DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores
2º Semestre, 2018/2019
Teste de frequência nº 1 (13/Abril/2019)

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

T1-A001-119C

Parte I - Resposta sem usar elementos de consulta

Questão 1

Num protocolo de comunicação seguro baseado em transporte UDP, as mensagens trocadas entre dois *endpoints* (endereço IP, porto nos *hosts* H1 e H2), são trocados protegidos da seguinte forma, sendo os componentes da mensagem identificados com as letras indicadas.

IV || Blowfish_K(M || SeqNr || $\text{HMAC-SHA-224}_\kappa$ (M)) || HMAC-SHA1_{Kmac} (V)

A	B	C	D

E

Deste modo, as cargas dos datagramas enviados entre os dois *endpoints* correspondem à concatenação dos componentes A, E, D enviados em cada caso pelo respetivo emissor, com E correspondendo à operação indicada e que envolve B e C.

No formato do processamento indicado:

- IV : é um vetor de inicialização (passado em Plaintext) de tamanho 64 bits
- Blowfish_κ : é o algoritmo criptográfico Blowfish, sendo este usado em modo CBC, com uma chave K de 448 bits e padding PKCS#5 da mensagem.
- SeqNr : é um número de sequência (inteiro de 32 bits), iterado em cada mensagem trocada, a partir de um número de sequência inicial gerado como número aleatório na primeira mensagem trocada entre o Host H1 e o Host H2.
- SHA-224: é a função de síntese de segurança SHA-224.
- HMAC-SHA1_K: resultado da computação HMAC com síntese SHA-1 (síntese de 160 bits), utilizando a chave Kmac.
- V : Corresponde à concatenação dos componentes *A, B e C*

a) De entre os componentes ***A, B, C, D*** *ou* ***E***, quais garantem PEER-AUTENTICATHION, MESSAGE-AUTHENTICATION, MESSAGE-INTEGRITY, MESSAGE-CONFIDENTIALITY, Proteção contra MESSAGE-REPLAYING e mitigação de DENIAL-OF-SERVICE ?

b) Se em vez de se usar o modo CBC se utilizassem os modo CCM ou GCM, qual dos componentes ***A, B, C*** , ***D*** seriam desnecessários ? Justifique.

c) Se em vez do componente ***D*** utilizasse apenas uma síntese SHA-1 em vez de HMAC–SHA1, o resultado seria o mesmo para efeitos das propriedades de segurança? Justifique.

d) Se numa determinada mensagem a representação de M corresponde a 64 bits, qual vai ser a dimensão em bits do componente ***E*** ? Justifique.

Questão 2

O protocolo seguinte (conhecido como protocolo Yahalom) concretiza em síntese um protocolo de autenticação e estabelecimento de uma chaves criptográfica simétrica (Ks) para comunicação segura entre Alice (A) e Bob (B), com auxílio de um Centro de Distribuição de Chaves, representado por S. O protocolo segue as premissas e notações utilizadas no estudo de diferentes protocolos de autenticação e distribuição de chaves simétricas com base em KDCs (*Key Distribution Centers*), usados como entidade confiável para A e B.

a) Complete as partes em falta na representação das quatro rondas de troca de mensagens do protocolo, para que este funcione corretamente com segurança e termine com a distribuição segura da chave.

A > B: A || Na

B > S: B || $\{ A, Na, Nb \}_{KBS}$

S > A: $\{ B, Ks, Na+1, Nb+1 \}_{KAS}$ || _____

A > B: $\{ A, Ks \}_{KBS}$ || _____

b) Este protocolo usado em processos de rekeying entre A e B para geração sucessiva de futuras chaves de sessão (com validade pré-determinada entre A e B) garante segurança futura ou passada perfeita (PFS – *Perfect Forward Secrecy* ou PBS – *Perfect Backward Secrecy*) ? Justifique.

Questão 3

O processamento para cifrar um bloco de texto em claro (*plainetext*), utilizando o algoritmo AES e adoptando o modo OFB, pode representar-se da seguinte forma:

$C_1 = P_1 \text{ XOR } S_S [E_{AES\text{-}256} (K, IV)]$

Em que: C_1 é o primeiro bloco *ciphertext*; P_1 é o primeiro bloco *plaintext*; IV é um vetor de inicialização e E_{AES} ( ) representa uma operação de AES (*encrypt*) com uma chave de 256 bits.

a) Escreva a expressão equivalente para calcular P_1 a partir de C_1 .
b) Escreva a expressão equivalente para calcular P_i a partir de C_i .
c) Em que consiste o processamento da função S_S e para que serve ?

Questão 4

a) Porque é que o protocolo Kerberos nas versões V4 e V5 estudadas pode ser atacado por um ataque de dicionário às passwords dos utilizadores que atuam como clientes perante os servidores de autenticação Kerberos (*Authentication Servers*) ? Justifique.
b) Se num mesmo reino (domínio de autenticação ou *realm* Kerberos V5) um cliente vai precisas de comunicar com diversos servidores, pode cada um destes servidores partilhar chaves com diferentes servidores TGS (*Ticket Granting Servers*) do mesmo domínio ? Porquê ?

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

Questão 5

Considere os seguintes princípios fundamentais de concepção de propriedades de segurança, tal como foram estudados: A) Economia do mecanismo (ou *Economy of Mechanism*) ; B) *Fail-safe defaults*, C) Mediação completa (*Complete mediation*), D) concepção aberta (*Open Design*), E) Separação de privilégios (*Privilege Separation*), F) Menor privilégio (*Least privilege*), G) Menor mecanismo comum (ou *Least common mechanism*), H) Aceitação psicológica (*Psycological Acceptability*), I) Isolamento (*Isolation*), J) Encapsulamento (*Encapsulation*), K) Modularidade (*Modularity)*, L) Proteção sobreposta (ou *Layering*) e M) menor surpresa (ou *Least astonishment*)

a) Num sistema de autenticação que combina o uso de passwords e um código (ou *token*) obtido por uma mensagem SMS ou obtido por uma aplicação que o calcula numa App num telemóvel), como sistema de autenticação multi-fator, como se pode usar, por exemplo, para acesso a contas Google Mail, a qual dos anteriores princípios corresponde essa proteção de segurança? Porquê ?

b) Quando um utilizador vai usar o seu computador para utilizar um browser de acesso à Internet para aceso ao sistema CLIP e para o efeito utiliza uma conta de Administrador de Sistema, que princípio de segurança estará a violar ? Porquê ?

Questão 6

Alice envia a Bob mensagens M cifradas (com base no algoritmo AES e modo CBC) com proteção de provas de autenticidade e integridade usando uma construção HMAC (implementando o standard RFC 2104) ou usando uma construção CMAC baseada no algoritmo AES.

Para o efeito está a pensar usar uma das seguintes variantes:

V1: $\{ M \}_{K1} \mid\mid HMAC_{K1} (\{ M \}_{K1})$

V2: $\{ M \mid\mid HMAC_{K1} (M) \}_{K1}$

V3: $\{ M \}_{K1} \mid\mid HMAC_{K2} (\{ M \}_{K1})$ em que a chave K1 é diferente de K2

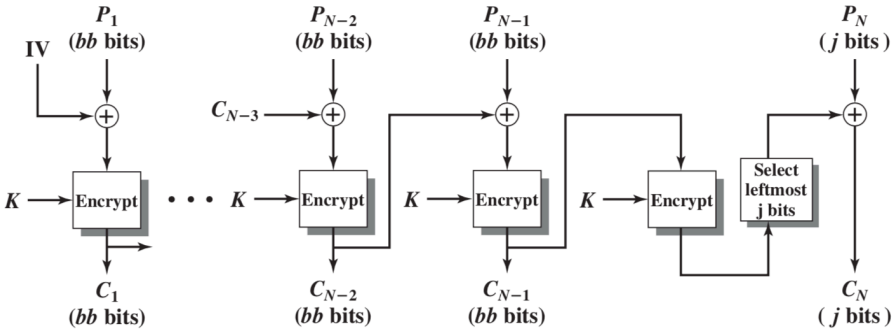
V4: $\{ M \}_{K1} \mid\mid CMAC_{K2} (\{ M \}_{K1})$ em que a chave K1 é diferente de K2

V5: $\{ M \mid\mid CMAC_{K1} (M) \}_{K1}$

Alice e Bob estão interessados em que a variante usada seja a que melhor endereça o *tradeoff* entre segurança, eficiência e mitigação da possibilidade de haverem ataques de DoS no canal. Alice e Bob pedem a sua opinião para a ajudar na escolha. Que variante proporia ? Justifique.

Questão 7

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 ?



Questão 8

a) Comparativamente ao uso de um único serviço KDC num protocolo de autenticação e distribuição de chaves, como é por exemplo o caso do protocolo de Needham-Schroeder para utilização com criptografia simétrica, que vantagens encontra em desdobrar esse papel nas entidades AS e TGS no caso de um protocolo como o Kerberos V4 ? (Note que nesta versão não possui ainda a noção de reinos ou domínios Kerberos).

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 perde ? Justifique.

c) Porque é que no protocolo Kerberos V5 não há o perigo de haver ataques do tipo replaying após uma chave ter sido estabelecida, mesmo que a validade de todos os tickets obtidos nas rondas das mensagens de 1 a 5 ainda se encontrem válidos

d) 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*).

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

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

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

(c) Client/Server Authentication Exchange to obtain service

Questão 9

O protocolo WEP (*Wired Equivalent Privacy*) era bastante utilizado (e por vezes ainda é) como protocolo de autenticação de computadores (clientes ou STA – *Station*) perante *Access-Points* (APs) para acesso a redes locais sem fios (WLANs). O Protocolo WEP assume que os clientes (STA) e os Access Points utilizáveis (APs) devem partilhar uma chave secreta, que de acordo com a definição é um segredo inicial estaticamente parametrizado (WEP Key) que pode ter uma representação de 10 carateres representados em hexadecimal (ou 40 bits), ou 26 carateres representados em hexadecimal (ou 104 bits), utilizado como material semente para geração de uma chave RC4 (Km) de 64 ou 128 bits (num e noutro caso), contendo como prefixo um vetor de inicialização de 24 bits.

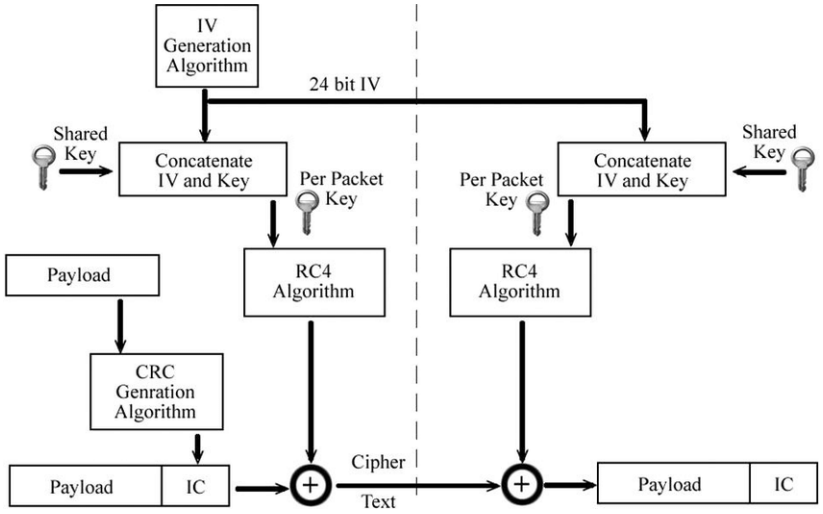
Quando um cliente quer ter acesso ao *Access Point*, desencadeia-se **o protocolo de autenticação** na seguinte forma:

STA > AS:	Request, <MAC Address>	// Request Authentication Message
AS > STA:	Nonce	// Random Challenge, com 128 bytes
STA > AS:	$\{\mathrm{Nonce}\}_{\mathrm{Km}}$	

// Nesta fase o AP decifra a mensagem para perceber de o desafio foi bem respondido)

STA > AS: Confirma o acesso (mensagem de sucesso cifrada com a chave Km)

Depois, **a comunicação segura** prossegue de acordo com a seguinte figura que ilustra o envio (*stream cipher*) dos dados entre o emissor (STA) e receptor (AS)



EMISSOR RECEPTOR

a) Apresente uma vantagem do protocolo de autenticação

b) Apresente uma fraqueza ou vulnerabilidade na confidencialidade da comunicação que possa ser explorada por um atacantes e que possa permitir quebrar a chave de cifra RC4 utilizada.

Sugestão para o seu raciocínio: usando um vetor de inicialização de 24 bits (como é o caso), há uma probabilidade de 50% de um mesmo vetor estar repetido após cerca de 5000 *frames* cifradas que tenham sido enviadas.