DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores - 1º Semestre, 2019/2020
Teste de frequência nº 1 (8/Novembro2019)

T1A00120C

Parte I - Respostas sem utilização de elementos de consulta

Questão 1

Num protocolo de comunicação que suporta um sistema de *messaging* baseado em transporte UDP, as mensagens M enviadas por um principal ***A*** num dispositivo H1 (IPa, PORTOa) a outro principal é enviada da seguinte forma, sendo os componentes da mensagem identificados com as letras indicadas e de acordo com a legenda seguinte.

Posteriormente, cada mensagem recebida de ***A*** por qualquer outro principal possui uma estrutura semelhante.

$$\underbrace{RSA_{KpubB}(K||IV)}_{A}||\underbrace{AES_K(M||SN||Nonce_A||Nonce_B||SHA_{512}(M))}_{B}||\underbrace{SIG_{KprivA}(E)}_{C}||\underbrace{HMAC_{Kmac}(F||IPa||Pa)}_{D}$$

E

F

Legenda:

||	Representa concatenação dos elementos criptográficos
Componente A	É um envelope de chave pública para distribuição da chave K (AES de 128 bits) e vetor de inicialização IV. A chave pública tem 2048 bits e usa-se *padding* OAEP.
IV	É um vetor de inicialização de 128 bits
IPa, Pa	IPa: Endereço IP; Pa: Porto, correspondendo ao endpoint <IP, Port> de onde a mensagem foi enviada
Componente B	Cifra AES do conteúdo indicado com chave K de 256 bits, em modo CBC e com *padding PKCS#5*, sendo usado na cifra o vetor de inicialização IV do componente A
SN :	Número de sequência (*long integer* de 128 bits), iterado em cada mensagem trocada a partir de um valor inicial igual ao valor inteiro do componente D da primeira mensagem enviada. Em cada nova mensagem o número de sequência é incrementado de um
NonceA	É um valor inteiro de 128 bits gerado pseudo-aleatoriamente pelo emissor
NonceB	Valor inteiro de 128 bits. Em cada mensagem trocada é o valor do último valor $Nonce_A$ recebido de uma dada origem, incrementado de 1. No início o valor $Nonce_B$ é enviado com o valor 0.
$SHA_{512}(X)$	É a síntese (*hash*) de segurança SHA 512 (família SHA-3) do conteúdo X
$HMAC_{Kmac}$	Constitui o componente D, sendo o resultado da computação HMAC com síntese SHA-256 (utilizando a chave Kmac que corresponde por sua vez a uma síntese SHA-256 do valor IV no envelope do componente A.
Componente C:	É uma assinatura digital do conteúdo do componente E, usando-se DSA, chave privada KprivA de 2048 bits e função de síntese SHA-256
Componente E	Corresponde à concatenação dos componentes A e B
Componente F	Corresponde à concatenação dos componentes E e C

Depois de analisar o protocolo responda às seguintes alíneas de a) a p). Considere apenas possíveis ataques às comunicações com base na tipologia da *framework* X.800. Os principais que trocam mensagens usam o formato indicado e executam corretamente o processamento de envio e verificação na recepção, atuando corretamente.

a) Qual o componente que garante PEER-AUTHENTCIATION do emissor?

b) O protocolo tem garantias de *peer-authentication* do endpoint <IP, porto> de onde está a ser enviada ?

c) Qual o componente que garante MESSAGE-INTEGRITY ?

d) De que tipologia é a proteção MESSAGE-INTEGRITY indicada em c) ?

e) Qual o componente ou componentes que garantem MESSAGE-CONFIDENTIALITY ?

f) De que tipo é a proteção de MESSAGE-CONFIDENTIALITY indicada em e) ?

g) Que componente ou componentes garante(m) DATA-ORIGIN AUTHENTICATION ?

h) A proteção estabelecida pelo protocolo garante TRAFFIC-FLOW-CONFIDENTIALITY ? Justifique.

i) A proteção estabelecida pelo protocolo garante NON-REPUDIATION ? Argumente.

j) No desenho do protocolo, o componente D tem como propósito minorar ataques de negação de serviço que tenham por alvo exaurir o processamento do receptor. Isso é bem conseguido ? Como poderia ser melhorado?

k) Que tamanho em bits terá o componente A ?

l) Se a mensagem M a proteger no protocolo tiver tamanho 1024 bits, qual será o tamanho do componente B?

m) Se a mensagem M a proteger no protocolo tiver tamanho 1124 bits, qual será o tamanho do componente B?

n) Qual vai ser o tamanho do componente D?

o) O processamento do componente C poderá ser possível mesmo que a mensagem M a proteger for muito grande (ex., maior do que 2048 bits) ?

p) Para processarem as mensagens do protocolo, qual é a o *setup* mínimo (inicializações ou parâmetros mínimos de associações de segurança necessários) que os principais já deverão ter ?

Questão 2

a) Em que situação considera vantajoso o uso de modos como GCM ou CCM em vez do modo CBC ? Justifique.

b) Se no protocolo indicado da questão 1 (componente B) usar GCM, haveria algum processamento redundante que já não acrescentaria segurança ? Qual e porquê ?

c) Usando um algoritmo simétrico em modo CFB, uma chave K, um vetor de inicialização IV, os blocos *ciphertext* C_1 e C_i são obtidos em geral dos correspondente blocos *plaintext* P_1 e P_i do seguinte modo:

$$C_1 = P_1 \text{ xor } Ss\,(E_K(IV)); \quad C_i = P_i \text{ xor } Ss\,(E_K(Ci\text{-}1))$$

c1) Indique a expressão que recupera P_1 e P_i decifrando C_1 e C_i

c2) Para que serve a função Ss nas expressões indicadas ?

Questão 3

a) Na construção de um envelope de chave pública, qual o propósito de segurança de usar *Padding* normalizado?

b) No protocolo da questão 1 (componente A) que vantagem ou desvantagem há em usar *padding* OAEP em vez de PKCS#1 ?

c) No protocolo da questão 1 (componente C) não se utiliza padding. Isso fragiliza a assinatura?

Questão 4

Usando-se SHA-512 para proteção de integridade (como é o caso no componente B do protocolo da questão 1) e admitindo que esta função não possui vulnerabilidades de criptanálise conhecidas:

a) Qual a probabilidade de se quebrar a propriedade conhecida como *SECOND-IMAGE RESISTANCE* (ou *Weak-Collision Resistance*) ? Indicar o resultado com uma expressão para calcular a probabilidade.

b) Qual probabilidade de se quebrar a propriedade conhecida como *STRONG-COLLISION-RESISTANCE* ? Indicar o resultado com uma expressão para calcular a probabilidade.

Questão 5

Dois principais vão usar o método de acordo de Diffie-Hellman para negociarem um segredo partilhado, com garantias de resistirem a um ataque "homem-no-meio" capaz de interceptar e gerar mensagens no canal. Para o efeito:

a) Para poderem fazer o acordo em segurança, devem enviar os respetivos números públicos gerados cifrados num envelope de chave pública, cifrando com um algoritmo criptográfico assimétrico (por exemplo, RSA) e usando a chave pública do destinatário. VERDADEIRO OU FALSO ? Justifique.

b) Para fazerem o acordo em segurança e com mais rapidez (ou menor latência), poderão usar parâmetros iniciais para a raiz primitiva e número primo P a usar no acordo, podendo estes valores serem conhecidos pelo atacante. VERDADEIRO OU FALSO ? Justifique.

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

Questão 6

Considere os seguintes princípios fundamentais de concepção de sistemas seguros estudados: P1) Economia do mecanismo (ou *Economy of Mechanism*) ; P2) *Fail-safe defaults*, P3) Mediação completa (*Complete mediation*), P4) concepção aberta (*Open Design*), P5) Separação de privilégios (*Privilege Separation*), P6) Menor privilégio (*Least privilege*), P7) Menor mecanismo comum (ou *Least common mechanism*), P8) Aceitação psicológica (*Psycological Acceptability*), P9) Isolamento (*Isolation*), P10) Encapsulamento (*Encapsulation*), P11) Modularidade (*Modularity)*, P12) Proteção sobreposta (ou *Layering*) e P13) menor surpresa (ou *Least astonishment*).

Responda às seguintes alíneas de **a)** a **h)** colocando ***X*** nas células da tabela. Deve focar a resposta com um único ***X*** por cada linha da tabela.

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
a)													
b)													
c)													
d)													
e)													
f)													
g)													
h)													

a) Que princípio de segurança se pretende endereçar quando se usa módulo de hardware criptográfico (ex., HSM – *Hardware Security Module*) ?

b) Qual o princípio de segurança endereçado por esquemas do tipo ONION-ENCRYPTION como reforço de segurança de algoritmos criptográficos simétricos

c) Que principio de segurança está a ser violado por um utilizador que usa sempre a mesma password para uso num sistema empresarial crítico, nas redes sociais e na sua conta de Email da Google (Gmail) ?

d) Se protegermos aplicações com base em tecnologias como ARM-TRUST-ZONE ou Intel SGX) para minimizar e delimitar por essa via a base de confiança do sistema, qual o princípio de segurança que estamos a atendar

e) Uma aplicação foi concebida de forma que os seus componentes estão estruturados em micro-serviços (ou componentes) que estão implementados em contentores *docker* (ou *docker containers*) estando estes assinados digitalmente para poderem ser verificados antes de serem executados. Que princípio de segurança endereça essa técnica ?

f) No sistema CLIP o lançamento de notas é uma operação que pode ser feita pelos utilizadores com papel de docente da FCT, não podendo essa operação ser feita por utilizadores com papel de aluno ou funcionário da FCT.

g) Um utilizador comprou um dispositivo IoT na loja que é uma fechadura electrónica (ou *smart locker*) que pode ser usada para proteger uma porta. O acesso ao dispositivo faz-se através de uma App Android ou IoS. Para abrir ou fechar a fechadura utiliza-se uma password de 8 carateres alfanuméricos, usada para computar um esquema do tipo *Password-Based Encryption* baseado no algoritmo DES, com *counter*=0 e *salt*=H(pwd). Do lado do dispositivo, a password está suportada em Hardware, não podendo ser modificada. Que princípio de segurança está aqui posto em causa ?

h) Após uma operação de LOGIN com autenticação baseada numa password numérica de 6 dígitos, um utilizador de um sistema de Banca Electrónica (ou *Internet Banking*) o utilizador pode efetuar um certo número de operações disponíveis, sendo uma delas a possibilidade de movimentar diariamente montantes limitados até 500 € em transferência interbancárias. Se no entanto pretender movimentar mais de 500 €, o utilizador deverá autenticar-se com uma password suplementar, baseada num código alfanumérico de 8 carateres alfanuméricos, que receberá no seu telemóvel através de uma mensagem SMS, sendo esse código válido num dado período de tempo, para essa operação

Questão 7

Na seguinte tabela quadro (que se encontra na folha de respostas) caracteriza a utilização de métodos criptográficos assimétricos e diferentes construções criptográficas para os diversos fins a que se destinam. Complete o quadro colocando SIM ou NÃO nas linhas que não estão preenchidas.

Objetivo: / Algoritmo / Construção e *Padding*	Confidencialidade, Envelopes confidenciais cifrados com chaves públicas	Autenticidade de principais, Assinaturas Digitais	Distribuição e estabelecimento anónimo de chaves de sessão e outros parâmetros secretos de associações de segurança	Distribuição e estabelecimento seguro e autenticado de chaves de sessão e outros parâmetros secretos de associações de segurança
Cifra RSA c/ *padding* PKCS#1	**Sim**	**Não**	**Sim**	**Não**
Cifra usando RSA com *padding* OAEP				
Assinatura RSA com SHA156 e *padding* PKCS#1				
Diffie-Hellman (DH)				

ECC				
DSA				
ECDH				
ECDSA	**Não**	**Sim**	**Não**	**Não**

Questão 8

Considere a especificação do protocolo de segurança SMCP (e respectivo formato de mensagens) referente à sua implementação do Trabalho Prático nº 1 (Fase 1).

`vId||sID||SMCPmsgType||SAttributes||SizeOfSecurePayload||SecurePayload||FastSecureMCheck`

`Componente SAttributes: SessionID||SessionName||SEA||Mode||Padding||H||MAC`

A partir do conhecimento que tem sobre o seu trabalho e o contexto da sua implementação do anterior protocolo (podendo também considerar eventuais diferenças que tenha considerado no caso da sua implementação específica), responda:

a) Considere que na parametrização MAC vai usar uma construção HMAC com síntese SHA-512 no componente *FastSecureMCheck* expresso em MAC (no componente *SAttributes*) e se vai usar SHA-1 para a função segura de síntese H (hash) expresso no componente *SAttributes* usado internamente no componente *SecurePayload*. Não obstante essa configuração poder ou não ser usada sem prejuízo da segurança, que vantagem ou inconveniente teria? Argumente.

b) Uma vez utilizando-se HMAC no componente *FastSecureMCheck* parecerá redundante voltar a usar-se outra construção MAC no componente *SAttributes* (em vez de uma única função de síntese expressa em H. Qual a vantagem de usar esses dois MACs ?

c) Preencha na tabela seguinte SIM ou NÃO sobre as proteções ou serviços de segurança garantidos, justificando sobre o suporte dos mesmos, tendo em conta as parametrizações (*setup*) pré-existente nos *endpoints* (aplicação MCHAT suportada) , considerando a implementação do seu trabalho (ou só fase 1, fase 2 ou integração de ambas).

Implementação REF: FASE 1 _____ FASE 2 : _____ AMBAS AS FASES INTEGRADAS: _____

Serviços de Segurança	Suporte : SIM ou NÃO	Mecanismo de segurança utilizado
Message Confidentiality Confidencialidade de mensagens		
Peer-Authentication (Autenticação de Principais)		
Message Authentication (Autenticação de Mensagens)		
Non Repudiation (Não Repudiação)		
Message Integrity (selective field integrity)		
Message Integrity w/ Recover		
Connection Oriented Integrity		
Connectionless Integrity		
Traffic Confidentiality (Confidencialidade de Tráfego)		
Ataques à ordenação de mensagens		
Anti-Message Replaying Service (Proteção contra retransmissão ilícita de mensagens)		

Questão 9

Analise o protocolo em anexo que vai ser executado por Alice e Bob para estabelecerem uma chave de sessão Ks AES com 256 bits, uma chave HMAC Kmac com 256 bits e um IV de 128 bits, para estabelecerem um canal seguro para usarem de seguida o protocolo da questão 8. O protocolo funciona em 3 rondas e utiliza o método de acordo de Diffie-Hellman, trocando mensagens no formato indicado. Pretende-se que o protocolo resista a adversários do tipo "homem-no-meio" atuando no canal de comunicação partilhado entre A e B, com capacidade de desencadearem ataques de acordo com tipologia de ataques prevista na *framework* X.800, incluindo retransmissão ilícita de mensagens ou ataques por reflexão.

Da sua análise do protocolo, responda às seguintes alíneas de a) a d).

a) Diga se acha o protocolo correto e resistente aos ataques considerados no modelo de adversário, assegurando as garantias necessárias de segurança. Justifique a resposta ou proponha correções se considerar algo errado.

b) Suponha que Alice e Bob pretendem renegociar periodicamente novos valores Ks, Kmac e IV, com garantia de segurança futura e passada perfeitas, reiniciando o protocolo. Porém, para poderem fazê-lo com segurança mas com mais rapidez (reduzindo a latência), irão sempre reutilizar os valores *P* e *G*. Que vantagens ou desvantagens tem isso ? Justifique**.**

c) Diga qual o tamanho (em bits) dos valores obtidos durante e após o acordo por Alice e Bob

De acordo com os dados no protocolo, o tamanho de YpubB será _____ bits

A assinatura na ronda 2 tem dimensão fixa ? Sim/Não: _____

Se na questão anterior considerar que a dimensão é fixa indique o nº de bits. Se não coloque X _____ bits

De acordo com os dados no protocolo, o tamanho de YpubA será _____ bits

A assinatura na ronda 3 tem dimensão fixa ? Sim/Não: _____

Se na questão anterior considerar que a dimensão é fixa indique o nº de bits. Se não coloque X _____ bits

O tamanho de Ks gerado por Alice e Bob será _____ bits

d) Suponha que no protocolo indicado se pretendia usar compressão para comprimir a dimensão das assinaturas nas rondas 2 e 3, de modo a que as mensagens transmitidas fossem mais pequenas. A compressão devia ser feita aos conteúdos das assinaturas antes de assinar ou depois de assinar ? Porquê ?

ANEXO: Protocolo da questão 9

Ronda 1 - Alice to Bob:

$Alice||Bob||RN1_A||G||P||CChain_A$

Alice e Bob: Identificadores de Alice e Bob respetivamente

$RN1_A$: *Random Nonce* de 128 bits, gerado e enviado por Alice

G: Raiz primitiva do número primo P, pré-calculada e proposta por Alice

P: Número primo, com representação inteira de 1024 bits

$CChain_A$ Cadeia de certificados X509v, contendo o certificado X509v3 de chave pública DSA de Alice (KpubA), sendo o certificado raiz de uma CA confiável por Bob, na validação direta da cadeia

Ronda 2 - Bob to Alice:

$Bob||Alice||H(G, P)||SIG_{KprivB}(Bob,Alice,RN1_A+1,RN1_B) || \{Bob,YpubB\}_{KpubA} ||CChain_B$

$RN1_A+1$: Resposta ao desafio $RN1_A$ enviado por Alice na mensagem M1

$RN1_B$: *Random Nonce* de 128 bits, gerado e enviado por Bob

H(): Função de síntese

$SIG_{KprivB}(X)$: Assinatura digital (DSA) de Bob do conteúdo X onde Bob confirma a utilização proposta por Alice dos parâmetros G e P, usando uma chave privada DSA de 1024 bits. Trata-se de uma assinatura DSA.

$YpubB$: Número público Diffie-Hellman calculado por Bob a partir dos parâmetros G e P e do respetivo número secreto YprivB, guardado por Bob de forma privada.

KpubA: Chave Pública RSA de Alice, que foi obtida na validação da cadeia CChainA em M1 e do certificado de Alice enviado nessa cadeia. A chave tem 1024 bits

$CChain_B$: Cadeia de certificados X509v3, contendo o certificado X509v3 da chave pública DSA de Bob (KpubB) e com o certificado raiz de uma CA confiável por Alice para efeitos da sua validação direta

Ronda 3 - Alice to Bob:

$SIG_{KrivA}(RN1_B+1)||\{ Alice,Ypub_A \}_{KpubB}$

KpubB: Chave Pública DSA de Bob, com 1024 bits e que foi obtida na validação da cadeia CChainB em M2 e do certificado de Bob enviado nessa cadeia

$YpubA$: Número público Diffie-Hellman calculado por Alice a partir dos parâmetros G e P e do respetivo número secreto YprivA, guardado por Alice de forma privada

$SIG_{KprivA}(X)$: Assinatura digital de Alice, usando uma assinatura RSA, com SHA-256 e padding PSS, sendo a chave privada usada de 1024 bits

Corolário: a partir das mensagens anteriores, Alice e Bob podem calcular uma chave de sessão com base nos valores YpubA e YpubB que foram trocados, da seguinte forma.

Alice: $Ks = SHA256((YpubB^{YprivA}) \bmod P) ; Kmac= SHA256(Ks); IV = MD5(Kmac||YpubA)$

Bob: $Ks = SHA256((YpubA^{YprivB}) \bmod P) ; Kmac= SHA256(Ks); IV = MD5(Kmac)||YpubB)$

Por cada mensagem trocada por Alice e Bob, enquanto a chave Ks for considerada válida, o IV será iterado por ambos (acrescentando 1, como se fosse um número de sequência).