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:

CSX4184: Network Security

L-T-P-Cr: 2-0-2-3

Pre-requisites: Prior knowledge of fundamentals of computer networks, Network Protocols.

Objectives/Overview:

- To impart knowledge of network security in the day to day life.
- To make students understand the concepts symmetric cryptography, asymmetric cryptography, and digital signature.
- To impart ability to design and implement of Virtual Private Networks, intrusion detection systems.
- To make students aware of common network vulnerabilities and attacks, defense mechanisms against network attacks.

Course Outcomes:

At the end of the course, a student should:

Sl. No	Outcome	Mapping to PO
1.	Recall basic concepts of Cryptographic Protocols	PO2, PO3
2.	Explain technologies behind Security mechanisms like Firewall, IDS	PO2, PO3
3.	Describe Network Security Protocols for privacy, source authentication, message integrity, message flow confidentiality, and anonymity	PO2, PO3,PO4
4.	Relate Threats, Vulnerabilities, Attack vectors and their counter measures	PO2, PO3

UNIT I: **Lectures: 4**

Computer Security concepts, OSI security Architecture, Security attacks, Security Services, security Mechanisms, model of network security, standards, Physical Layer Security, network device security.

UNIT II: **Lectures: 6**

Symmetric encryption Principles, Block cipher algorithms, random and pseudorandom numbers, stream ciphers and RC4, block cipher modes, secure hash functions, message authentication codes, public-key-cryptography principles, digital signature, access control .

UNIT III: **Lectures: 8**

Key distribution and user authentication, Kerberos, X.509 Certificates, federated identity management, web security considerations, Secure Socket layer, transport layer security, HTTPS 160, Secure Shell(SSH), IEEE 802.11i Wireless LAN Security, wireless application protocol overview, Wireless transport layer security, WAP end-to-end security.

UNIT IV: **Lectures: 8**

Electronic mail security , Pretty good privacy, S/MIME, Domain keys Identified Mail, IP Security overview, IP security Policy, Encapsulating security payload, combining security association, Internet key exchange, DNSSec, eSMTPS, TCP session hijacking, ARP attacks, route table modification, UDP hijacking, and man-in-the-middle attacks.

UNIT V: **Lectures: 6**

System Security- Types of malicious software, viruses, worms, DoS, DDoS, BOF, countermeasures, IDS concepts, IDS types and detection models, IDS features, IDS deployment considerations, Firewalls characteristics, Types of Firewalls, Firewall location and Configuration.

UNIT VI: **Lectures: 7**

Voice over IP (VoIP) and PBX security, VoIP components, VoIP vulnerabilities and countermeasures, securing a PBX, Proxy or application level gateways as security devices, VPN

UNIT VII: **Lectures: 3**

Privacy protection and anonymity services, Electronic payment system.

Text/Reference Books:

1. “Network Security Essentials: Applications and Standards” by William Stallings, Pearson
2. “Network Security private communication in a public world”, C. Kaufman, R. Perlman and M. Speciner, Pearson
3. LAN Switch Security: What Hackers Know About Your Switches, 1st Ed. (2007), by Eric Vyncke and Christopher Paggen.
4. “Designing Network Security”, Merike Kaeo, 2nd Edition, Pearson Books
5. “Building Internet Firewalls”, Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2nd Edition, Oreilly publisher
6. “Practical Unix & Internet Security”, Simson Garfinkel, Gene Spafford, Alan Schwartz, 3rd Edition, O’reilly publisher