Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

EIGHTH SEMESTER B.TECH DEGREE EXAMINATION, MAY 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		What is brute force attack?	(4)
2		Discuss different types of attacks that can occur in an organization.	(4)
3		Describe discretionary policies for Biba model.	(4)
4		What is phishing? Give an example.	(4)
5		Differentiate between polymorphic and metamorphic worm.	(4)
6		How do you reduce the impact of XSS vulnerabilities?	(4)
7		Describe frame spoofing with a neat diagram.	(4)
8		Describe the security enhancements present in UMTS.	(4)
9		What is SOAP binding? Explain with the help of a HTTP message.	(4)
10		List the security threats in RFID based identification and tracking systems.	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	What is role based access control. Illustrate with suitable example the concept of role inheritance.	(4)
	b)	Differentiate between Discretionary and Role based access control.	(2)
	c)	Briefly discuss Mandatory access control implemented in a typical secure operating system.	(3)
12	a)	Demonstrate Chinese wall security model with neat diagram.	(5)
	b)	Classify each of the following as a violation of confidentiality, integrity, availability or some combination thereof. Also justify your answer. i. John copies Mary's homework. ii. Paul crashes Linda's system iii. Carol changes the amount of Angelo's check from 100 to 1000 iv. Gina forges Roger's signature on a deed.	(4)

13	a)	Interpret about the star property in Bell -LaPadula model.	(4)
	b)	Write Windows access control algorithm.	(5)

PART C

Answer any two full questions, each carries 9 marks.

14	a)	How Buffer OverFlow (BOF) vulnerability makes software insecure. Explain different ways in which BOF exploitations occur.	(5)
	b)	Explain XSS vulnerabilities.	(4)
15	a)	Describe Kermack-McKendrick Model of worm propagation.	(5)
	b)	Explain any two categories of topological worms.	(4)
16	a)	Explain how can you detect and prevent SQL Injection vulnerabilities.	(5)
	b)	Name any worm that exploited buffer overflow vulnerability. Explain its characteristics.	(4)

PART D

Answer any two full questions, each carries 12 marks.

17	a)	Explain link level security provided by Bluetooth.	(6)
	b)	Describe entity authentication and key agreement in GSM Networks.	(6)
18	a)	How security is implemented in online credit card payment systems?	(8)
	b)	What are the main concerns involved in online credit card payment systems?	(4)
19	a)	Explain MAC generation and encryption in CCMP.	(6)
	b)	Explain any two technologies for web services.	(6)

****