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:

CSXX1921: ***Computer Systems and Security*** **L-T-P-Cr: 3-0-0-3**

Pr-requisites:

- **Computer Networks**
- **Programming in C or equivalent**
- **Web Programming**

Course Outcomes:

At the end of the course, a student should have:

Sl. No.	Outcome	Mapping to POs
1.	Ability to discover bugs that pose cyber security threats, explain and recreate exploits of such bugs in realizing a cyber attack on such software, and explain how to fix the bugs to mitigate such threats	PO2, PO3,PO4
2.	Ability to discover and realize cyber security holes in standard networking protocols, both in network architecture, standard protocols (such as TCP/IP, ARP, DNS, Ethernet, BGP etc), explain mitigation methods and revisions of standards based on cyber threats.	PO3,PO4
3.	Ability to explain and simulate mobile software / OS bugs posing cyber security threats, explain and recreate exploits, and explain mitigation techniques.	PO3,PO4
4.	Ability to discover and Articulate threats in SCADA and Critical Infrastructure	PO1,PO5

Unit 1: Software and System Security

- Control hijacking attacks and prevention – buffer overflow, integer overflow, bypassing browser memory protection;
- Tools and techniques for writing robust application software
- Security vulnerability detection tools, and techniques – program analysis (static, concolic and dynamic analysis)
- Privilege, access control, and Operating System Security
- Exploitation techniques, and Fuzzing

12 Lectures

Unit 2: **Network Security & Web Security**

- Security Issues in TCP/IP – TCP, DNS, Routing (Topics such as basic problems of security in TCP/IP,, IPsec, BGP Security, DNS Cache poisoning etc)

- Network Defense tools – Firewalls, Intrusion Detection, Filtering
- DNSSec, NSec3, Distributed Firewalls, Intrusion Detection tools
- Threat Models, Denial of Service Attacks, DOS-proof network architecture
- Security architecture of World Wide Web, Security Architecture of Web Servers, and Web Clients
- Web Application Security – Cross Site Scripting Attacks, Cross Site Request Forgery, SQL Injection Attacks
- Content Security Policies (CSP) in web
- Session Management and User Authentication, Session Integrity
- Https, SSL/TLS
- Threat Modeling, Attack Surfaces, and other comprehensive approaches to network design for security

16 Lectures

Unit 3: **Security in Mobile Platforms**

- Android vs. ioS security model, threat models, information tracking, rootkits
- Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities
- Viruses, spywares, and keyloggers and malware detection

6 Lectures

Unit 4: Introduction to Hardware Security

- Threats of Hardware Trojans and Supply Chain Security
- Side Channel Analysis based Threats, and attacks

4 Lectures

Unit 5: Issues in Critical Infrastructure and SCADA Security

- Security issues in SCADA
- IP Convergence Cyber Physical System Security threats
- Threat models in SCADA and various protection approaches
- Machine learning and SCADA Security

4 Lectures

Text Books:

Course will be primarily based on the various publication in the domain and same will be shared with the class before the commencement of the semester.