राष्ट्रीय प्रौद्योगिकी संस्थान जमशेदपुर
NATIONAL INSTITUTE OF TECHNOLOGY JAMSHEDPUR
(An Institution of National Importance under MHRD, Government of India)

Department of Computer Applications

Spring Semester 2019-20

Course File

Course Code : CA4202
Course Title : Network Security
Batch : M. Tech (ISSE) II Semester
Faculty In-charge: Dr. Alekha Kumar Mishra
E-mail : alekha.ca@nitjsr.ac.in
Contact number : 8249803116

Course Description: The course covers theories and concepts of computer security, focusing in particular on the security aspects of the networks and the Internet. It surveys cryptographic tools used to provide security, such as shared key encryption, public key encryption, key exchange, digital signature, and entity authentication . It then studies how these tools are utilized in the internet protocols and applications such as SSL/TLS, IPSEC, Kerberos, PGP, S/MIME etc. System security issues, such as viruses, intrusion, and other cyberthreats will also be discussed with threat analysis.

Course Objectives:

i) Review the issues involved in approaches key distributions and analyze the risks involved.
ii) Identify the major types of threats to information security and the associated attacks
iii) Study the methods for remote user/entity authentication using cryptographic techniques.
iii) Learn and implement the concepts of securing computer network protocols, based on the application of cryptography techniques.

Course Outcomes:

i) Develop strategies to protect organization information assets from common attacks.
ii) Learn how security policies, standards and practices are developed.
iii) Learn the role of cryptography in network security and their implementation in various network protocols.
iv) Learn and use of authentication protocols work and the role of digital signatures in generating digital certificates.
v) Learn and analyze the working principles of secure protocol layers such as IPSec, TLS/SSL, PGP and S/MIME.

Text / Reference Books:

1) “Cryptography and Network Security: Principles and Practice” by William Stallings, 7th Edition, Pearson
2) “Cryptography and Network Security” by Behrouz A Forouzan and Debdeep Mukhopadhyay, McGraw Hill
3) “Cryptography and Network Security” by Atul Kahate

Course Plan:

Lecture No	Topics to be covered	Refer to Books (References)
1	Course overview, objective and requirements	T2
2	Network Security Requirements	T2
3-4	Security Threats in Networks	T1, Internet
5	Entity Authentication Techniques	T2
6	Password based authentication	T2
7-8	Challenge-Response protocols	T2
9-10	Zero-knowledge protocols	T1
11- 12	Symmetric key management & distribution	T1
12-13	Public key distribution	T1 & T2
14	Public key Certificates	T1
15	X.509 Certificates	T1
16	Certificate Revocation	T1
17	Public key infrastructure	T1 & T2
18 - 19	KERBEROS	T1 & T2
20-26	TLS : Introduction, Architecture, Session parameters, Record Protocol, Handshaking protocol,	T1 & T2
27	Secure Shell	T1
28 - 34	IPSec : Operation modes, AH, ESP, Security Associations, IPSec Policies	T2
35- 37	Internet Key Exchange (IKE)	T2
38	Security in Application Layer	T1
39	E-mail Security	T1
40- 44	PGP : Introduction, Scenarios, Certificates, Key rings, Packet and Message	T2
45 - 47	S/MIME	T1 & T2
48 -50	Revision	

Evaluation Scheme:

S.No.	Evaluation Component	Weightage	Nature of Component
1	Mid-term Examination	30%	Closed book
2	End-term Examination	50%	Closed book
3	Teacher’s Assessment	20%	Programming Tasks, Presentation, & Attendance.

Consultation Hours: Monday 2 PM - 4 PM and Thursday 1 PM to 3 PM

Dr. Alekha Kumar Mishra.