Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058, India

(Autonomous College Affiliated to University of Mumbai)

Mid Semester Examination

March 2020

Max. Marks: 20 | Duration: 1 Hrs.
Class: T.E. | Semester: VI
Course Code: IT63 | Branch: IT
Name of the Course: Information and Network security

Instruction:
(1) All questions are compulsory
(2) Draw neat diagrams
(3) Assume suitable data if necessary

Q. No.		Max. Marks	CO-BL-PI
1	Discuss and justify, two advantages of capabilities over ACLs and two advantages of ACLs over capabilities.	5	2-2-3.1.1
	OR		
	The Bell-LaPadula model was motivated by the requirement of data confidentiality while the Biba model was motivated by the requirement of data integrity. a. Can MLS be used to simultaneously satisfy the requirement of both confidentiality and integrity? If so, how? If no, why not? Justify	5	2-4-3.1.6
2	On an OS supporting RBAC a. Can/should a user be able to login with multiple roles? Why or why not? b. Can/should a user be allowed to switch between roles? If so, how? If not, why not? c. At any given point in time, should it be possible for a user be in more than one role? Why or why not?	3	2-3-6.1.1
	OR		
	What is the distinction between a polymorphic and a metamorphic worm? How might metamorphic software be used for good instead of evil?	3	3-4-8.1.1
3	Consider a DRM system implemented in software on a PC. State limitations of DRM system and justify why is encryption necessary but not sufficient to provide "persistent protection".	5	3-3-8.1.1

4	a. Construct a Playfair matrix with the key "occurrence". b. Encrypt this message: "Must see you over Cadogan West". c. Decrypt the message encrypted in question "b".	1 2 2	1-3-2.1.1
5	Here is a message that was encrypted using the columnar transposition on a rectangular array with keyword "analyst". **"TRLEE LIGCI GEHAL ANTNC TECYE NEN"** Decrypt this message to retrieve the original message.	2	1-3-2.1.1
	OR		
	Here is a message that was encrypted using the columnar transposition on a rectangular array with keyword "Pilgrim". **"NSIREMMSARCLAUSENOAEBDOSSHNO"** Decrypt this message to retrieve the original message.	2	1-3-2.1.1

XXXX