Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

EIGHTH SEMESTER B.TECH DEGREE EXAMINATION(S), OCTOBER 2019

Course Code: CS472

Course Name: PRINCIPLES OF INFORMATION SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

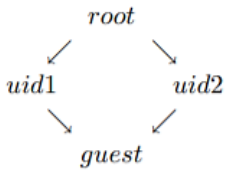
1		Explain the need of information security.	(4)
2		Distinguish between vulnerability and threat. Give example.	(4)
3		Explain Clark-Wilson Model with a neat diagram.	(4)
4		Illustrate SQL injection with an example.	(4)
5		Briefly explain the life cycle of a computer virus.	(4)
6		Explain XSS or Cross Site Scripting.	(4)
7		What is a poll control frame? How does an attacker exploit a poll control frame?	(4)
8		List out any 4 lacunae/pitfalls in GSM Security. Give a brief explanation.	(4)
9		Discuss the strength and weakness of Secure Electronic Transactions.	(4)
10		Explain the entities involved in a web service.	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file bobrc, which Bob owns, but Alice can only read it.Only Cyndy can read and write the file cyndyrc, which she owns. Assume that the owner of each of these files can execute it. Create the corresponding access control matrix.	(6)
	b)	What is a CIA Triad? Explain.	(3)
12	a)	State the *-property for the Chinese Wall model	(4)
	b)	Explain Biba Model.	(5)
13	a)	Differentiate between Discretionary and Mandatory Access Control	(4)
	b)	You are given a security policy stating that a subject has access to an object if and only if the security level of the subject dominates the security level of the	(5)

object. What is the effect of using the following lattice with this policy?



PART C

Answer any two full questions, each carries 9 marks.

14 a) How does buffer overflow vulnerability occur? How does a canary variable detect buffer overflow attack? (5)

b) What is software vulnerability? What are the common types of software flaws that lead to vulnerability? (4)

15 a) Explain various Internet propagation models for worms. (6)

b) Explain about code red worms. (3)

16 a) What are topological worms? Explain any 2 Topological worms. (5)

b) Differentiate between stored and reflected XSS. (4)

PART D

Answer any two full questions, each carries 12 marks.

17 a) How is security enhanced in UMTS when compared to GSM? (8)

b) How is encryption of messages between cell phone and base station achieved in GSM? (4)

18 a) Explain various security threats associated with RFID systems. (6)

b) What are the various elements in XML Encryption? Explain. (6)

19 a) How is data protection achieved in WEP? What are its drawbacks. (6)

b) Explain dual signature with respect to SET. (3)

c) With an example, explain SAML assertion. (3)

****