DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Disciplina: Segurança de Redes e Sistemas de Computadores
1º Semestre, 2021/2022
Teste de Frequência Nº 2 (05/Jan/2022)

`Código do Enunciado: T2-A798-AF02`

Parte I – Parte sem consulta

Questão 1. Considere o problema da revogação de certificados de chave pública. Explique:

a) Qual a diferença entre controlar a validade dos certificados através de listas do tipo CRL ou controlar a validade através do protocolo OCSP

b) Numa CRL, quantas assinaturas digitais existem para comprovar a validade da lista?

c) Como são identificados e indexados os certificados que devem ser considerados revogados numa lista do tipo CRL ?

d) Dado um certificado que se está a validar, como é possível saber a informação para obtenção da lista de revogação atualizada e como é possível obter a informação para proceder à validação através de OCSP ?

e) Em que consiste e para que serve um certificado em formato CSR (ou PKCS#10) ?

Questão 2

a) No modelo da Framework PKIX associada à gestão do ciclo de vida de solicitação e gestão de certificados de chave pública, qual o papel de uma entidade RA e qual a diferença entre uma entidade RA e uma entidade CA ?

b) Nas funções de gestão no modelo PKIX, em que consiste a noção de "*Cross-Certification*"?

Questão 3. Considere os 5 subprotocolos da pilha TLS considerando as versões TLS 1.0 a 1.2, nomeadamente: AP (*Alert Protocol*), CCSP (*Change Cipher Spec Protocol*), HP (*Handshake Protocol*), HBEAT e RLP (*Record Layer Protocol*), bem como os respetivos tipos de mensagens (ou *message types e respetivos encapsulamentos RLP*)

a) Na estruturação dos subprotocolos indicados em TLS, quais associa ao nível sessão e quais associa ao nível conexão?
b) Qual ou quais dos protocolos não usa(m) assinaturas digitais utilizando criptografia assimétrica ?
c) Qual o papel do subprotocolo CCSP ?
d) Qual o papel do subprotocolo HBEAT ?
e) Qual dos subprotocolos indicados é inexistente na versão TLS 1.3?
f) Que subprotocolo esteve na origem da vulnerabilidade ocorrida na implementação openssl que ficou conhecida por *Heartbleed*?

Questão 4

Indique resumidamente vantagens ou melhorias de desempenho e de segurança da especificação TLS 1.3, comparativamente à versão TLS 1.2.

Parte II – Parte com consulta (apenas usando materiais impressos e individuais)

Questão 5

Considere a cadeia de certificação (obtida de uma conexão HTTPS do *endpoint* https://cloudflare.com bem como os atributos do certificado assinalado (www.cloudflare.com), dados em anexo.

a) Porque é que o certificado mostrado não pode ser usado numa cadeia de certificação em que aparecesse numa posição de topo ou intermédia nessa cadeia (devendo nesse caso a cadeia ser considerada não válida) ? Porquê ?

b) Pode o certificado indicado ser usado para estabelecer uma conexão TLS com o servidor www.cloudflare.com por parte de um cliente que pretende estabelecer uma *ciphersuite* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 e protocolo TLS 1.2 ? Justifique.

c) Qual o interesse em serem utilizadas no certificado duas funções de síntese que aparecem como atributos FINGERPRINT ? Justifique.

d) Que tipo de assinatura digital e respetivo algoritmo criptográfico deverá ter sido usado na assinatura do atributo "*Signature*" do campo de atributos "*Public Key Info*" ? Porquê ?

Questão 6

Considere o a seguinte sequência de mensagens de uma conexão TLS/TCP, cuja captura foi obtida com a ferramenta *Wireshark*.

No.	Source	Destination	Protocol	Length	Info
1	192.168.32.1	192.168.32.146	TCP	66	46692 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2	192.168.32.146	192.168.32.1	TCP	66	https > 46692 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
3	192.168.32.1	192.168.32.146	TCP	54	46692 > https [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	192.168.32.1	192.168.32.146	TLSv1.2	229	Client Hello
5	192.168.32.146	192.168.32.1	TCP	54	https > 46692 [ACK] Seq=1 Ack=176 Win=30336 Len=0
6	192.168.32.146	192.168.32.1	TLSv1.2	1450	Server Hello, Certificate, Server Key Exchange, Server Hello Done
7	192.168.32.1	192.168.32.146	TLSv1.2	216	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
8	192.168.32.1	192.168.32.146	TLSv1.2	382	Application Data
9	192.168.32.146	192.168.32.1	TCP	54	https > 46692 [ACK] Seq=1397 Ack=666 Win=32512 Len=0
10	192.168.32.146	192.168.32.1	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11	192.168.32.146	192.168.32.1	TLSv1.2	428	Application Data
12	192.168.32.1	192.168.32.146	TCP	54	46692 > https [ACK] Seq=666 Ack=2013 Win=65700 Len=0
13	192.168.32.1	192.168.32.146	TLSv1.2	382	Application Data
14	192.168.32.146	192.168.32.1	TLSv1.2	428	Application Data
15	192.168.32.1	192.168.32.146	TCP	54	46692 > https [ACK] Seq=994 Ack=2387 Win=65324 Len=0

TCP HANDSHAKE

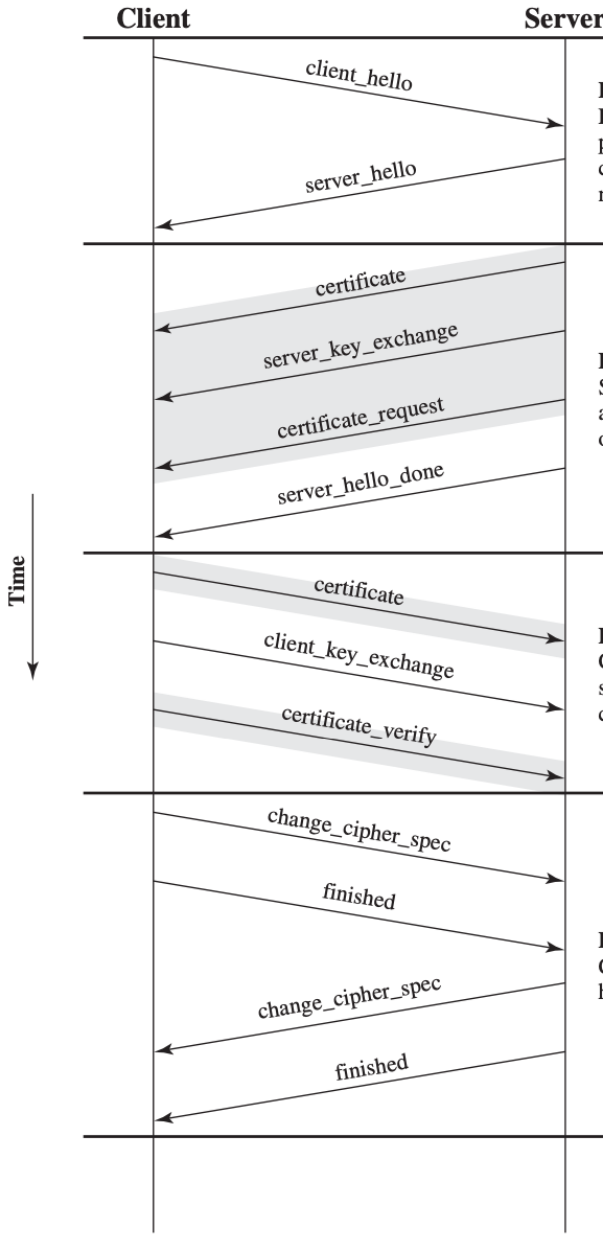
a) De acordo com a análise desta captura indique, **justificando de forma clara e inequívoca**, se o *handshake* corresponde ao estabelecimento de uma sessão TLS com autenticação mútua cliente/servidor, autenticação unilateral do cliente (com possível inversão do papel de cliente da conexão TCP como *endpoint* servidor TLS) ou autenticação unilateral do servidor (sem inversão de papeis entre cliente e servidor da conexão TCP).

b) Após qual das mensagens na captura indicada já ficou estabelecida ou selecionada a *ciphersuite* TLS que será usada entre os *endpoints* TLS cliente e servidor ?

Questão 7 . Como sabe, a especificação TLS é hoje materializada com base no protocolo de transporte TCP (para a concretização TLS/TCP) ou no protocolo UDP (para a concretização

DTLS/UDP), independentemente da especificação base do protocolo (por exemplo, TLS 1.2, bem como DTLS 1.2).

Considere o seguinte fluxo de referência do *handshake*, válido para qualquer uma das versões acima. Porque é que não fará sentido o cliente enviar a mensagem "*certificate_verify*" no caso de não mandar também a mensagem "*certificate*" ou esta mesma ser enviada com conteúdo nulo? Justifique.



Questão 8 .

Responda a esta questão que se relaciona com o seu conhecimento sobre TLS e/ou DTLS, tendo em conta a sua implementação concreta do projeto 2 e o respetivo contexto de especificação e opção da implementação entregue para avaliação.

Na sua implementação, suportou formas de overlaying (ou sobreposição) dos protocolos SAPKDP e/ou SRTSP em algum dos seguintes encapsulamentos (ENCAP) e respetivas parametrizações para TLS e/ou DTLS: (conforme a sua **opção de implementação A, B, C, D ou E**):

ENCAP 1) SAPKDP/TLS/TCP (consideradas na opção A e parte da opção D)

ENCAP 2) SAPKDP/DTLS/UDP (considerado na opção E)

ENCAP 3) SRTSP/DTLS/UDP (na opção C)

ENCAP 4) SRTSP com encapsulamentos parciais em TLS/UDP e DTLS/UDP (na opção B ou como parte das opções D ou E)

a) Qual dos encapsulamentos acima (ENCAP 1, 2, 3 ou 4) corresponde à sua implementação?

b) A sua implementação (Projeto 2) sobrepõe as propriedades de segurança que estavam já suportadas nos protocolos SAPKDP e/ou SRTSP (conforme o seu caso), às propriedades de segurança que tem agora com o novo encapsulamento com TLS e/ou DTLS (conforme o seu caso).

   Discuta, dadas as seguintes propriedades de segurança e após a concretização da dolução do Projeto 2, quais as que considera serem PROPRIEDADES DE SEGURANÇA REFORÇADAS, PROPRIEDADES DE SEGURANÇA REDUNDANTES ou NOVAS PROPRIEDADES DE SEGURANÇA (antes inexistentes), considerando a anterior implementação dos protocolos SAPKDP e/ou SRTSP, respetivo fluxo de mensagens e construções e mecanismos criptográficos utilizados (Projeto 1)

   B1) *Peer-Authentication* (Autenticação de Principais)

   B2) *Non-Repudiation* (Não-Repudiação)

   B3) *Message Confidentiality* (Confidencialidade de mensagens)

   B4) *Traffic-Flow Confidentiality* (Confidencialidade de tráfego)

   B5) *Message Integrity* (Integridade de mensagens)

   B6) *Mitigation of DoS* (forma de mitigação de possível ataque de negação de serviço)

ANEXO PARA RESPOSTA DA QUESTÃO 5

www.cloudflare.com
Issued by: Cloudflare Inc ECC CA-3
Expires: Sunday, 18 September 2022 at 00:59:59 Western European Summer Time
This certificate is valid

Details

Subject Name	
Country or Region	US
County	California
Locality	San Francisco
Organisation	Cloudflare, Inc.
Common Name	www.cloudflare.com
Issuer Name	
Country or Region	US
Organisation	Cloudflare, Inc.
Common Name	Cloudflare Inc ECC CA-3
Serial Number	01 D2 1F C8 3C C6 CA 03 A1 0F 13 95 C2 A7 26 1C
Version	3
Signature Algorithm	ECDSA Signature with SHA-256 (1.2.840.10045.4.3.2)
Parameters	None
Not Valid Before	Saturday, 18 September 2021 at 01:00:00 Western European Summer Time
Not Valid After	Sunday, 18 September 2022 at 00:59:59 Western European Summer Time
Public Key Info	
Algorithm	Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters	Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key	65 bytes: 04 E2 80 08 0A 68 99 48 ...
Key Size	256 bits
Key Usage	Encrypt, Verify, Derive
Signature	70 bytes: 30 44 02 20 68 6A 57 7C ...

Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Digital Signature

Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO

Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)

Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	80 4D 4A 42 32 AE 09 8F 51 07 4B A8 D4 D4 76 A8 BB 41 B0 31

Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	A5 CE 37 EA EB B0 75 0E 94 67 88 B4 45 FA D9 24 10 87 96 1F

Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	*.www.cloudflare.com
DNS Name	www.cloudflare.com

Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(2.23.140.1.2.2)
Qualifier ID #1	Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI	http://www.digicert.com/CPS

Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl3.digicert.com/CloudflareIncECCCA-3.crl
URI	http://crl4.digicert.com/CloudflareIncECCCA-3.crl

Extension	Embedded Signed Certificate Timestamp List (1.3.6.1.4.1.11129.2.4.2)
Critical	NO
SCT Version	1
Log Operator	Google
Log Key ID	29 79 BE F0 9E 39 39 21 F0 56 73 9F 63 A5 77 E5 BE 57 7D 9C 60 0A F8 F9 4D 5D 26 5C 25 5D C7 84
Timestamp	Saturday, 18 September 2021 at 01:11:13 Western European Summer Time
Signature Algorithm	SHA-256 ECDSA
Signature	71 bytes: 30 45 02 21 00 BC A0 C9 ...
SCT Version	1
Log Operator	DigiCert
Log Key ID	51 A3 B0 F5 FD 01 79 9C 56 6D B8 37 78 8F 0C A4 7A CC 1B 27 CB F7 9E 88 42 9A 0D FE D4 8B 05 E5
Timestamp	Saturday, 18 September 2021 at 01:11:13 Western European Summer Time
Signature Algorithm	SHA-256 ECDSA
Signature	71 bytes: 30 45 02 20 53 0C A4 2B ...
SCT Version	1
Log Operator	Cloudflare
Log Key ID	41 C8 CA B1 DF 22 46 4A 10 C6 A1 3A 09 42 87 5E 4E 31 8B 1B 03 EB EB 4B C7 68 F0 90 62 96 06 F6
Timestamp	Saturday, 18 September 2021 at 01:11:13 Western European Summer Time
Signature Algorithm	SHA-256 ECDSA
Signature	71 bytes: 30 45 02 21 00 ED 20 39 ...

Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://ocsp.digicert.com
Method #2	CA Issuers (1.3.6.1.5.5.7.48.2)
URI	http://cacerts.digicert.com/CloudflareIncECCCA-3.crt

Fingerprints

SHA-256	C4 31 3D 39 3D 60 76 65 D5 67 5A AC FC 1A 45 6B A9 03 84 32 EF 01 52 E7 B9 A8 41 01 3C BC 0F 2F
SHA-1	04 52 18 C4 BE 5E B8 C2 73 08 93 D3 94 D1 B6 62 76 AF 79 A0