Nirma University

Institute of Technology, School of Technology

MTech Computer Science and Engineering

Semester – II

L	T	P	C
3	0	2	4

Course Code	6CS261
Course Name	Embedded System Security

Course Learning Outcomes (CLOs):

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

1. comprehend the basics of embedded firmware, hardware and software vulnerabilities and their causes
2. identify the vulnerabilities related to embedded systems using state of the art tools and technologies
3. understand and apply countermeasures against the introduced attacks

Syllabus:

Teaching Hours

Unit I **5**

Introduction to Embedded Systems: Embedded hardware units, Embedded system software, Device drivers and interrupt services, Inter-process communication and synchronization of processes

Unit II **10**

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

Unit III **15**

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

Unit IV **15**

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

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.

Laboratory Work:

Laboratory work will be based on above syllabus with minimum 6 experiments to be incorporated.

Suggested Readings^:

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, Springer-Verlag Berlin and Heidelberg GmbH & Co. KG

L=Lecture, T=Tutorial, P=Practical, C=Credit

^this is not an exhaustive list