राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUTE 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:**

CSX4205: Wireless & Mobile security

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

Pre-requisites: Prior knowledge of fundamentals of wireless networks and mobile communication.

Objectives/Overview: This course will address various issues (attacks and defense strategies) in wireless and mobile security, including WEP and WPA, wireless jamming attacks, device fingerprinting, key management, location based access control, location privacy, wireless paring, mobile health security, vehicle network security, RFID hacking and authentication, smartphone system security, etc. It is intended for Master or Doctoral students who are interested in the current development of wireless and mobile security.

Course Outcomes – After completing this course, students should:

S.NO	Outcome	Level of Attainment
CO-1	Familiarize with the issues and technologies involved in designing a wireless and mobile system	Remember, Understand
CO-2	Understanding of the various way through which wireless networks can be attacked and tradeoffs in protecting networks.	Remember, Understand
CO-3	Design and implement wireless security protocols for source authentication, message integrity, message flow confidentiality, and anonymity.	Apply, Analyze, Evaluate
CO-4	Relate with new Threats, Vulnerabilities and Countermeasures in mobile networks.	Create

Course Outcomes–Cognitive Levels–Program Outcomes Matrix –
[H: High relation (3); M: Moderate relation (2); L: Low relation (1)]

Course Outcomes	Program Outcomes											
	PO-1 (Engineering knowledge)	PO-2 (Problem analysis)	PO-3 (Design/ development of solutions)	PO-4 (Conduct investigations of complex problems)	PO-5 (Modern tool usage)	PO-6 (The engineer and society)	PO-7 (Environment and sustainability)	PO-8 (Ethics)	PO-9 (Individual and team work)	PO-10 (Communication)	PO-11 (Project management and finance)	PO-12 (Life-long learning)
CO-1	H	M	H	L	H	M	M	M	H	H	M	M
CO-2	M	H	H	M	H	M	M	L	L	M	M	H
CO-3	H	M	H	H	H	M	M	H	M	M	H	H
CO-4	H	H	L	L	H	M	M	M	H	H	M	M

UNIT I: **Lectures: 6**

Overview of Wireless LAN physical components Wireless LAN topologies and technologies 802.11 a/b/g/n/ac Features, Understanding, Building and Configuring Wireless Networks Configure and install wireless adapters, access points, bridges and antennas, security features of 802.11 Wireless networks.

UNIT II: **Lectures: 8**

Wireless Application Protocol Overview, Wireless Transport layer security, WAP End-to-End Security, PSK Authentication, TKIP Encryption and AES-CCMP Encryption, key management in wireless network.

UNIT III: **Lectures: 8**

Vulnerabilities in Cellular Services, Cellular Jamming Attacks & Mitigation, Wireless Jamming Attacks, Security in Cellular VoIP Services, Mobile application security

UNIT IV: **Lectures: 8**

Enterprise Wireless Security, IEEE.11, Enterprise Wireless Security Devices (Thin Access Point) Wireless VLANs, Security threats and vulnerabilities in Wireless networks, Vulnerabilities of IEEE.11 Security, MAC Address Filtering Weaknesses, hacking Personal Wireless Security, WEP, WPA1 and WPA2, Caffe Latte Attack Basics, Caffe Latte Attack Demo , Koreks

Chopchop Attack, Fragmentation And Hirte Attack, Cracking PEAP Hotspot Attacks, Hacking Isolated Clients

UNIT V: **Lectures: 12**

Overview of WLAN security, Mobile IP security -, Attacks on 802.11 networks, Introduction/overview of ad hoc networks, Trust & reputation in ad hoc networks , Secure MANET routing, Node replication attacks, Collaborative cross-layer attacks, MAC misbehavior in MANETs, Security in hybrid systems, Location security & privacy , Location security & privacy, Vehicle Network Security, RFID Hacking and Authentication, Smartphone System Security, Smart Grid Security.

Text Book/Reference Books:

1. 802.11 Wireless Networks: The Definitive Guide by Matthew Gast, O'Reilly Media
2. Next Generation Wireless LANs: 802.11n and 802.11ac by Eldad Perahia and Robert Stacey, Cambridge University Press
3. Controller-Based Wireless LAN Fundamentals: An end-to-end reference guide to design, deploy, manage, and secure 802.11 wireless networks by Jeff Smith, Jake Woodhams, Robert Marg, Cisco press14
4. Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions by Joshua Wright , Johnny Cache, McGraw Hill.
5. BackTrack 5 Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran