NIRMA UNIVERSITY

Institute:	Institute of Technology, School of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	6CS261ME25
Course Title:	Embedded System and Security
Course Type:	Department Elective-III
Year of Introduction:	2025-26

Credit Scheme

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

Course Learning Outcomes (CLO):

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

1. explain the core concepts related to embedded system security (BL1)
2. explain the security and trust aspects of the embedded system (BL2)
3. exploit the vulnerabilities related to embedded systems using state-of-the-art tools and technologies (BL3)
4. apply countermeasures against the introduced attacks. (BL3)

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	04
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	08
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	08
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	10

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. Tehranipoor, Mohammad; Wang, Cliff, 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, Springer-Verlag Berlin and Heidelberg GmbH & Co.

Suggested List of Experiments:

Sr. No.	Name of Experiments/Exercises	Hours
1	Blinking LEDs Using a Microcontroller	2
2	Reading Sensor Data Using I2C Communication	2
3	Interrupt Handling in Embedded Systems	4
4	Secure Boot Implementation	4
5	Reverse Engineering with JTAG	4
6	Cryptographic Hashing for Data Integrity	4
7	Implementing Stack Canaries for Buffer Overflow Protection	2
8	Firmware Vulnerability Analysis Using Binwalk	4
9	Bus Monitoring and Decoding Using Logic Analyzers	4
10	Simulating a Fault Injection Attack on an Embedded System.	2