[Knowledge for Development]

KIBABII UNIVERSITY

UNIVERSITY EXAMINATIONS
2015/2016 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR ONE SEMESTER TWO EXAMINATIONS

FOR THE MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

COURSE CODE : MIT824

COURSE TITLE : SECURITY ARCHITECTURE & ANALYSIS

DATE: 13/05/2016 **TIME:200PM-400PM**

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO

SECTION A (Compulsory – 20 Marks)

QUESTION ONE

(a) Explain each of the following terms

(i) Security Architecture (2 Marks)

(ii) Dependability. (2 Marks)

(iii) System architecture (2 Marks)

(b) Effective and efficient security architectures consist of three components. These are the people, processes, and tools that work together to protect companywide assets. To align these components effectively, the security architecture needs to be driven by policy stating management's performance expectations, how the architecture is to be implemented, and how the architecture will be enforced.

Outline the components that should form part of an effective and carefully planned security architecture and should be evaluated during audits of the security architecture.

(5 Marks)

(c) Security policies and procedures should help the organization implement the elements needed to support the architecture.

Explain four of these elements. (4 Marks)

(d) A system can be viewed according to several layers (usually three: its sense, its functions, and its composition)

Illustrate this concept using the mobile phone system (5 Marks)

SECTION B (Attempt any TWO Questions from this section – 40 Marks)

QUESTION TWO

(a) Survivability is the ability of a computer-communication system-based application to satisfy and to continue to satisfy certain critical requirements (e.g., specific requirements for security, reliability, availability and correctness) in the face of adverse conditions. Survivability must be defined with respect to the set of adversities that are supposed to be withstood.

Distinguish between reliability and availability (4 Marks)

(b) Discuss the Survivability of the computer-communication infrastructures on which the national infrastructures depend, such as the Internet and its eventual successors. (6 Marks)

(c) Enterprise survivability is a requirement on the enterprise as a whole. Other such highest-layer application requirements might include preservation of human safety for friendly humans, destruction of unfriendly humans by a tactical system in a hostile environment and detailed accountability of system and human actions in terms of the application functionality.

Discuss five necessary system security properties (10 Marks)

QUESTION THREE

(a) Assessments are an essential component of the security architecture because they enable the company to determine the architecture's effectiveness. As part of the assessment, internal auditors can recommend that the organization creates a cross-functional team.

Suggest the composition of such a team. (8 Marks)

(b) System Survivability, security, reliability, and performance - need to be implemented in such a way that the desired properties can be achieved dependably. Defensive measures include establishment of appropriate requirements, good system design that is consistent with the requirements, good system development and coding practice including the use of modern software engineering and sound programming languages among other things.

Discuss four attributes that are highly desirable in ensuring dependable survivability of a system. (12 Marks)

QUESTION FOUR

(a) Problems in system operation and use involve people and external factors.

Use three examples to illustrate such problems. (8 Marks)

(b) Discuss six of the many stages of system development and use during which risks may arise, along with a few examples of what might go wrong (and, in most cases, what has gone wrong in the past). (12 Marks)

QUESTION FIVE

(a) Breakdowns in system survivability are often attributed to either security problems or reliability problems. However, there is an interesting crossover between the two types of problems, whereby causes and effects may be related and in some cases intermixed.

Discuss the following intermixed cases:

(i) Reliability problems that also could have been security problems. (5 Marks)

(ii) Security problems that could also have been reliability problems. (5 Marks)

(b) Discuss five countermeasures to manage a database. (10 Marks)