DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores
2º Semestre, 2018/2019
Teste de frequência nº1, 2ª Chamada (9/Maio2019)

Copie corretamente para a sua folha de resposta o código de referencia indicado:

SSRC-1819-T1-R001-119R

Parte I - Resposta sem usar elementos de consulta

Questão 1

a) Apresente definições que caracterizem e permitam diferenciar com clareza as seguintes propriedades de segurança, apresentando em cada caso um exemplo concreto que identifique cada uma das propriedades

- Confidencialidade orientada à conexão (*connection confidentiality*)
- Confidencialidade não orientada à conexão (*connectionless confidentiality*)

b) Apresente definições que caracterizem e permitam diferenciar com clareza as seguintes propriedades de segurança, apresentando em cada caso um exemplo concreto que identifique cada uma das propriedades

- Confidencialidade de trafego (*traffic-flow confidentiality)*

c) De acordo com os requisitos enunciados para o trabalho prático nº 1 (considerando apenas os requisitos tal como endereçados na fase 1), discuta se os mecanismos de segurança providenciados garantem confidencialidade de tráfego ou autenticidade de principais (*peer-authentication*).

Questão 2

Considere que uma mensagem M trocada entre dois principais (correspondendo ao envio de A para B), é protegida com as seguintes construções criptográficas nos componentes Ci apresentados.

$IV \,||\, E_K(M \,||\, Nonce_A \,||\, HMAC\text{-}SHA\text{-}384_K (M)) \,||\, SHA\text{-}512 (C4)$

C1 C2 C 3 C5

C4

Sabendo que:

- IV : é um vetor de inicialização;
- E_K (...) : resultado de uma cifra simétrica AES, sendo este usado em modo GCM, com uma chave K de 256 bits e *padding* PKCS#5. (Notar que este algoritmo processa blocos de 128 bits).
- $Nonce_A$: é um *nonce* gerado pelo emissor A, de 128 bits, a partir de uma função baseada num algoritmo de geração pseudo-aleatória e que será memorizado pelo receptor.
- SHA-512: é a função de síntese de segurança SHA-512.
- $HMAC\text{-}SHA\text{-}384_K$: resultado da computação HMAC com síntese SHA-384 utilizando K como a chave Kmac, ou seja a mesma chave usada na cifra AES
- SHA-512: função de síntese de segurança SHA-512
- V : Corresponde à concatenação dos componentes *C1, C2, C3*

a) Poderá o componente C4 ser usado de forma a que o destinatário possa mitigar ataques DoS por simples modificação (*tampering*) da mensagem por parte de um atacante no canal que apenas pretende levar o destinatário a computações criptográficas para fazer a detecção do ataque de *tampering*? Justifique.

b) A partir dos dados, qual o tamanho que deve ter o componente C1 ? Justifique.

c) Se a mensagem M tiver 1 KByte (1024 bits) qual será o tamanho do componente *ciphertext* C4 ? Justifique.

d) Se a mensagem M tiver 824 bits, qual será o tamanho global da mensagem (ou seja a concatenação de C1, C4 e C5) ? Justifique.

e) Dados os componentes do processamento criptográfico, que componentes seriam dispensáveis de modo a diminuir o tamanho da mensagem total a transmitir, garantindo no entanto as mesmas propriedades de segurança da especificação indicada ? Justifique.

f) O IV está a ser passado em claro. Isso constitui uma fraqueza que coloca em perigo a proteção de confidencialidade? Argumente.

Questão 3

Considere o protocolo de autenticação e distribuição de chaves para A e B de acordo com o modelo de *Neuman-Stubblebine*), com base num KDC (*Key Distribution Center*) e apenas com utilização de criptografia simétrica.

Após o estabelecimento da chave K_{AB} e em subsequentes comunicações, A e B pretendem autenticar-se futuramente (em próximas interações), enquanto a chave K_{AB} for considerada válida por B, num intervalo temporal contado por B a partir do *timestamp* T_B. Nesse caso, nas próximas interações, A e B autenticar-se-ão do seguinte modo num protocolo em 3 rondas, envolvendo novos *nonces* $N_{A'}$ e $N_{B'}$ gerados por A e B respetivamente:

Ronda 1: A -> B : _____

Ronda 2: B -> A : $N_{B'} \,||\, E(K_{AB}, N_{A'})$

Ronda 3: A-> B : $E(K_{AB}, N_{A'})$

Nota: $E(K_{AB}, X)$ representa X cifrado com a chave K_{AB}

a) Como deverá ser a mensagem da ronda 1 para o propósito enunciado ?
b) Discuta se o protocolo (quer o inicial quer o protocolo de autenticação das interações posteriores) garantem segurança futura e passada perfeita. Justifique.

Questão 4

Considere o protocolo Kerberos V5

a) Para que serve ou qual o propósito da chave *SubKey* na mensagem da ronda 6 ? Que vantagem vê nesse propósito ?
b) Para que serve ou qual o propósito do *Seq#* na mensagem da ronda 6 ? Que vantagem vê nesse propósito ?
c) Nas mensagens das rondas 1 a 5, são usados *timestamps* e *nonces*. Que vantagem vê na utilização dos *nonces* para além dos *timestamps* que também permitiriam controlar a frescura das mensagens no controlo *anti-replaying* ? Argumente.

Protocolo de distribuição de chaves (modelo Neuman-Stubblebine)

- S: é o KDC; A e B são os identificadores dos principais envolvidos que querem estabelecer uma chave
- S_i é um identificador de sessão
- K_{as} é uma chave criptográfica anteriormente partilhada entre A e S
- K_{bs} é uma chave criptográfica anteriormente partilhada entre B e S
- N_a e N_b são *nonces* (gerados aleatoriamente por A e B respetivamente)
- T_a e T_b são *timestamps* calculados a partir dos relógios de A e B respetivamente
- K_{AB} é a chave de sessão que será distribuída.

O protocolo desenvolve-se em 3 rondas de mensagens envolvendo A, B e S:

$$A \rightarrow B : A, N_A$$

Alice notified Bob of intent to initiate secure communication.

$$B \rightarrow S : B, N_B, \{A, N_A, T_B\}_{K_{BS}}$$

Bob generates a times stamp and a nonce, and sends this to the trusted Server.

$$S \rightarrow A : \{B, N_A, K_{AB}, T_B\}_{K_{AS}}, \{A, K_{AB}, T_B\}_{K_{BS}}, N_B$$

The trusted Server generates a session key and a message for Alice to forward to Bob.

$$A \rightarrow B : \{A, K_{AB}, T_B\}_{K_{BS}}, \{N_B\}_{K_{AB}}$$

Protocolo Kerberos V5:

(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 $\mathrm{E}_{Kc,v}[\, TS_2 \| Subkey \| Seq\# \,]$

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

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

Parte II – Para as respostas podem ser usados elementos impressos e individuais de consulta

Questão 5

Testou-se um programa para testar a diferença entre usar o algoritmo DES e Triple DES. O programa testou o tempo de realizar 1000 cifras de um bloco de 1K bits (ou 1024 bits), usando as seguintes *ciphersuites*:

C1: DES/CTR/NoPadding, Chave de 56 bits
C2: DESede/CTR/NoPadding, Chave de 168 bits

Os resultados médios obtidos com 100 observações foram:

C1: 433 nanosegundos por cada bloco de 64 bits
C2: 1,196 milisegundos por cada bloco de 64 bits (~2,76 x C1)

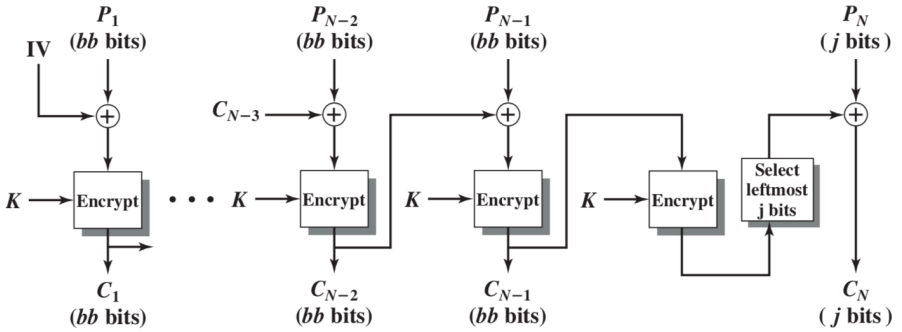
a) Explique o diferencial de tempos e argumente sobre se considera justificáveis os resultados indicados.
b) O que esperaria se o teste fosse feito para uma ciphersuite DESede/ECB/NoPadding, Chave de 112 bits ? Justifique

Questão 6

A seguinte figura apresenta o esquema da estrutura e computação de um HMAC, tendo por base uma estrutura normalizada pelo RFC 2104. Apresente as razões que identifica para as vantagens da estrutura dessa construção HMAC. Tente enumerar 5 boas razões que vê como vantagens do esquema apresentado, face à utilização de construções que usam apenas uma função de síntese.

Questão 7

a) Vai usar-se um algoritmo criptográfico simétrico (exemplo, AES) que processa blocos de tamanho B (no caso do AES são blocos de 128 bits) e com padding (ex., PKCS#5), sendo a cifra feita em modo ECB. Em que condições o perigo de detecção de padrões de bits no *ciphertext* correspondentes a padrões de bits no *plaintext* pelo uso do modo ECB não existe ? Justifique.
b) Considere o seguinte modo que pode ser usado para utilização com algoritmos de cifras de bloco. Uma vez que do ponto de vista de segurança este modo garante u nível de segurança similar à do modo CBC, que vantagem principal vê na sua utilização ?



c) Comparativamente a usar CTR apresente as vantagens ou desvantagens que encontra na utilização do modo anterior ?

Questão 8

a) No sistema Kerberos (V5), supondo que o servidor TGS de um domínio de autenticação A (*realm A*) partilha chaves com um servidor TGS de um domínio B (*realm B*) e o TGS do domínio B (*realm B*) partilha chaves com um servidor TGS do domínio C (*realm C*), seria possível a um utilizador do domínio A (*realm A*) utilizar um recurso (servidor final) no domínio C (*realm C*) ? Como e porquê ?

b) Se nas rondas de mensagens do protocolo Kerberos V5 não for completada a última mensagem trocada entre o servidor final e o cliente, que garantia de segurança se perderia ? Justifique.

c) Argumente sobre se o protocolo Kerberos (versão 5) garante ou não segurança futura ou passada perfeita (PFS – *Perfect Futrure Secrecy* ou PBS – *Perfect Bacward Secrecy*).

Questão 9

No contexto desta questão tenha em mente os pressupostos de cálculo temporal para quebra de chaves criptográficas, na discussão da robustez dos algoritmos simétricos dadas as dimensões das chaves. A ideia é aplicar o mesmo tipo de ataque para quebrar passwords, dadas as regras de escolha de passwords.

Suponhamos que as passwords num sistema como o clip eram atribuídas através de um processo de geração de 8 caracteres irrepetíveis, obtidos por combinações de:

26 carateres (alfabeto para língua inglesa);
10 números, de 0 a 9
10 sinais de pontuação no conjunto { ? % & ? + - , ; . : }

Suponha que um atacante tentará atacar essas passwords dado que pode inferir os *usernames* (na forma como são usados no sistema clip). Para o efeito, o atacante vai usar um processo de força bruta, tendo capacidade para testar uma *password* por segundo. Note que no sistema CLIP, apenas quando se acaba de introduzir totalmente a informação "username" e "passwords" o sistema dará feedback ao utilizador com informação de sucesso ou insucesso da operação de autenticação e que o atacante poderia usar um número ilimitado de tentativas (já que o sistema nunca bloquearia acessos a uma conta de utilizador com mais do que X tentativas falhadas).

a) Sabendo que o número de combinações independentes de K carateres sem repetições num conjunto de N é dada por N^K, calcule **o tempo médio** (probabilidade =0,5) de uma password assim gerada poder ser quebrada ? Indique a expressão do seu cálculo e o resultado do mesmo.
b) Repita a) mas considerando que a combinação de caracteres na geração não pode repetir caracteres. Note que o número de quaisquer combinações simples de K caracteres de um conjunto de N, pode ser dado pela fórmula:
   n ! / (n-k) !
   Justifique o seu cálculo.
c) Calcule o mesmo **tempo médio**, nas condições de b) para PINs de 4 caracteres numéricos que podem ser repetíveis (como é o caso de emparelhamentos de dispositivos Bluetooth) nas mesmas condições do poder do atacante
d) Num dado sistema de banca electrónica de uma instituição bancária conhecida os utilizadores autenticam-se por um teclado virtual, usando *usernames* (designados por números de contrato) de 6 dígitos numéricos e *passwords* usadas como códigos numéricos de acesso 6 dígitos numéricos. Sabe-se que a probabilidade de se acertar num nº de contrato à primeira tentativa, será neste caso $6{,}61376 \times 10^{-6}$. Considerando não ser possível obter a password por um ataque de "*phishing*" e não conhecendo nenhum número válido de contrato de um utilizador e muito menos o respetivo código de acesso, calcule o **tempo médio** que demoraria um atacante de força bruta com uma capacidade de testar automaticamente 1000 combinações de números de contratos e todos os códigos de acesso em cada segundo, para acertar numa combinação válida de número de contrato e código de acesso, fazendo assim um "login" ilícito.