राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUE OF TECHNOLOGY PATNA
संगणक विज्ञान एंव अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना-८००००५, बिहार / ASHOK RAJPATH, PATNA-800005, BIHAR
Phone No.: 0612-2372715, 2370419, 2370843, 2371929 Ext- 200, 202 Fax-0612-2670631 Website: www.nitp.ac.in

No:- **Date:**

CSX4268: Embedded Systems and Hardware Security

L-T-P-Cr: 3-0-0-3

Pre-requisites: None

Objectives/Overview:

- Explain the concepts, issues, principles, and mechanisms in embedded systems security such as embedded security trends, software and hardware vulnerabilities, physical attacks and security policies.
- Design and analyse secure practical embedded systems with security as a design metric, not as an afterthought
- Protection of the design intellectual property against piracy and tampering
- Detection and isolation of hardware Trojans

Course Outcomes:
At the end of the course, a student should:

Sl. No	Outcome	POs
1.	Describe the vulnerabilities in the current embedded systems design flow	PO1, PO2, PO6
2.	Recognize common vulnerabilities and attacks on embedded communication protocols	PO1, PO2, PO10
3.	Integrate security as a design metric in the constraints of embedded device performance	PO3, PO5, PO12
4.	Develop defence mechanisms for embedded hardware	PO3, PO4, PO12

Syllabus:
UNIT I: Embracing Embedded Systems Security: Introduction to embedded systems, Embedded system trends, Buffer overflow exploits, Mitigation of buffer overflow attacks, Return-to-libc attack

UNIT II: Software Security, Embedded Cryptography: Secret key cryptography, public key cryptography, hash functions, authentication techniques, etc., Key management for embedded systems

UNIT III: Data Protection Protocols for Embedded Systems: Data-in-motion protocols: IP-based network security, Data-at-rest protocols, Protecting against Scan-based Side Channel Attacks, Basics of PCB Security, Counterfeit Detection and Avoidance

UNIT IV: Hardware Security: Hardware Trojans: IC Trust (Taxonomy and Detection), Basics of VLSI Design and Test, Security Based on Physically Uncolorability and Disorder, Hardware Metering, Watermarking of HW Ips, Physical Attacks and Tamper Resistance, Fault Injection Attacks, Security of RFID Tags

UNIT V: Smart Home Security and Privacy: Vulnerability analysis, Countermeasures

UNIT IV: Other Emerging Research Topics: Implantable medical device security, Security and privacy vulnerabilities of in-car wireless systems, RFID security , GPS spoofing and countermeasures, Wireless electronic warfare: jamming and anti-jamming techniques, Smartphone security

Textbook:

1. David Kleidermacher and Mike Kleidermacher, Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development, 1st Edition, Newnes, 2012.
2. Wenliang Du. Computer Security: A Hands-on Approach. 1st Edition, 2017.
3. M. Tehranipoor and C. Wang (Eds.), Introduction to Hardware Security and Trust, Springer, 2011
4. Software: Xilinx ISE package, Synopsys Verilog simulation package and HSpice, Cadence Design System,
5. Programming and Scripting Software (Matlab, Python, C/C++)