**Birla Institute of Technology & Science, Pilani**

**Work-Integrated Learning Programmes Division**

**Second Semester 2020-2021**

**Mid-Semester Test (EC-2 Regular)**

Course No. : SS ZG681

Course Title : CYBER SECURITY

Nature of Exam : Open Book

No. of Pages = 3

# No. of Questions = 5

Weightage : 30%

Duration : 2 Hours

Date of Exam : Friday, 05/03/2021 (AN)

Note:

1. Please follow all the *Instructions to Candidates* given on the cover page of the answer book.
2. All parts of a question should be answered consecutively. Each answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.
4. Consider the following security levels and security categories: [2 x 3 = 6]

* Security Levels: TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), RESTRICTED (R), and UNCLASSIFIED (U) (highest to lowest)
* Security categories: MKTG, MFG, HR, R&D

Based on Bell LaPadula security model, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. While analyzing each question, specify the property for read and write on which your analysis is based.

Assume that discretionary access controls allow anyone access unless otherwise specified.

1. Explain simple security condition and \*-Property using the security levels as examples
2. Apple, cleared for (TS, { MKTG, HR }), wants to access a document classified (S, { MFG, HR }).
3. Banana, cleared for (C, { HR }), wants to access a document classified (C, { MFG }).

1. Consider the following security levels and security categories: [2 x 3 = 6]

* Security Levels: TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), RESTRICTED (R), and UNCLASSIFIED (U) (highest to lowest)
* Security categories: MKTG, MFG, HR, R&D

Based on Bell LaPadula security model, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. While analyzing each question, specify the property for read and write on which your analysis is based.

Assume that discretionary access controls allow anyone access unless otherwise specified.

1. Explain simple security condition and \*-Property using the security levels as examples
2. Mango, cleared for (TS, { MKTG, HR }), wants to access a document classified (C, { MKTG }).
3. Orange, who has no clearances (and so works at the U level), wants to access a document classified (C, { MFG })
4. A common technique for inhibiting password guessing is to disable an account after three consecutive failed login attempts.
5. Explain what is the principle of least common mechanism
6. Discuss how this technique might prevent legitimate users from accessing the system. Why is this action a violation of the principle of least common mechanism?

[2 + 2 + 3 = 7]

1. A common technique for inhibiting password guessing is to disable an account after three consecutive failed login attempts.
   1. Explain what is the principle of least common mechanism
   2. Discuss how this technique might prevent legitimate users from accessing the system. Why is this action a violation of the principle of least common mechanism?

[2 + 2 + 3 = 7]

1. Consider the discussion we had in class regarding Attack Trees
2. Develop an attack tree for gaining access to a social media account Facebook.
3. Identify various components (at least two) involved in user authentication for the given social media account.
4. For at least two of the components, discuss attack strategies. [2 + 2 + 3 = 7]
5. Consider the discussion we had in class regarding Attack Trees
6. Develop an attack tree for gaining access to a customer’s account in an e-commerce application.
7. Identify various components (at least two) involved in user authentication for the given customer’s account.
8. For at least two of the components, discuss attack strategies. [2 + 2 + 3 = 7]
9. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.
10. An organization managing public information on its Web server.
11. A law enforcement organization managing extremely sensitive investigative information.
12. A financial organization managing routine administrative information (not privacy-related information).
13. Employee office computer with UI institutional data.
14. University web server hosting department and course data. [1 x 5 = 5]
15. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.
16. An online retail store website with flash sales every week.
17. A housing property bidding application website for government projects.
18. A health-care app containing reports and data of patients belonging to multiple diagnostic labs.
19. A government portal having the country's covid-19 vaccination tracking and progress information.
20. An online real time bidding application for live sports events, having user’s activity and bidding details. [1 x 5 = 5]
21. [2 + 3 = 5]
22. Given a scenario where you need to design the security aspects to secure wifi of your organization. Which of the methods for securing wi-fi you would choose to use and reject to use. Explain with reasons.
23. An organization requires a range of IP addresses to assign one to each of its 1200 computers. The organization has approached an Internet Service Provider (ISP) for this task. The ISP uses CIDR and serves the requests from the available IP address space 202.61.0.0/17. The ISP wants to assign an address space to the organization which will minimize the number of routing entries in the ISP’s router using route aggregation. Which of the following address spaces are potential candidates from which the ISP can allot any one of the organization ?

I. 202.61.84.0 / 21

II. 202.61.104.0 / 21

III. 202.61.64.0 / 21

IV. 202.61.144.0 / 21

Justify your answer.

1. [2 + 3 = 5]
2. Given a scenario where you need to design the security aspects to secure wifi of your organization. Which of the methods for securing wi-fi you would choose to use and reject to use. Explain with reasons.
3. An Internet Service Provider (ISP) has the following chunk of CIDR-based IP addresses available with it: 245.248.128.0/20. The ISP wants to give half of this chunk of addresses to Organization A, and a quarter to Organization B, while retaining the remaining with itself. Which of the following is a valid allocation of addresses to A and B?

(A) 245.248.136.0/21 and 245.248.128.0/22

(B) 245.248.128.0/21 and 245.248.128.0/22

(C) 245.248.132.0/22 and 245.248.132.0/21

(D) 245.248.136.0/24 and 245.248.132.0/21

Explain your answer.

\*\*\*\*\*\*\*\*\*