JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE PHD IN IT SECURITY AND AUDIT

FOR 2024/2025 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE: ICD 1107
COURSE TITLE: Database and Distributed Systems Security

EXAM VENUE: **STREAM: PHD IN IT SECURITY AND AUDIT**

DATE:15/1/25 **EXAM SESSION: 9-12.00 NOON**

TIME: 3.00 HOURS

INSTRUCTIONS:

Answer any THREE questions

Candidates must hand in their answer booklets to the invigilator while in the examination room

Question One [20 Marks]

a. As companies grow and storage needs expand beyond a traditional, singular database setup, companies may find themselves needing a more elaborate database option. Distributed databases allow businesses to get all of the benefits of a database, with the capacity to store more data and make it accessible across the entire computer network. Distributed databases do a wonderful job of providing internal data with organizational structure, increased shareability, improved availability, modular growth capacity, and improved processing speeds. However, no data storage solution is without its downfalls. You have been invited to discuss about systems vulnerabilities that resource owners and users should be aware of and how to strengthen the distributed systems against them. (10marks)

b. A study by Gartner states that 75% of the world population will have its personal information covered under privacy regulations by 2024. The massive scale at which data is processed today and the growing reliance on technology underscore the pressing need for data security. Data regulations help establish guidelines for sensitive information protection and promote transparency, trust, and accountability. Organizations are thus legally obliged to protect customer and user data from being lost or stolen and ending up in the wrong hands. Discuss the local and international regulations that bind organizations on data security. (10marks)

Question Two [20 Marks]

a. Access control is one of the most essential cybersecurity practices. Meticulous management of user access rights helps to secure sensitive data and reduces the chance of a successful attack. However, choosing an access control model relevant to your organization can be tricky. As an expert you have been approached to guide on how a telecommunication company would implement database security on a distributed environment, specifically focusing on access controls. Discuss the possible access controls, describing to the organization how they work and the strengths and demerits of each of the access control models. (20marks)

Question Three [20 Marks]

a. A distributed system needs additional security measures than centralized system, since there are many users, diversified data, multiple sites and distributed control. Discuss the types of database security. (10marks)

b. Security must be considered not only when designing and creating a database, but also once it is in use. Auditing and Logging is implemented comprehensively to track and monitor activities within the database. Explain the activities that are critical that require monitoring. (10marks)

Question Four [20 Marks]

a. Transaction-processing systems (TPS) are becoming increasingly more available as commercial products. However, the approaches to the issues associated with using TPS in multilevel secure environments are still in the research stage. Discuss the issues of multilevel security in distributed transaction-processing system. (10marks)

b. Security architecture is crucial for protecting critical assets, mitigating risks, ensuring compliance, maintaining business continuity, building trust, reducing costs, enabling growth, and fostering a security-focused culture within a company. According to Cybersecurity Ventures, in 2023 the cost of cybercrime will hit $8 trillion and by 2025 it will grow to $10.5 trillion. Implementing a well-designed security architecture offers numerous advantages, including reduced security breaches, improved incident response, and cost savings. A security architecture framework is a set of consistent guidelines and principles for implementing different levels of business security architecture. Companies may opt to devise their own frameworks or by combining international standard frameworks. Discuss the following frameworks:

(10marks)

i. The Open Group Architecture Framework (TOGAF),
ii. Sherwood Applied Business Security Architecture (SABSA) and
iii. Open Security Architecture (OSA)

Question Five [20 Marks]

Usage of online payment methods is on the rise. Back in 2023, the number of cashless transactions worldwide amounted to 1.335 billion. This number reflects the positive tendency among consumers to pay for goods, products, and services online. Such a vast number of payments and, respectively, orders to be processed by businesses makes it necessary to have a system for handling transactional, order, and customer data — a Transaction Processing system (TPS). Discuss some of the best practices for securing transaction processing systems. (20marks)