NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	BTech CSE
Course Code:	4CS210DE25
Course Title:	Embedded System Security
Course Type:	Disciplinary Minor- Elective
Year of Introduction:	2025-26

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to –

1. relate the fundamentals of embedded firmware, hardware, and software vulnerabilities and their causes (BL2)
2. apply the knowledge of tools and technologies to exploit the vulnerabilities related to embedded systems (BL3)
3. implement appropriate countermeasures against the introduced attacks (BL5)
4. design hardware-based trust platforms and implement physically unclonable functions. (BL6)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Introduction to Embedded Systems:** Embedded hardware units, Embedded system software, Device drivers and interrupt services, Interprocess communication and synchronization of processes	06
Unit-II	**Embedded System Security and Trust**: Physical attacks, Side-channel analysis, Trusted integrated circuit, Trusted platform module (TPM), Hardware Trojans, Cryptographic hashing, Stack-based attacks against embedded systems (Code injection and return-oriented programming), Physically unclonable functions, Fault injection attacks, Reverse engineering, Supply chain security and trust	12
Unit-III	**Embedded Hardware Security and Hacking**: Securing external memory, JTAG/Debug port considerations, Physical attack vectors, Temper detection and logging, soldering techniques, Board analysis methodology, Component Identification, Device instrumentation, Bus monitoring and decoding, Access via JTAG	12
Unit-IV	**Embedded Software Security and Exploitation**: Fundamentals of embedded software security, Common firmware vulnerabilities, Software vulnerabilities in ARM/MIPS/etc., Embedded code vulnerabilities, Assembly code analysis, Exploitation techniques on ARM/MIPS/x86, Defenses against ARM exploits, Security practices for embedded software, Defensive software architectures, Defensive hardware interfaces	15

Self-Study:
The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content.

Suggested Readings/ References:

1. Mohammadm Tehranipoor, Cliff Wang, Introduction to Hardware Security and Trust, Springer
2. David Kleidermacher and Mike Kleidermacher, Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development, Elsevier Science, Newnes Publication.
3. Louis Goubin and Mitsuru Matsui, Cryptographic Hardware and Embedded Systems - CHES 2006, Springer
4. Colin O'Flynn and Jasper van Woudenberg, The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks, No Starch Press

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Simulate Malware attacks on embedded systems and implement protective measures.	04
2	Simulate Brute-force attacks on embedded systems and implement protective measures.	04
3	Simulate Memory Buffer Overflow attacks on embedded systems and implement protective measures.	06
4	Simulate Man in the Middle attack on embedded systems and implement protective measures.	04
5	Simulate Domain Name System (DNS) poisoning attacks on embedded systems and implement protective measures.	04
6	Simulate Distributed Denial of Service (DDoS) attacks on embedded systems and implement protective measures.	04
7	Simulate Session Hijacking attacks on embedded systems and implement protective measures.	04