SOMAIYA VIDYAVIHAR UNIVERSITY

11/05/2024 (E)

Semester: January 2024 –April 2024		
Maximum Marks: 100 Examination: ESE Examination		Duration:3 Hrs.
Programme code: 01 Programme: B.Tech Computer Engineering	Class: T.Y.B.Tech	Semester: VI (SVU 2020)
Name of the Constituent College: K. J. Somaiya College of Engineering	Name of the department: Computer Engineering.	
Course Code: 116U01C602	Name of the Course: Information Security.	
Instructions: 1)Draw neat diagrams, wherever applicable. 2) All questions are compulsory. 3) Assume suitable data wherever necessary.		

Que. No.	Question	Max. Marks
Q1	Solve ***any Four*** of the following:	**20**
i)	"*Security professionals balance the cost and effectiveness of controls with the likelihood and severity of harm.*" Explain with supporting example – harm, likelihood and control in the above statement.	5
ii)	Interpret the outcome of the following: and justify the statement $D(E(M,K_U), K_U) = M = E(D(M,K_U),K_U)$ where M is the message, E is encryption function, D is the decryption function and K is the key for user U.	5
iii)	List three controls that could be applied to detect or prevent off-by-one errors.	5
iv)	Are computer-to-computer authentications subject to the weakness of replay attack? Why or Why not? Justify.	5
v)	List down the weaknesses of Wired Equivalent Privacy (WEP).	5
vi)	What are trade secrets? What are the two main requirements for information to be protectable as a trade secret?	5

Que. No.	Question	Max. Marks
Q2 A	Solve the following:	**10**
i)	Write the strengths and weakness of DES.	5
ii)	Explain the Feistal structure of DES.	5
	OR	
Q2 A	A program is written to compute the sum of the integers from 1 to 10. A programmer, well trained in reusability and maintainability, writes the program so that it computes the sum of the numbers from k to n. However, a team of security specialists scrutinizes the code. The team certifies that this program properly sets k to 1 and n to 10; therefore, the program is certified as being properly restricted in that it always operates on precisely the range 1 to 10. List and explain the different ways that this program can be sabotaged so that during execution it computes a different sum, such as 3 to 20.	10
Q 2 B	Solve *any **One***:	**10**
i)	Explain different compile-time and run-time defences for buffer overflow.	10
ii)	Explain the flaw and countermeasures for the following: (a) Undocumented Access Point. (b) Integer Overflow.	10

Que. No.	Question	Max. Marks
Q3	Solve *any **Two***:	**20**
i)	If you forget your password for a website and you click (forgot my password), sometimes the company sends you a new password by email but sometimes it sends you your old password by email. (a) Compare these two cases in terms of vulnerability of the website owner. (b) Mention the countermeasures for overcoming these vulnerabilities.	10
ii)	What do you understand by clickjacking? Explain a technique by which a browser could detect and block clickjacking attacks.	10
iii)	What are email-based attacks? Explain any one such attack and the countermeasures for prevention of the same.	10

Que. No.	Question	Max. Marks
Q4	Solve *any **Two***:	**20**
i)	List and explain any three threats to network communication.	10
ii)	With reference to network security, explain the following terms: (a) Port Scanning. (b) Any one tool for Port Scanning with features. (c) Outcome/Result of Port Scanning.	10
iii)	Write the different functionalities of a firewall. Why is firewall a good place to implement a VPN? Explain.	10

Que. No.	Question	Max. Marks
Q5	Write Short notes on *any **four**:*	**20**
i)	Digital Signatures.	5
ii)	Ransomwares.	5
iii)	Authentication mechanisms.	5
iv)	Link Encryption Vs End-to-End Encryption.	5
v)	Demilitarized Zones (DMZ).	5
vi)	Difference between Laws and Ethics.	5