NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	3CSDE353
Course Title:	Embedded System Security
Course Type:	(□ Core/ □ Value Added Course / √ **Department Elective** / □ Institute Elective/ □ University Elective/ □ Open Elective / □ Any other)
Year of Introduction:	2022-23

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

Course Learning Outcomes (CLOs):

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

1. explain the basics of embedded firmware, hardware and software vulnerabilities and their causes (BL2)
2. make use of tools and technologies to exploit the vulnerabilities related to embedded systems (BL3)
3. develop appropriate countermeasures against the introduced attacks (BL6)
4. design hardware-based trust platforms and implement physically Unclonable functions (BL6)

Syllabus: **Total Teaching hours: 45**

Unit	Syllabus	Teaching hours
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	15

for embedded software, Defensive software architectures, Defensive hardware interfaces

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

Suggested Readings/ References:

1. Tehranipoor, Mohammad; Wang, Cliff (Eds.), 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

Suggested List of Experiments:

Sr No.	Title	Hours
1	Simulate Malware attack on embedded systems and implement protective measures.	04
2	Simulate Brute-force attack on embedded systems and implement protective measures.	04
3	Simulate Memory Buffer Overflow attack 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 attack on embedded systems and implement protective measures.	04
6	Simulate Distributed Denial of Service (DDoS) attack on embedded systems and implement protective measures.	04
7	Simulate Session Hijacking attack on embedded systems and implement protective measures.	04