K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

May – June 2025

PhD Program: Academic Year 2024-25
Course Work Examination

Course Code: **PhD102** and Course Name: **Information Security - 5 - Secure Systems Engineering**
Date: 21-05-2025 Duration: 2.00 PM to 4.30 PM Max. Marks: 70

Instructions:
(1) All questions are compulsory.
(2) Draw neat diagrams wherever applicable.
(3) Assume suitable data, if necessary.

QN	**Question**	Max. Marks	CO	BT Level
Qu-1	Solve any **Six** questions out of **Eight.**	**30**		
i)	Describe how stack layout is affected during a buffer overflow attack.	5	CO1	2
ii)	List and explain two compiler-level techniques to detect/prevent buffer overflows.	5	CO2	2
iii)	How does a heap overflow differ from a stack overflow?	5	CO4	2
iv)	Differentiate between Discretionary Access Control (DAC) and Mandatory Access Control (MAC).	5	CO3	4
v)	Explain how confinement is used to secure mobile applications.	5	CO5	2
vi)	What are the challenges in developing secure applications using SGX?	5	CO6	2
vii)	What is a micro-architectural attack? Give one example.	5	CO3	2
viii)	Describe any two hardware threats in embedded systems.	5	CO4	2
Qu-2	Solve any **TWO** questions out of **THREE.**	**20**		
i)	Explain in detail how a buffer overflow attack works. Illustrate with C code and show how the stack is manipulated during the attack.	10	CO2	2
ii)	Compare and contrast compile-time, runtime, and hardware-level protections against buffer overflow. Support your answer with examples.	10	CO4	4
iii)	What is buffer overread? Explain its working using the Heartbleed vulnerability as a case study.	10	CO6	2
Qu-3	Solve any **TWO** questions out of **THREE.**	**20**		
i)	Explain how capabilities and information flow control models help in implementing confinement in secure systems.	10	CO1	2
ii)	How do secure world and normal world interact in ARM TrustZone? Explain with an example of secure key management.	10	CO3	2

iii)	What are hardware Trojans? Discuss the lifecycle threats they pose and outline techniques for detection and prevention in chip design and manufacturing.	10	CO5	2

****