Departamento de Informática
Faculdade de Ciências e Tecnologia
UNIVERSIDADE NOVA DE LISBOA

Curso de Engenharia Informática (2º Ciclo)

Segurança em Sistemas e Redes de Computadores

SSRC-0809-EN-2.1.A

2º Semestre 2007/2008

Exame de Época Normal, 11/Julho/2008

Notas:

- O enunciado tem 6 questões, divididas em diversas alíneas. Pode optar por responder a qualquer uma das questões identificadas com A ou B, de forma alternativa.
- Podem utilizar-se quaisquer elementos de consulta excepto computadores ligados em rede ou quaisquer outros dispositivos de comunicações.
- As respostas a entregar devem estar escritas a tinta.
- Deve ler-se completamente e com atenção cada questão e as suas alíneas antes de responder.
- A interpretação do enunciado é considerada um factor de avaliação.
- A duração da prova é de 2h30min

---------- A preencher pelos alunos ----------

Nº de aluno: _____ Nome: _____

Nº TOTAL de páginas entregues (excepto esta capa): _____
(numere as páginas na forma nº da página /Nº TOTAL e coloque o nº e nome em cada página.)

---------- A preencher pelo docente ----------

1)	2)	3)	4)	5)	6)	TOTAL

INF Controlo:

Questão 1)

a) Em que consiste, do ponto de vista da operação de cifra, a utilização do parâmetro DESede para referir o algoritmo criptográfico a usar no caso de um programa JAVA que utiliza o suporte JCE ? Justifique a sua resposta em função das operações que têm lugar subjacente à operação de cifra associada ao parâmetro DESede.
b) Que vantagens identifica em utilizar uma sequência CIFRA-DECIFRA-CIFRA, intrínseco ao método subjacente ao parâmetro DESede indicado ?
c) Na utilização da cifra DESede pode usar-se chaves de 112 bits ou de 168 bits. De acordo com a) e b) como são usadas as referidas chaves ?

Questão 2)

Considere que está a usar Triple Des com dupla chave (112 bits) e modo ECB. Se existir um erro num bloco cifrado (*cipherpext*) transmitido, apenas o bloco em claro (*plaintext*) correspondente sairá afectado. Se no entanto usar modo CBC, haverá uma propagação do erro na operação de decifra. Por exemplo, se o erro num bloco ciphertext Ci (de uma sequência de blocos cifrados transmitidos) ocorrer, isso implicará em errros nos blocos Pi e Pi+1.

a) Algum dos blocos posteriores a pi+1 será afectado ? Como ?
b) Qual o tamanho dos blocos Pi e Ci nas condições enunciadas ?
c) Suponha que tem um ficheiro F, que vai ser transmitido de acordo com as condições enunciadas, sendo inicialmente dividido em blocos F1, F2, F3, …. Fn | PADDING. A ideia é que estes blocos funcionarão como blocos P1, P2, … Pn|PADDING que serão então cifrados para os blocos C1, C2, … Cn, nas condições enunciadas. Admita que, ao fazer-se o processamento de divisão pelos blocos Fi, ocorreu um erro num bit, num certo bloco Fj. Deste modo, o bloco Pj conterá um erro num bit em relação à informação original do ficheiro, tendo este erro sido provocado antes da operação de cifra para posterior transmissão. Qual vai ser a implicação no receptor, quando tentar recuperar o ficheiro original ? Justifique a sua resposta.
d) Qual a vantagem de utilizar como PADDING, nas condições referidas, um método de padding do tipo PKCS1, PKCS5 ou PKCS7 (nota: recorde-se que as operações de Padding enunciadas são simplesmente parametrizáveis na inicialização das estruturas de cifra, nomeadamente quando está a utilizar um ambiente do tipo Java JCE).

Questão 3)

a) Qual a diferença entre uma assinatura digital baseada num método HMAC e outra baseada num método CMAC ? Comparativamente, que vantagens ou desvantagens apresentaria entre os dois esquemas ?
b) Um principal adopta uma assinatura CMAC para autenticar uma mensagem M. Para a assinatura vai usar o método Triple DES parametrizado com uma chave K de 168 bits (ou tripla chave DES), modo CBC e um vector de inicialização nulo. Sendo necessário, utilizará PADDING nulo. Envia então a assinatura CMAC, juntamente com a mensagem M para um principal com quem partilha a chave K. Se o receptor utilizar Triple DES mas usar um modo CFB em vez de CBC (com blocos de 64 bits) e usar o bloco C1 como vector de inicialização, isso permitiria reconhecer a assinatura. Isto é verdadeiro ou falso ? Justifique.
c) Explique qual a diferença entre resistência fraca a colisões e resistência forte a colisões numa função de síntese segura. Diga quais as implicações, do ponto de vista de segurança, entre utilizar uma função de síntese segura H() que apenas suporta uma das propriedades e não a outra, numa assinatura digital de chave pública (exemplo uma assinatura RSA), independentemente do método de *Padding* que for utilizado.

Questão 4)

O seguinte protocolo, que concretiza a noção de *3-Way authentication procedure* utilizando certificados X509v3, tal como é apresentado por Stallings (blibliografia base da disciplina) contém uma vulnerabilidade. Recordando, no essencial, o protocolo referido representa-se a seguir, de acordo com a notação seguida pelo autor para as assinaturas de autenticidade subjacentes ao protocolo.

A > B A {ta, rA, B}
B > A B {tB, rB, A, rA }
A > B A {rB}

Na discussão do protocolo, o autor refere que o teste dos valores tA e tB pode ser opcional. Suponha no entanto que A e B já anteriormente tinham utilizado o mesmo protocolo e que, um adversário C (actuando como MIM), tinha então interceptado as três mensagens do protocolo. Suponha que A e B possuem uma implementação do protocolo que opta por não fazer qualquer verificação e processamento de tA e tB como *nonces* e que decidem passar esses valores como constantes (por exemplo, com valores nulos).

Suponha que, mais tarde, C desencadeia um ataque da seguinte forma:

C > B A{0, rA, B }
Ao que B responde (pensando estar a comunicar com A):
B > C B{0, rA' , A, rA }

Admita que C convence posteriormente A a desencadear uma autenticação perante si, actuando em nome de B (eventualmente por um ataque prévio de tipo *phishing* a A que o leve a desencadear um protocolo de autenticação perante C).

Nesse caso A vai desencadear o protocolo de acordo com a sua implementação:
A > C A{ 0, rA' , B }

C, pode responder a A da seguinte forma, usando o mesmo *nonce* dado a C por B:
C > A C{ 0, rB' , A, rA' }

ao que A, naturalmente responderá:
A > C A{rB'}

E isto é exactamente o que C precisa para convencer B de que está comunicando com A. Assim, C enviará para B

C > B A{rA'}

Sugira uma melhoria ao protocolo, o mais simples possível (ou com o menor impacto possível do ponto de vista de implementação), para evitar o ataque indicado.

Questão 5)

Tome como referência a estrutura dos chaveiros de chaves públicas e chaves privadas tal como estão especificados no sistema PGP.

a) Os primeiros 16 bits do resultado da função de síntese que for usada numa assinatura numa mensagem PGP são colocados em claro na estrutura da mensagem. Tal tem um objectivo concreto. Qual é o objectivo e qual a sua relevância ?
b) Em que medida o facto referido em a) afecta ou diminui a segurança e até que ponto a decisão de passar os referidos 16 bits em claro permite de facto conseguir o objectivo pretendido? Justifique a sua resposta.
c) Apresente duas estruturas de dados designadas por PubkeyRing e PrivatekeyRing que mapeiem o mais rigorosamente possível a especificação desses chaveiros. *Sugestão: o mais simples é apresentar duas estruturas de dados em JAVA, por exemplo.*
d) Escreva, em pseudo-código, a função ProcReceivedCertif (X509 Certificate) que, recebendo um certificado de chave pública que chegou numa mensagem de Email, realiza o processamento de actualização, de acordo com a especificação e as condições de gestão de confiança, do chaveiro de chaves públicas.

    Nota: Pode definir funções e parâmetros, indicando qual a sua especificação das mesmas do ponto de vista do processamento intermédio que asseguram e que sejam usadas ao nível do pseudo-código dea função ProcReceivedCertif().

Questão 6)

a) Uma vez que o protocolo TCP garante ordenação de mensagens numa conexão Cliente/Servidor, porque é que o protocolo SSL (ou TLS) possui um mecanismo usado pelo receptor para reordenar blocos ao nível do *Record Layer Protocol (RLP)* que eventualmente cheguem fora de ordem ? Justifique.
b) Refira que vantagens ou desvantagens comparativas encontra, do ponto de vista de **segurança** e do ponto de vista de **eficiência**, entre utilizar um modo autenticação do tipo FIXED-DIFFIE-HELLMAN ou EPHEMERAL-DIFFIE-HELLMAN na parametrização de uma conexão SSL ? Justifique bem a sua resposta.
c) O sistema CLIP, visto como uma aplicação WEB e que bem conhece, utiliza como estratégia de segurança o suporte SSL com autenticação unilateral e autenticação de utilizadores com passwords ditas estáticas. Suponha que se pretende realizar uma melhoria de segurança no serviço CLIP e que se colocam três cenários: no primeiro cenário coloca-se a possibilidade de proteger o tráfego subjacente às interacções com base em IPSec. No segundo cenário coloca-se como hipótese passar a usar SSL em modo de autenticação mútua. O terceiro cenário têm em vista passar a usar um esquema do tipo OneTimeKeys (ou SecureIDs) com tokens para autenticação multi-factor e com base em passwords dinâmicas, distribuídos aos utilizadores. Critique cada uma das opções em termos de vantagens, desvantagens, o que cada cenário poderia melhorar em termos de defesas e que tipos de ataques continuariam a

poder ficar em descoberto. NOTA: considere apenas ataques baseados num modelo de adversário do tipo Dolev-Yao.

Questão 7A)

a) De acordo com o que conhece do protocolo SET e da sua especificação concreta, como pode o "cardholder" ter certeza que em circunstância alguma o seu número de cartão de crédito será do conhecimento de um "Merchant" ? Justifique a sua resposta.
b) O protocolo SET protege ou não um "Merchant" de poder vir a não receber o valor de uma venda por repúdio posterior por parte do "Acquirer" de ter que se responsabilizar por esse pagamento ? Note que a obtenção do pagamento e a efectivação da venda são eventos assíncronos (separados de vários dias ou mesmo semanas). Justifique a sua resposta.

Questão 7B)

Quando se usa IPSec em modo túnel, é necessário acrescentar um novo cabeçalho IP de um pacote externo para encapsular um pacote interno (inner).

a) O pacote externo (de encapsulamento) pode ser IPV6, encapsulando um pacote interno IPV4 ? O pacote externo (de encapsulamento) pode ser IPV4, encapsulando um pacote interno IPV6 ? Justifique a resposta.
b) Embora a especificação IPSec contemple a possibilidade de duas associações de segurança (SAs) em modo transporte poderem associar AH e ESP no mesmo fluxo de dados, apenas uma ordem de processamento desses protocolos (ESP depois de AH ou AH depois de ESP) fará mais sentido ou poderá ser mais apropriada. Qual e porquê ? Justifique a sua resposta.