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

Curso de Engenharia Informática (2º Ciclo)
Teste nº 2 (frequência), 19/Dez/2009

Segurança em Sistemas e Redes de Computadores

SSRC-0910-EN-2.1.A

Notas:

- O enunciado tem 6 questões, divididas em diversas alíneas e duas partes: uma sem consulta (3 questões) e outra com consulta (3 questões). Cada uma destas partes deve ser respondida em cerca de 1 hora.
- Podem utilizar-se na parte com consulta 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 ou justificação e argumentação das respostas face às perguntas é considerado um factor de avaliação.
- A duração da prova é de 2h00min

---------- 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) (SEM CONSULTA)

a) Que vantagens e desvantagens encontra em utilizar um modo de cifra simétrica como o CTR. Apresente a sua resposta, argumentando bem porque considera essas vantagens e desvantagens. De modo a clarificar a resposta pode justificar com base em cenários de aplicação que permitam justificar a preferência por outros modos.

b) Considere o modo de cifra CFB (Cipher Feedback Block Mode). Em que situações adoptaria este modo e porquê ? (Justifique a resposta, ilustrando com m exemplo de protocolo ou de aplicação em que escolheria utilizar esse modo como uma possível escolha).

c) No modo CFB, considerando uma unidade de transmissão com tamanho de x bits, representa-se o processamento do modo da seguinte forma:

C1 = P1 XOR { Sx(IV) }K
Ci = Pi XOR { Sx(Pi-1) }K

C1) Em que consiste a função Sx () ?
C2) Indique uma expressão que permita obter P1 e blocos genéricos Pi em função ds blocos cifrados.

d) Considere que e pretende implementar uma função de síntese segura – que chamaremos de RSAHashing (recorde as suas propriedades principais) utilizando um método assimétrico como o RSA. A ideia é processar uma síntese a partir de uma mensagem M do seguinte modo (utilizando algum processamento de Padding normalizado e conhecido), ex., OAEP ou qualquer outro:

- Primeiro fragmenta-se a mensagem em múltiplos blocos M1, M2, …. Mn
- Cifra-se o primeiro bloco B1 = { M1 }Kpriv
- A seguir obtém-se M2' = B1 XOR M2 e cifra-se de modo a obter B2 = {M2'}Kpriv
- itera-se sucessivamente o processo da mesma forma até ao último bloco, de modo a obter-se então Bn.
- No final, o bloco Bn seria usado como síntese da mensagem

Este processo de realiza uma síntese seria seguro ? (mais uma vez recorde as propriedades de uma síntese segura).

Para ajudar na sua resposta, verifique que com o processo referido:

RSAHashing(B1, B2) = RSA (RSA (B1) XOR B2)
Em que RSA(Bi) = Bi^Kpriv mod N, para um par de chaves Kpriv, Kpub, sendo Kpub e N conhecidos.

Note que o método não seria seguro se RSAHashing (C1, C2) = RSAHasing (B1,B2) desde que um atacante escolha arbitrariamente C1 e C2, pois isso violaria a propriedades da resistência fraca a colisões.

Questão 2) SEM CONSULTA, resposta dada no máximo em meia página.

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. Nota: A{X1, X2, …} Significa que a concatenação dos campos Xi está assinada por A (com base em criptografia assimétrica).

A > B A {tA, rA, IdB}
B > A B {tB, rB, IdA, 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, IdB }
Ao que B responde (pensando estar a comunicar com A):
B > C B{0, r'B , IdA, 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, r'A , IdC }

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

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

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{r'B} Pelo que B acredita que está a comunicar com A.

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, sem utilizar timestamps que obriguem a sincronização de relógios.

Questão 3) SEM CONSULTA

a) Considere o protocolo Kerberos, que se fornece em anexo. Supõe-se que interprete correctamente o protocolo e tenha em consideração o funcionamento e propósito do mesmo.

De modo a evitar o problema deste protocolo ser vulnerável no caso de ataque às passwords de clientes no contexto da interacção de autenticação com o componente AS, pretende-se propor uma nova solução que parte do princípio que se usam certificados X509v3 associados apenas ao componente AS e a todos os clientes que se precisam de autenticar. Estes certificados serão geridos e distribuídos a partir de uma solução PKI.

Proponha uma alteração ao protocolo para viabilizar esta solução. A sua solução deve ser compatível com o restante fluxo de mensagens do protocolo (interacções com os componentes TGS, servidores finais e suporte a múltiplos domínios de autenticação).

Nota: basta alterar as mensagens necessárias e apresentar a justificação. Pode responder na própria folha (anexa) onde se encontra a especificação do protocolo (Kerberos V5)

b) Apresente uma especificação sumária sobre a arquitectura da solução do trabalho prático nº 2. Na arquitectura deve apresentar um esquema com os componentes da arquitectura e uma descrição da sua operação e deverá especificar o fluxo de mensagens previsto para a autenticação de clientes (utilizadores finais). Sugestão: apresente a sua resposta em dois níveis:

   B1) Arquitectura, descrição de componentes e fluxo geral das mensagens (com a informação relevante que viaja em cada mensagem) para a execução do protocolo de autenticação. Nesta descrição deve indicar quais os dados de setup (segredos, chaves criptográficas, etc) que cada entidade tem instalados para poder executar o protocolo de autenticação.
   (1 página)

   B2) Apresente então noutra página a estrutura das mensagens, com o detalhe necessário em relação às operações criptográficas ou tipos de dados, justificando em cada mensagem o papel desses dados e o que se tenciona proteger no protocolo de autenticação.

Questão 4 (com consulta)

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.

Questão 5 (com consulta)

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) 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 (com consulta)

Suponha que se tem uma implementação do sistema SET suportada integralmente em SSL e que utiliza autenticação mútua entre todas as entidades na comunicação para suportar todo o fluxo de mensagens do protocolo. Seria possível que alguns dos certificados utilizados pelas entidades SET pudessem corresponder aos certificados X509v3 que já devem existir para as próprias conexões SSL ? Quais e porquê ? Justifique adequadamente a sua resposta.