Feb 22, 2022

Introduction to Computer and Network Security

Part 1

Question 1 [40 points]

In the context of TLS, (a) draw the message sequence chart of the handshake protocol for version 1.2 and briefly describe each step, (b) explain how TLS provides for authentication, confidentiality, and integrity.

Question 2 [10 points]

What is a digital certificate and what are its main components?

Part 2

Question 3 [40 points]

In the context of access control, explain (a) explain what is a confused deputy with the help of an example, (b) how capabilities allow for avoiding a confused deputy attack, (c) explain the notion of Discretionary Access Control (DAC), (d) explain the notion of Mandatory Access Control (MAC), and (e) discuss the main advantages and disadvantages between DAC and MAC.

Question 4 [10 points]

Describe the technique of k-anonymity and explain how it can mitigate linkage attacks.

Please, remember…

On each sheet, make sure to write: Name Surname Student ID number Question number	The file containing the scan of your answers should be named as follows: surname-name-studentIDnumber.pdf