1.	Title of the course	Computer Systems Security
2.	Course number	CS402M
3.	Structure of credits (L-T-P-C)	2-0-2-3
4.	New course/modification to	Modified with CS531L/COMPUTER SYSTEMS SECURITY
5.	To be offered by	Computer Science and Engineering
6.	Proposed by	V Mahendran
7.	Prerequisite	CS306L/COMPUTER NETWORKS
8.	**Course Objective(s):** To acquire the basic knowledge of cyber security systems through both exploiting system vulnerabilities and using techniques to prevent system exploitations.	
9.	**Course Content:** Review of systems concepts; System exploitation and defense: buffer overflow attacks, privilege separation and capabilities, sandboxing, program analysis; Web and network security: web security models, cross-site scripting attacks and defenses, structured query language injection attacks, secure hypertext transfer protocol, transport layer security, session management, anonymous communication, security issues in transmission control protocol/internet protocol and defense, firewall, intrusion detection, filtering; Mobile security: mobile threat and security models, rootkits, virus, spywares and malware detection; Emerging technologies; Machine learning for security.	
10.	**Textbook(s):** 1. Erickson J, Hacking: The Art of Exploitation, 2nd Edition, No Starch Press (2008). 2. Seitz J and Arnold T, Black Hat Python, 2nd Edition, No Starch Press (2021).	
11.	**Reference(s):** 1. Jaeger T, Operating System Security, Morgan and Claypool (2008). 2. Anderson R, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition, Wiley (2021).	