(Ref. 20170707)

DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores - 2º Sem. 2016/2017
Prova Final de Exame (Recurso e Melhoria) - 7/Julho/2017

PARTE I (Questões para resposta sem consulta)

Questão 1

a) Defina as seguintes duas tipologias de mecanismos de segurança usados em serviços de segurança (usando a terminologia da *framework* X.800)
   C1) Mecanismos específicos
   C2) Mecanismos *pervasivos* (ou permeados)

b) Considerando um serviço ou aplicação WEB protegido por HTTPS (que utiliza por exemplo um servidor aplicacional com arquitetura do tipo LAMP (Linux, Apache, MySQL e PHP) refira três diferentes mecanismos de cada um dos tipos definidos em b) que estejam associados à operação de segurança dessa solução).

c) Considere a tipologia de ataques, serviços e mecanismos de segurança definidos na *framework* OSI X.800. Tenha em conta a subcategorização da propriedade da confidencialidade nas respetivas categorias (*connection confidentiality, connectionless confidentiality, selective-field confidentiality e traffic flow confidentiality*). Quais dessas subcategorias não são garantidas no suporte de confidencialidade fornecido pelo protocolo TLS

Questão 2

Considere a terminologia X.800 ou RFC2828 associadas às subcategorizações da propriedade de integridade de dados (*Data-Integrity*) e o contexto de construções de assinaturas digitais com métodos de chave pública.

Um emissor enviou uma mensagem de correio electrónico PGP, usando o algoritmo de assinatura RSA e *padding* seguro OAEP para assinar a mensagem. Diga se se verificam as seguintes garantias:

G1) Verificação de integridade orientada à conexão, ~~sem~~ com recuperação (*Connection-integrity with Recovery*), na validação do receptor.

G2) Integridade parcial não orientada à conexão (*Selective-Field Connectionless Integrity*) na validação do receptor

G3) Se o emissor enviar duas mensagens iguais as assinaturas de cada uma que serão verificadas pelo receptor serão diferentes no seu conteúdo (bytes), embora iguais na dimensão.

G4) Se o emissor enviar duas mensagens iguais as assinaturas de cada uma que serão verificadas pelo receptor serão diferentes no seu conteúdo (bytes) e também na sua dimensão.

Questão 3

Considere o sistema Kerberos, quer na variante estudada V4 como na versão V5. A utilização de um sistema de autenticação multifator que utilizesse tokens permitiria melhorar a segurança do protocolo? Em quê, porquê e como ?

Questão 4

No sistema PGP, se receber uma mensagem de Email associada à disseminação de uma revogação de uma chave pública que se encontra no chaveiro de chaves públicas do receptor, qual deve ser o procedimento atendendo ao estado em que a entrada dessa chave pública e respetiva informação de confiabilidade ? Justifique.

Questão 5

Considere o modo de autenticação FIXED-DIFFIE-HELLMAN como opção que se pode usar por normalização de *handshake* do protocolo TLS.

a) Em que consiste esse modo e como funciona quando se tem autenticação mútua Cliente/Servidor ?

b) O que garante a autenticação de um *endpoint* na validação realizada pelo outro ?

c) Neste tipo de *handshake* é possível garantir segurança futura perfeita ? Justifique.

Escolha uma e uma só das seguintes questões 6-A ou 6-B para responder:

Questão 6-A

Tenha em conta os modelos de controlo de acesso DAC e RBAC.
Considere um sistema de software em que existem 10 diferentes papéis $\mathbf{R}_i$ (com i=1,2,3, ... 10) associados a funções diferenciadas que os utilizadores exercem quando executam operações que o sistema disponibiliza. Para cada papel $\mathbf{R}_i$ existem $\mathbf{N}_i$ utilizadores (com j=1, 2, 3 .... n) e o número de permissões requeridas para a esse papel é P_i (com i=1,2,3,... m).

a) Qual é o número necessário de relações que devem ser definidas entre utilizadores (autenticados) no sistema e permissões, no caso de se ter um modelo de controlo de acessos do tipo DAC ? Justifique.

b) Quantas relações devem ser definidas entre utilizadores (autenticados) no sistema e permissões, no caso de se adoptar um modelo controlo de acessos do tipo RBAC ? Justifique.

Questão 6-B

A autenticação de um utilizador no UNIX utiliza um ficheiro de texto */etc/passwd*. Esse ficheiro contém uma linha para cada utilizador do sistema com

- *username* do utilizador
- *userid*
- A entrada contem também um valor de 16 bits (*salt*) que é gerado aleatoriamente quando o utilizador é criado
- um *hash* PH que envolve ao salt e a password escolhida pelo utilizador. O algoritmo usado para calcular PH é conhecido.

a) Quando um utilizador faz login apresenta o seu *username* e a sua *password*. Como é que é verificada a identidade do utilizador?
b) O ficheiro */etc/passwd* pode ser lido por qualquer utilizador. Diga como poderia ser conseguido um ataque para obter passwords de utilizadores.
c) Considere que se modifica o sistema descrito de forma a que a informação anteriormente guardada no ficheiro */etc/passwd* é dividido por dois ficheiros:
   - um ficheiro */etc/passwd* onde fica toda a informação anteriormente disponível sobre o utilizador (nome, uid, gid, ...) mas não fica o hash PH.
   - um ficheiro */etc/shadow* onde fica apenas o uid e o hash PH

   Explique as vantagens desta divisão da informação por dois ficheiros.

DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores - 2º Sem. 2016/2017
Prova Final de Exame (Recurso e Melhoria) - 7/Julho/2017

PARTE II (Questões de resposta com consulta)

Questão 6

Numa máquina UNIX/Linux o programa *sendmail* executa-se tendo associado o uid root e
- faz bind de um socket para a porta 25 (o que só o utilizador *root* pode fazer)
- recebe mensagens para encaminhar ou entregar a utiizadores (*mailboxes*) locais dessa máquina
- usa o protocolo SMTP

As mensagens para um utilizador local AAA são depositadas num ficheiro que pertence a este utilizador e cujas permissões num sistema UNIX são

- owner AAA
- group AAA
- Permissões (máscara de permissões): rw- --- ---

Naturalmente na mesma máquina poderá haver vários utilizadores que recebem *mail* nesse sistema.

a) Seria necessário que o programa *sendmail* executasse tendo sempre associado o *uid* da *root* ? Como é que relaciona esta situação com o princípio dos mínimos privilégios (tal como definido nos princípios e requisitos de concepção de um sistema de controlo de acesso) ?

b) Porque é que esta abordagem comporta riscos de segurança ?

c) Proponha uma alternativa para o funcionamento do programa sendmail que minimizasse os aspectos que descreveu em b)

Questão 7

a) Como alternativa ao modo CBC e processamentos de *padding* PKCS#5 ou PKCS#7, no processamento de um algoritmo criptográfico simétrico, pode adoptar-se um modo vulgarmente conhecido por CTS – *Ciphertext Stealing*), como representado em anexo. Analise esse processamento comparativo ao CBC diga que vantagens encontra na adopção deste modo comparativamente a CBC. Refira um exemplo em que essa vantagem pode ser interessante.

b) No sistema PGP (como estudado ou descrito no RFC 2440 referente à implementação OpenPGP), nas operações de cifra de mensagens de correio electrónico usa-se o modo CFB e não o modo CBC. Do ponto de vista de segurança não haveria grande diferença, mas no caso concreto do PGP que vantagens vê na utilização do modo CFB ? Justifique.

c) Uma assinatura RSA com construção PSS pode ser programada em JAVA (usando o suporte JCE), definindo-se e parametrizando-se do seguinte modo:

Signature signature = Signature.getIntance ("SHAwithRSAandMGF1");

O processamento em concreto desta assinatura sobre uma mensagem M faz-se com base em quatro passos de computação:

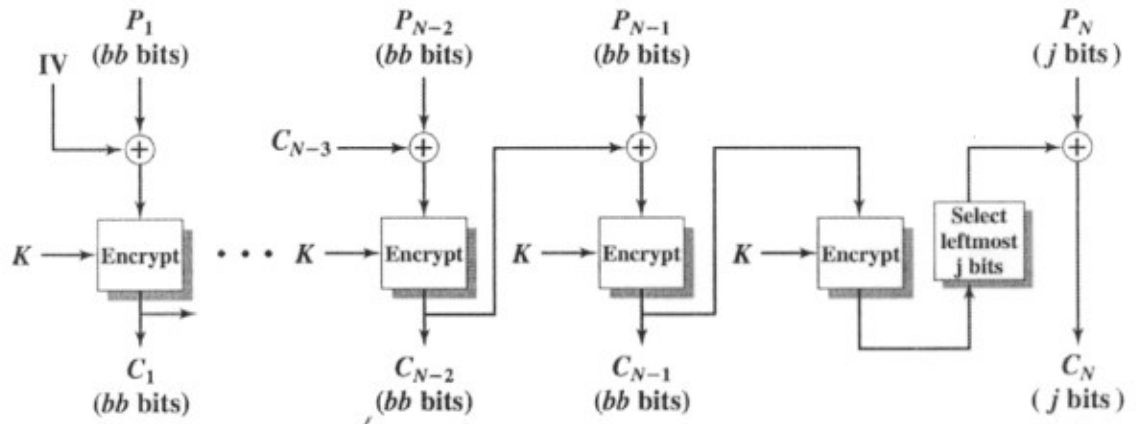
1. M1 = 0x00 || 0x00 || 0x00 || 0x00 || 0x00 || 0x00 || 0x00 || 0x00 || H(M) || S
2. M2 = 0x00 || 0x00 || 0x00 || 0x00 || 0x00 || 0x00 || 0x00 || 0x00 || 0x01 || S
3. M3 = Mask (M2, H(M1)) || H(M1) || 0xBC
4. Ms = RSAencrypt(Kpriv, M3) sendo Ms a assinatura calculada.

Num processamento típico como indicado, *S* é um valor aleatório designado por SALT (20 bytes), *H(M)* é uma função de síntese segura (no caso da definição acima será SHA1), Mask() é uma função de mascaramento ou de transformação *one-way* (com propriedades semelhantes a uma síntese segura– no caso concreto a função MGF1 usa SHA-1 como último passo e devolve 160 bits).

Questão: Se estamos a usar pares de chaves RSA de 2048 bits (isto é, vamos assinar com chave privada de 2048 bits) existe um tamanho máximo da mensagem M (original) que se pode assinar no caso de uso daquela construção? Justifique.

d) Que vantagem vê na utilização da construção de assinatura digital PSS (na alínea b) quando se processam assinaturas de mensagens cujos conteúdos têm tendência a ser muitas vezes iguais ? Justifique.

ANEXO para resposta à questão 8 a)



ANEXO para resposta à questão 10

(1) C → AS $Options \| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1$

(2) AS → C $Realm_c \| ID_C \| Ticket_{tgs} \| \mathrm{E}(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$Ticket_{tgs} = \mathrm{E}(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $Options \| ID_v \| Times \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $Realm_c \| ID_C \| Ticket_v \| \mathrm{E}(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$Ticket_{tgs} = \mathrm{E}(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

$Ticket_v = \mathrm{E}(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| \mathrm{AD}_C \| Times])$

$Authenticator_c = \mathrm{E}(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Options \| Ticket_v \| Authenticator_c$

(6) V → C $\mathrm{E}_{K_{C,V}} [\, TS_2 \| Subkey \| Seq\# \,]$

$\mathrm{Ticket}_v = \mathrm{E}(K_v, [\mathrm{Flags} \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = \mathrm{E}(K_{c,v}, [ID_C \| Realm_c \| TS_2 \| Subkey \| Seq\#])$

(c) Client/Server Authentication Exchange to obtain service