ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)
ORGANISATION OF ISLAMIC COOPERATION (OIC)
Department of Computer Science and Engineering (CSE)

SEMESTER FINAL EXAMINATION   SUMMER SEMESTER, 2022-2023
DURATION: 3 HOURS   FULL MARKS: 150

CSE 6291: Information Security
This is an open book exam, allowing printed materials and handwritten notebooks.
Programmable calculators are not allowed. Do not write anything on the question paper.
Answer all 5 (five) questions. Figures in the right margin indicate full marks of questions.

1. Assume that you are building a software called Nexus, dubbed the entry point to the Internet. The software connects to a specific web address, retrieves and showcases content from that address, and facilitates the transmission of user data to and from that address.

   a) Identify the complicated security issues that can arise from these simple tasks.   14

   b) Determine the possible attack vectors against your software.   6

   c) Discuss why your software would be susceptible to these sorts of attacks compared to other   5
   tools and technologies.

2. Carol, an ABC Bank PLC customer, encountered trouble loading the fund transfer page while using internet banking. To address this, she downloaded an add-on from a dubious website promising to resolve the issue. Despite installation, the loading performance remained unchanged. Instead, Carol started getting random CAPTCHAs that need to be solved before she can perform any transactions.

   ABC Bank PLC's internet banking website employs HTTPS protocol for encrypted communication during transit. Additionally, it utilizes two-factor authentication to verify transactions. Surprisingly, when Carol performed a transaction from the same website, the money was transferred to some unfamiliar account.

   a) With proper justifications, identify the potential types of attacks Carol has been subjected   12
   to.

   b) With necessary figures, explain how, despite the security measures employed by ABC Bank   10
   PLC, such transaction to unfamiliar accounts could occur.

   c) Discuss the possible reasons on why Carol is getting the random CAPTCHAs.   8

3. Idaho University of Telecommunications (IUT) mandates students to provide personal details upon admission. With multiple administrative offices like the Registrar's Office, Provost Office, and Finance and Accounts Office, each needing access to this information, the university sends copies to all departments. However, not all offices require all data. For instance, the Registrar's Office only needs student IDs and enrolled courses, while the Finance and Accounts Office requires IDs and fee records. Again, if students need to update their information, they must visit each office individually. At the same time, it is difficult to identify accidental or malicious changes to the information.

   a) Propose a solution to the problems discussed in the given scenario and justify how the solu-   1 + 10
   tion can mitigate the problems.

   b) Briefly discuss the security requirements of your proposed solution.   14

   c) Users and programs often make mistakes collecting data, computing results, and entering   15
   values. Discuss how your solution can help catch these errors and possibly correct them
   after they are stored.

4. Microsquish, a multinational technology company, heavily depends on office supplies to sustain its daily activities. The central supply room oversees inventory management, including printer cartridges, notepads, and staplers. Departments across the organization request supplies as necessary. For instance, the Marketing Department recently requested 200 reams of printer paper for an upcoming promotional campaign. This initiates a process wherein the supply room takes the following steps:

- Step 1: The supply room staff verifies the availability of 200 reams of printer paper in the database. If the required quantity is unavailable, the requisition is denied, halting the process.

- Step 2: Assuming that there are 300 reams of printer paper currently in stock, the supply room deducts 200 from the inventory figure in the database, leaving 100 reams remaining.

- Step 3: The cost of 200 reams of printer paper is debited from the Marketing Department's office supplies budget and recorded in the database for financial tracking.

- Step 4: The supply room verifies the remaining printer paper quantity (100 reams) to assess if it falls below the predefined reorder point. As it's now below this point, a notification is triggered to reorder printer paper. The item status is updated to "on order" in the database to prevent excess orders and aid in tracking pending rows.

- Step 5: A delivery order is generated, detailing the quantity (200 reams) and destination for the Marketing Department. Upon fulfillment, the printer paper is dispatched to support the department's promotional activities.

The entire operation is executed and tracked in a centralized database.

   a) List the potential database problems that can occur.   4

   b) Propose a solution to the problem and discuss how your solution can address the issues.   1 + 15

   c) With brief explanation, illustrate the step-by-step process of executing the aforementioned operation following your solution.   15

5. General software engineering principles are intended to lead to correct code, which is certainly a security objective, as well. However, there are also activities during program design, implementation, and fielding specifically to improve the security of the finished product. Considering this issue, one of your friends, Olivia, who will open a software company upon graduation, has come to you, an information security expert, for help. Based on the knowledge that you gained throughout the course, provide suggestions on the design principles that she needs to follow for ensuring security of the software.   10