de dados em classes de segurança e impõem as regras que proíbem o fluxo de informação a partir dos níveis de segurança mais altos para os mais baixos.

b) os campos estao cifrados com uma chave correspondente ao nivel de segurança

18 - Considere as bases de dados com segurança multi-nível. Indique duas formas de evitar que uma aplicação com um nível de segurança consiga usar dados classificados com níveis de segurança superiores.

Separação da base de dados em bases de dados correspondentes a cada nivel de segurança. Cifra dos campos dos registos da base de dados em que a chave está relacionada com o nivel de segurança à qual as aplicaçoes de nivel mais baixo não têm acesso.

18 - Explique em que medida, e porquê, os smart cards são úteis na exploração dos pares de chaves assimétricas.

Porque a chave privada esta dentro do cartao e nao pode ser extraida sem a destruição do mesmo, isto significa que o utilizador pode criar assinaturas digitais facilmente e sem comprometer a segurança.

20. Considere a revogação de certificados de chaves públicas. Explique:

a. Em que consiste um certificado de revogação.
b. Por que razão é preciso manter e consultar listas de certificados de revogação.

a) é um certificado especial que afirma que uma dada chave publica pertence a uma dada entidade deixa de ser

valida apartir de uma certa data.

b) existem varias razoes para a revogaçao de um certificado e a maioria pode trazer riscos de segurança. Por esta razão é desejavel saber quais os certificados que ainda são considerados correctos!1!1One!

19 Qual é o propósito dos registos universais de vulnerabilidades comuns (Common Vulnerabilities and Exposures, CVE)?

Vulnerabilities e exposições comuns, ou CVE, é um dicionário da segurança público-sabida da informação vulnerabilities e exposições.

20 - Explique por que razão as Java Virtual Machines (ou os Java Run-time Environments) não permitem que as classes java.* sejam carregadas a partir da rede.

Porque permite modificar as classes base do java.

20 - As classes Java carregadas numa Java Virtual Machine (ou num Java Run-time Environment) são segregadas por
diferentes Protection Domains. Explique:

a. Que vantagens advém dessa segregação?
b. Qual é a política base para a sua realização?
a) as classes de cado dominio partilham das mesmas permissoes, que são se registringem às minimas necessárias para que as classes possam desempenhar as suas funções. Deste modo é impossivel que uma classe dum dominio interfira com outro, por exemplo: uma classe de acesso ao suporte de armazenamento de dados fisico não deve ter acesso a funções de FUCK THIS I'LL BE A STRIPPER acesso à rede.
b) É uma aplicação do principio do privilégio minimo (“least privilege”)

20. **Explique por que razão as Java Virtual Machines (ou os Java Run-time Environments) impõem restrições aos locais de onde carregam classes para uma determinada aplicação?**

AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA