United International University (UIU)

Dept. of Computer Science & Engineering (CSE)

Final Exam Year: 2021 Trimester: Summer

Course: CSE 4531 Computer Security,

Total Marks: 25, Time: 1 hour 15 minutes

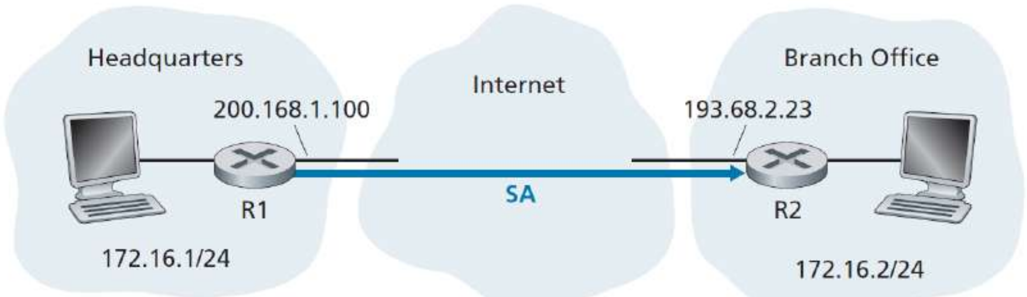
There are FOUR questions. Answer all of them. Figures in the right-hand margin indicate full marks.

Any examinee found adopting unfair means will be expelled from the trimester / program as per UIU disciplinary rules

1. Suppose a community center in France has requested you to design a room reservation system for the center. France is a member of the European Union; hence your designed system must comply with GDPR. They intend to use an on-line form to allow the public to reserve the rooms. Payment can be made through cash on arrival or can be paid through a specific bank before the event. The center has set up a committee to run the facilities and to ensure electricity/logistics etc. are available. Committee members will require contact information for those who make bookings in case there are any last-minute changes. [5]

   Explain which factors you would consider for ***Capture****,* ***Store****, and* ***Use*** *stages of the GDPR information life cycle while designing your system.*

2. a) Consider the following Figure. Suppose Trudy is a man-in-the-middle, who can insert datagrams into the stream of datagrams going from R1 and R2. As part of a replay attack, Trudy sends a duplicate copy of one of the datagrams sent from R1 to R2, and Trudy also increases the sequence number of the datagram. Will R2 decrypt the duplicate datagram and forward it into the branch-office network? Why or why not? Justify your answer. [3]



   b) Assume two transport mode SA are bundled to allow both AH and ESP protocols on the same end-to-end flow. Explain why performing the ESP protocol before performing the AH protocol is the recommended ordering of these security protocols. [2]

3. a) Explain the double-spending problem with an example. Discuss how double spending is handled in Bitcoin? [2]

   b) A particular TLS session can serve to different TLS connections. Explain how [3]

	handshaking is done is such cases.	
4.	a) Your organization has decided to centralize anti-virus support on a server which automatically updates virus signatures on user’s PCs. When calculating risk due to viruses, the annualized loss expectancy (ALE) is $105,000. The cost of this anti-virus countermeasure is estimated to $30,000/year, and it will lower the ALE to $80,000. Is this a cost-effective countermeasure? Why or why not? b) A vulnerability in the MySQL Server database could allow a remote, authenticated user to inject SQL code that runs with high privileges on a remote MySQL Server database. A successful attack could allow any data in the remote MySQL database to be read or modified. The vulnerability occurs due to insufficient validation of user-supplied data as it is replicated to remote MySQL Server instances. An attacker requires an account on the target MySQL database with the privilege to modify user-supplied identifiers, such as table names. The account must be on a database which is configured to replicate data to one or more remote MySQL databases. An attack consists of logging in using the account and modifying an identifier to a new value that contains a fragment of malicious SQL. This SQL will later be replicated to, and executed on, one or more remote systems, as a highly privileged user. *Analyze the description above by using **CVSS v2** method to find the **base vector** and **base score** of this vulnerability. **Justify** your base vector.*	[3] [7]