DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Segurança de Redes e Sistemas de Computadores
2º Semestre, 2015/2016

PROVA DE EXAME, 17/Junho/2016)

A preencher pelo aluno

Nº Aluno	
Nome	
Nº de Folhas entregues, sem contar com esta folha)	

A preencher pelos docentes

Grupo do Trabalho Prático		
TRAB 1:	Nº	Nº
TRAB 2:		

Avaliação do Teste

DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores
2º Semestre, 2015/2016

PROVA DE EXAME, 17/Junho/2016) / PARTE I

Questão 1

Considere a *framework* de segurança X.800, os seus conceitos e terminologia. Tenha em conta as noções e definições das propriedades de segurança, serviços de segurança, mecanismos de segurança e tipologias de ataques.

a) Qual a diferença entre mecanismos de segurança e serviços de segurança ?

b) Qual a diferença entre as propriedades designadas por "*Connection Confidentiality*" (ou confidencialidade orientada à conexão) e "*Connectionless Confidentiality*" (ou confidencialidade não orientada à conexão) ? Dê um exemplo para ilustrar essa diferença tendo por base as propriedades asseguradas pelo protocolo TLS no que diz respeito à garantia dessas propriedades.

c) Os mecanismos de segurança são classificados em duas categorias: mecanismos permeados (*pervasive mechanisms*) e mecanismos específicos (*specific mechanisms*). Indique a diferença entre estas duas noções e dê exemplo de mecanismos de um e de outro tipo.

d) Considerando a tipologia de ataques definidos na *framework* X.800, diga, justificando a sua resposta, que tipologias de ataques são defendidos por cada um dos seguintes mecanismos:

   A) HMACs eouCMACs
   B) Uma assinatura de chave pública que usa RSA, combinando uma síntese SHA256 e padding PKCS#1
   C) Uma função de síntese que usa o algoritmo SHA512
   D) O algoritmo assimétrico de Diffie-Hellman
   E) Um algoritmo criptográfico assimétrico como RSA.

e) Porque é que uma prova de autenticidade e integridade estabelecida por um algoritmo HMAC ou CMAC não pode assegurar o princípio de não repudiação de mensagens trocadas entre dois subscritores um canal de comunicação seguro ? Justifique a sua resposta.

Questão 2

a) Num processo de criptanálise (ou criptoanálise) de um dado algoritmo criptográfico , o que diferencia a abordagem dos critérios de estudo a seguir identificados? Na sua diferenciação deve identificar bem o que é conhecido pelo criptanalista (ou criptoanalista) em cada caso, considerando: O algoritmo criptográfico em causa,

   Critério I - *Type of Attack: Chosen Plaintext*
   Critério II – *Type of Attack: Chosen Text*

b) À parte o custo computacional necessário e o tempo necessário para realizar um ataque de força bruta a um algoritmo criptográfico, indique os dois critérios práticos que estão na base de se considerar que para uma determinada aplicação um determinado algoritmo criptográfico seja considerado computacionalmente seguro

c) Considere o algoritmo criptográfico simétrico DES que usa uma chave de 56 bits, o que é considerado hoje susceptível de ser uma cifra fraca face a ataques por força bruta. Para mitigar essa fragilidade e continuar a usar o algoritmo base, pode adoptar-se uma implementação baseada em Triple DES. Indique em que consiste o processamento Triple DES, qual o racional da sequência das operações envolvidas no processamento para cifrar e decifrar e qual a dimensão da chave criptográfica que pode ser usada ?

d) Considere o processamento do modo CTR usando um algoritmo criptográfico simétrico para cifra dos blocos (P1, P2, ... Pn). A representação desse processamento pode ser descrita pela seguinte função:

Ci = Pi xor E(K, CTRi)
Em que CTRi corresponde ao passo de um contador
Pi representa o bloco plaintext i
Ci representa o bloco ciphertext i

Escreva a função que dado cada bloco Ci decifra o respetivo bloco Pi
Pi = ...

f) Vai ter que escolher um modo de cifra de blocos para cifrar informação com um algoritmo simétrico (como por exemplo AES), num protocolo cliente/servidor que implementa uma aplicação de emulação de um terminal virtual remoto (com as características similares a SSH). A ideia é proteger a confidencialidade da informação trocada entre o cliente e o servidor. De enter todos os seguintes modos: ECB, CBC, CTR, OFB ou CFB, que modo escolheria e qual os fatores principais que o levaria a escolher esse modo.

Questão 3

Considere a utilização de um algoritmo criptográfico simétrico para cifra de blocos. Um emissor pretende cifrar um ficheiro, enviando sucessivamente diversos blocos (*ciphertext)*, C1, C2, ... Cn, usando um determinado modo. O canal para o emissor transmitir o ficheiro cifrado ao receptor não é fiável e pode perder mensagens ou pode trocar bits na informação transmitida.

a) **Considere inicialmente o caso em que apenas se observam trocas de bits (e não perda de bits ou de mensagens).**

a1) Se estiver a usar ECB, verificando-se uma troca de um bit num dado bloco Pi, até que ponto isso afecta a transferência de todo o ficheiro e como poderia recuperar essa situação? Justifique.
a2) Considerando a situação tal como em a1), qual a diferença se estiver a usar o modo CBC ? Justifique.
a3) Considerando a situação tal como em a1) ou a2), qual a diferença se estiver a usar o modo CFB ? Justifique

b) **Considere agora o caso em que se observam perdas de mensagens (mas não perdas de bits de cada mensagem nem trocas de bits na mesma mensagem).**

b1) Se estiver a usar ECB, verificando-se a perda de um bloco Pi, até que ponto isso afecta a transferência de todo o ficheiro e como poderia recuperar essa situação? Justifique.
b2) Considerando a situação tal como em b1), qual a diferença se estiver a usar o modo CBC ? Justifique.
b3) Considerando a situação tal como em b1) ou b2), qual a diferença se estiver a usar o modo CFB ? Justifique

DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Segurança de Redes e Sistemas de Computadores
2º Semestre, 2015/2016

PROVA DE EXAME, 17/Junho/2016) / PARTE II

Questão 4

a) Dizemos que a vantagem de usar o algoritmo de *Diffie Hellman* num processo de estabelecimento de chaves entre dois principais é que tal assegura propriedades de segurança futura perfeita e segurança passada perfeita. Em que consiste essa noção e porque é que essa propriedade é satisfeita? Justifique.

b) Explique em que consiste um ataque homem no meio que comprometa o estabelecimento de um canal seguro que assegure confidencialidade, quando é usado o método de *Diffie-Hellman* (DH) para estabelecer a chave de confidencialidade. Estruture a sua resposta mostrando como se processa o acordo de DH entre dois principais A e B e os cálculos computacionais envolvidos.

c) Para evitar o ataque em b), A e B possuem certificados de chave pública RSA (X509v3), emitidos por uma Autoridade de Certificação da confiança de A e B e que trocaram e validaram entre si, anteriormente ao desencadeamento do protocolo do acordo DH que desencadearão de seguida. Uma vez verificados esses certificados A passa a ter confiança na chaves públicas de A (KpubA) e B passa a ter confiança na chave pública de B.

   Então, para desencadearem o acordo DH evitando o ataque homem no meio em b), bastará:

   C1) que A e B troquem os números privados no acordo DH de modo que estes são assinados com as respetivas chaves privadas

   C2) que A e B troquem os números públicos do acordo DH, sendo estes cifrados pelo emissor usando a chave pública dos destinatário

   C3) que A e B troquem os números públicos no acordo DH de modo que estes são assinados pelo emissor com as respetivas chaves privadas

   C4) que A e B troquem os números públicos no acordo DH de modo que estes são assinados pelo emissor com as respetivas chaves privadas, mas estejam necessariamente protegidos pela chave pública do receptor

Questão 5

a) Um emissor pretende cifrar uma mensagem M de 4 Kbits assegurando confidencialidade no envio de M , usando para o efeito uma chave pública do destinatário, e cifrando M usando o algoritmo RSA. A chave pública do destinatário tem 2048 bits. Isso é possível ? Justifique.

b) Um emissor pretende assinar uma mensagem M de 4 Kbits com a sua chave privada RSA, de modo a enviar a assinatura de M a um destinatário. A chave privada a usar tem 2048 bits. Isso é possível ? Justifique.

Questão 6

a) Considere o protocolo TLS, como uma pilha que engloba quatro sub-protocolos: HANDSHAKE, ALERT, RECORD LAYER PROTOCOL E CHANGE-CIPHER-SUITE. Qual o papel de cada um desses sub-protocolos na normalização TLS (ou SSL) ?

b) No estudo dos modos de autenticação TLS no protocolo HANDSHAKE TLS este pode ser parametrizado para autenticação mútua, anónima ou unilateral (do cliente ou do servidor). Para além disso, podem usar-se também diferentes modos de estabelecimento de chaves (o que está relacionado com as *ciphersuites* adoptadas pelo cliente e pelo servidor nas diferentes versões do protocolo), entre os quais se destacam:

RSA
FDH (ou Fixed DIffie Hellman)
EDH (ou Ephemeral Diffie Hellman)
ADH (ou Anonymous DIffie Hellman)

Qual a diferença entre FDH e EDH ?

c) O protocolo TLS assegura sempre condições de segurança futura perfeita no estabelecimento de chaves de sessão, no contexto da conclusão com sucesso do handshake ? Justifique.

d) Considerando que está a usar TLS com estabelecimento de chaves do tipo EDH, com base em autenticação mútua cliente/servidor, tendo estes certificados válidos de chaves públicas RSA com chaves de 2048 bits. Em que circunstâncias consideraria que o estabelecimento com base em EDH pode torna-se fraco ou mais susceptível a vulnerabilidades que podem colocar em causa o estabelecimento da chave de sessão ? Justifique.

Questão 7

Considere o protocolo Kerberos V5 (representado em anexo).

a) É sempre necessário que o servidor AS possua chaves secretas simétricas partilhadas com o TGS no mesmo domínio (ou realm)? Justifique
b) É necessário que o AS possua chaves secretas simétricas partilhadas com um TGS de outro domínio (ou realm) ? Justifique.
c) Qual o interesse da última mensagens e nomeadamente a mensagem 6 e qual a importância do seu conteúdo nas condições de segurança estabelecidas pelo protocolo ?

Questão 8

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*
- um *hash* PH da 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 para permitir que programas não privilegiados possam obter informação presente no ficheiro /etc/passwd. Isto permite a um utilizador do sistema saber facilmente a password dos outros utilizadores? Justifique.

c) Suponha que um atacante com conta no sistema e acesso ao ficheiro */etc/passwd* tem uma lista de passwords usadas com frequência. Diga como é que esse atacante poderia conduzir um ataque para descobrir a password de um utilizador que se suspeita usar um password que consta na lista.

d) Sem alterar o conteúdo do ficheiro */etc/password* diga como poderia dificultar o ataque descrito em c).

e) Suponha que é realizado um ataque nas condições descritas em c) a um sistema com centenas de utilizadores. O ataque utiliza uma tabela pré-calculada de valores de PH para passwords comuns. Como é que poderiam ser adivinhadas as passwords de alguns utilizadores?

f) Suponha agora que se acrescenta a cada entrada um valor de 16 bits (*salt*) que é gerado aleatoriamente quando o utilizador é criado. Esse valor é guardado em claro no ficheiro */etc/passwd*. Esta técnica aumenta a dificuldade do ataque referido em c)? Justifique.

g) Explique como é que o uso do *salt* dificulta o ataque descrito em e).

Questão 9

O cumprimento do **princípio dos mínimos privilégios** impõe que as entidades activas existentes num sistema computacional (por exemplo, utilizadores / processos) apenas tenham, num dado momento, acesso à informação ou recursos que são necessários para os seus legítimos objetivos nesse momento. Nas alíneas seguintes discute-se se este princípio é seguido em várias situações num sistema operativo multi-utilizador como o Linux.

a) O CPU tem de ter dois modos de utilização (utilizador /sistema). Explique porque é que o CPU tem dois modos e diga, justificando, se é válido o princípio dos mínimos privilégios.

b) O acesso pelos processos aos ficheiros no UNIX utiliza um modelo classificado como Discretionary Access Control (DAC). Diga como funciona o controlo de acesso aos ficheiros pelos processos.

c) O funcionamento que descreveu em b) respeita o princípio dos mínimos privilégios? Justifique a sua resposta.

d) Como é sabido, existe nos sistemas UNIX um utilizador com nome *root*; processos associados a este utilizador têm todos os privilégios; processos pertencentes a outros utilizadores têm muito menos privilégios. Diga quais são os perigos associados a esta situação e diga, justificadamente se o princípio dos mínimos privilégios é aplicado.