Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Eighth semester B.Tech degree examinations, September 2020

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 access control mechanism provides enhanced security in SELinux? How is the security provided?	(4)
2		Illustrate with an example how access is granted by an access control matrix.	(4)
3		Describe Biba integrity model.	(4)
4		How can buffer overflow vulnerability be prevented?	(4)
5		What is timing attack?	(4)
6		How did Code Red propagate?	(4)
7		With the help of a diagram explain the key hierarchy in 802.11i.	(4)
8		What is the need for Link Level Authentication in Bluetooth?	(4)
9		Describe the strength and weakness of secure electronic transaction	(4)
10		Describe SAML assertion with an example.	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)		Distinguish between discretionary and mandatory access control	(3)
	b)		Let L and C be the set of sensitivity/clearance levels and set of categories respectively. L= {UNCLASSIFIED, CONFIDENTIAL,TOP SECRET} and C={Sales, NewProducts, BusinessPartners}. Here TOP SECRET is at the highest clearance level and UNCLASSIFIED the lowest.	
		(i)	How can two documents with security labels <TOP SECRET,{Sales}> and <UNCLASSIFIED,{Sales,NewProducts}> be compared?	(3)
		(ii)	What is the minimum clearance that a subject should have to access the two documents?	(3)
12	a)		Explain waterfall model for providing security.	(5)
	b)		Explain Star property of Bell- LaPadula Model.	(4)

13	a)	Rima, shankar and david are three users of a computer system. They own the files A, B and C respectively Rima is able to write the files B and C shankar can read and write files A & C David can read file A and write file B. The owner of each of these files can execute it. Create the corresponding access control matrix	(4)
	b)	Demonstrate Chinese wall Security model with a neat diagram.	(5)

PART C

Answer any two full questions, each carries 9 marks.

14	a)	What are topological worms? Illustarte email and P2P worms.	(5)
	b)	Explain Kermack-McKendrick Model of worm propagation.	(4)
15	a)	Describe SQL injection vulnerability.	(5)
	b)	How can a shell code be used for exploiting stack overflow?	(4)
16	a)	Discuss cross site scripting vulnerabilities.	(4)
	b)	Explain different worm characteristics.	(5)

PART D

Answer any two full questions, each carries 12 marks.

17	a)	Explain Integrity protection and encryption in UMTS.	(6)
	b)	Illustrate the need for frame spoofing.	(6)
18	a)	What are the various elements in XML signatures?	(6)
	b)	Describe Secure Electronic Transaction.	(6)
19	a)	Explain Authentication and Key Agreement in 802.11i.	(6)
	b)	Explain any one mechanism used in RFID for ensuring the security. Mention any one attack that can occur in RFID system.	(6)

****