DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Course: Computer Networks and Systems Security
1º Semester, 2021/2022
Midterm Frequency Test Nr. 2 (05/Jan/2022)

`Test CODE: T2-A798-AF02`

Part I – Closed Book Part

Question 1. Consider the methods used to control the revocation of X509v3 certificates

a) Explain the difference in the revocation control using CRLs (Certificate Revocation Lists) or OCSP (Online Certificate Status Protocol).

b) In a CRL, how many digital signatures exist for the revocation of the respective certificates?

c) Given a CRL to control the possible revocation of a certain certificate, explain how the certificate must be searched in the CRL (i.e., what Certificate attribute is used to index the certificate in the list?)

d) Where is the information related to communication endpoints to obtain the last version of issued CRL or to support the OCSP protocol for a given certificate?

e) Explain what is a CSR formatted certificate (or PKCS#10) and the objective for which such certificates are used.

Question 2

a) Considering the PKIX Framework, explain the difference in the roles of RA and CA entities.

b) Explain the purpose or relevance of the "*Cross-Certification*" management function, as one of the notions in the PKIX framework model.

Question 3. In the TLS stack (from TLS 1.0 to T LS 1.2), there are different subprotocols: AP (*Alert Protocol*), CCSP (*Change Cipher Spec Protocol*), HP (*Handshake Protocol*), HBEAT e RLP (*Record Layer Protocol*), with the correspondent message types in RLP encapsulations)

a) What subprotocols are associated to TLS Session-Level abstraction and what subprotocols are associated to the TLS-Connection abstraction?
b) What subprotocols don't use digital signatures with asymmetric cryptographic methods?
c) Explain the purpose of the CCSP subprotocol.
d) What subprotocols above are not included in the version TLS 1.3?
e) What protocol originated the vulnerability implementation in *openssl,* known as the *Heartbleed* vulnerability?

Question 4

Summarize the main improvements in security and performance comparing TLS v1.3 with the previous TLS 1.0, 1.1 or 1.2 versions.

Part II – Open Book Part (only can use printed and individual materials)

Question 5

Consider the certificate chain (obtained in a HTTPS connection to the *endpoint* https://cloudflare.com as well as the certificate for the entry (www.cloudflare.com) and respective attributes (IN ANNEX)

a) Explain why the represented certificate cannot be used as an intermediate or top-level certificate in a certification chain because in this case the chain must be rejected in a validation process.

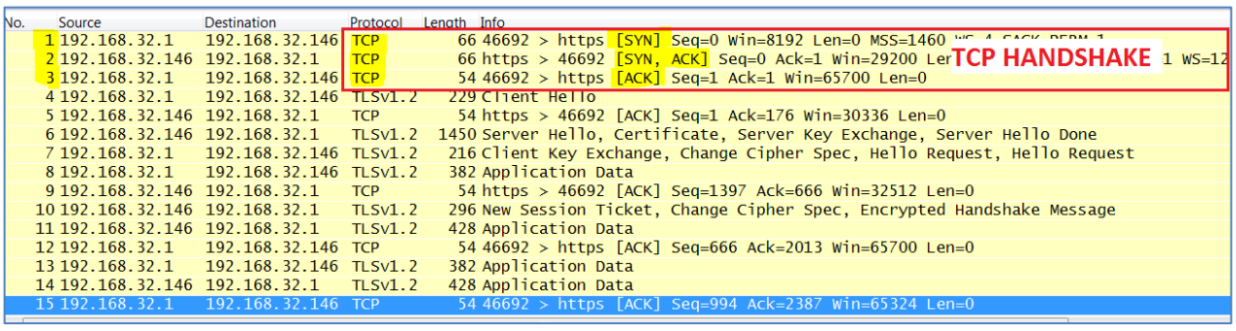
b) Is it possible the use of the certificate the above certificate if a client wants to establish a TLS 1.2 session fixing the *ciphersuite* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384? Why?

c) Explain the purpose or interest of two different secure hash functions in the FINGERPRINT attributes in the same certificate.

d) What type of digital signature and cryptographic algorithm it is used the "*Signature*" attribute in the "*Public Key Info*" ? Why ?

Question 6

Consider the following sequence of a traffic capture including TCP and TLS messages (obtained with the Wireshark tool)



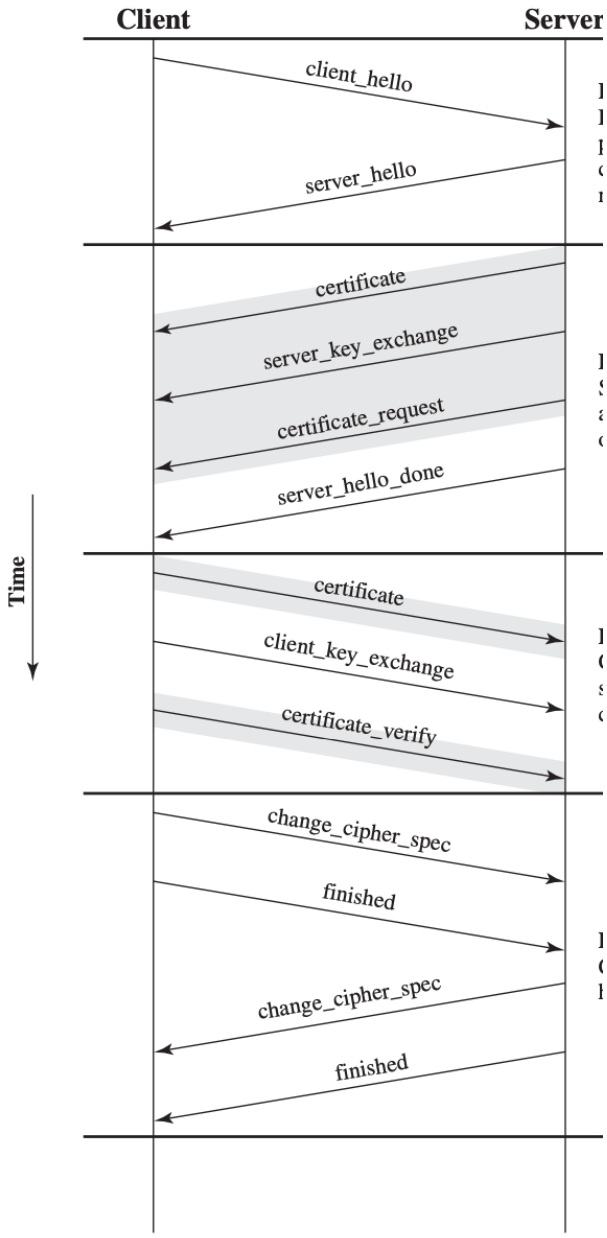
a) Can you say, unequivocally, what authentication mode was used from the following ones: SERVER-ONLY Authentication; CLIENT-ONLY AUTHENTICATION; SERVER-ONLY AUTHENTCIATION with a possible inversion of TCP Client Role in the TLS Server Role; or MUTUAL AUTHENTICATION ? Why ?

b) What is the message in the flow thar defined the TLS *ciphersuite* that will be used by the Client and the Server after he conclusion of the handshake with success

Question 7 . The TLS specification is today materialized in two different encapsulations, using TCP (case of TLS/TCP) and UDP (case of DTLS/UDP), independently of the TLS or DTLS version (example, TLS v1.2 or DTLS v1.2)

Given the *handshake* reference flow (valid for DTLS or TLS) explain why is not expected to observe the message certificate-verify sent by the client if we don't observe previously the message *certificate* also sent by the client or if the message *certificate* sent by the client has a null

payload? Explain this considering the purpose or context as well as the cryptographic support for the message-type *certificate verify*.



Question 8

Answer this question considering the context of implementation and specification OPTION of your Project Assignment #2, as delivered for evaluation.

Considering all the possible encapsulations for overlaying SAPKDP and SRTSP protocols: (according to the possible overlaying options **A, B, C, D or E**):

ENCAP 1) SAPKDP/TLS/TCP (overlaying encapsulation for Option A and Part of Option D)

ENCAP 2) SAPKDP/DTLS/UDP (overlaying encapsulation for Option E

ENCAP 3) SRTSP/DTLS/UDP (Corresponding to Option C)

ENCAP 4) SRTSP with partial encapsulations in TLS/UDP and DTLS/UDP (corresponding to Option B or part of options D and E)

a) What encapsulation (ENCAP 1, 2, 3 or 4) corresponds to your implementation of Project Assignment #2 ?

b) Considering the following security properties (from B1 to B6) and those already supported by the overlayed SAPKDP or SRTSP protocols, previously to the implementation of the Project Assignment #2 and refer what properties you consider as:

   REDUNDANT SECURITY PROPERTIES IN THE SOLUTION AFTER PA#2

   ENFORCED SECURUTY PROPERTIES IN THE SOLUTION AFTER PA#2

   NEW SECURITY PROPERTIES, IN THE SOLUTION AFTER PA#2, NOT SUPPOTED BEFORE

   B1) Peer-Authentication

   B2) Non-Repudiation

   B3) Message Confidentiality

   B4) Traffic-Flow Confidentiality

   B5) Message Integrity

   B6) Mitigation of DoS

ANNEX (for Question 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