DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

COURSE PLAN – PART I			
Course Title	**Network Security**		
Course Code	**CS652**	**No. of Credits**	**3**
Course Code of Pre-requisite subject(s)			
Session	**Jan. 2018**	**Section (if, applicable)**	**Single**
Name of Faculty	**Dr. S. Selvakumar**	**Department**	**Computer Science and Engineering**
Email	**ssk@nitt.edu**	**Telephone No.**	**0431 – 2503239**
Name of Course Coordinator(s) (if, applicable)	**Dr. S. Selvakumar**		
E-mail	**ssk@nitt.edu**	**Telephone No.**	**0431 - 2503239**
Course Type	**Elective course**		

Syllabus (approved in BoS)

Unit -I

Overview of Network Security, Security services, attacks, Security Issues in TCP/IP suite-Sniffing, spoofing, buffer overflow, ARP poisoning, ICMP Exploits, IP address spoofing, IP fragment attack, routing exploits, UDP exploits, TCP exploits.

Unit-II

Authentication requirements, Authentication functions - Message Authentication Codes - Hash Functions - Security of Hash Functions and MACs - MD5 message Digest algorithm - Secure Hash Algorithm - RIPEMD - HMAC Digital Signatures, Authentication protocols-Kerberos, X.509.

Unit-III

IP Security-AH and ESP, SSL/TLS, SSH, Web Security-HTTPS, DNS Security, Electronic Mail Security (PGP, S/MIME).

Unit-IV

Intruders, Viruses, Worms, Trojan horses, Distributed Denial-Of-Service (DDoS), Firewalls, IDS, Honey nets, Honey pots.

Unit-V

Introduction to wireless network security, Risks and Threats of Wireless networks, Wireless LAN Security (WEP, WPA).

COURSE OBJECTIVES

- To understand the network security, services, attacks, mechanisms, types of attacks on TCP/IP protocol suite.
- To comprehend and apply authentication services, authentication algorithms
- To comprehend and apply network layer security protocols, Transport layer security

protocols, Web security protocols.

- To understand the wireless network security threats.

COURSE OUTCOMES (CO)

- Be able to determine appropriate mechanisms for protecting the network.
- Design a security solution for a given application, system with respect to security of the system

Course Outcomes	Aligned Programme Outcomes (PO)							
	P0-1	P0-2	P0-3	P0-4	P0-5	P0-6	P0-7	P0-8
1. Ability to comprehend fundamental principles	B	S	B	S	B	S	S	B
2. Ability to apply theoretical concepts in practical scenarios	S	B	M	B	S	S	S	B
3. Ability to solve numerical problems in Cryptography and network security	B	S	B	M	S	S	S	M

S=0.6 M=0.4 B=0.0

COURSE PLAN – PART II

COURSE OVERVIEW

Network Security course deals with the issues and challenges of securing the network protocols, various attack definitions, and their solutions. Further, it also deals with the issues and challenges of securing the information and the solutions to overcome them.

COURSE TEACHING AND LEARNING ACTIVITIES

S. No.	Week/Contact Hours	Topic	Mode of Delivery
		Unit 1	
1.	Week 1	Overview of Network Security	Pen-Board, PPT
2.	Week 1	Security services, attacks, Security Issues in TCP/IP suite	Pen-Board, PPT
3.	Week 1	Sniffing, spoofing, buffer overflow	Pen-Board, PPT
4.	Week 2	ARP poisoning, ICMP Exploits	Pen-Board, PPT
5.	Week 2	IP address spoofing, IP fragment attack	Pen-Board, PPT
6.	Week 2	Routing exploits, UDP exploits	Pen-Board, PPT
7.	Week 3	TCP exploits	Pen-Board, PPT
		Unit 2	
8.	Week 3	Authentication requirements, Authentication functions	Pen-Board, PPT
9.	Week 3	Message Authentication Codes	Pen-Board, PPT
10.	Week 4	Hash Functions	Pen-Board, PPT
11.	Week 4	Security of Hash Functions and MACs	Pen-Board, PPT
12.	Week 4	MD5 message Digest algorithm	Pen-Board, PPT
13.	Week 5	Secure Hash Algorithm	Pen-Board, PPT
14.	Week 5	RJPEMD, HM AC Digital Signatures	Pen-Board, PPT
15.	Week 5	Authentication protocol s-Kerberos, X.509	Pen-Board, PPT
		Unit III	
16.	Week 6	IP Security	Pen-Board, PPT
17.	Week 6	AH and ESP	Pen-Board, PPT

18.	Week 6	SSL/TLS	Pen-Board, PPT
19.	Week 7	SSH	Pen-Board, PPT
20.	Week 7	Web Security	Pen-Board, PPT
21.	Week 7	HTTPS	Pen-Board, PPT
22.	Week 8	DNS Security	Pen-Board, PPT
23.	Week 8	Electronics Mail Security (PGP, S/MIME)	Pen-Board, PPT
		Unit IV	
24.	Week 8	Intruders, Viruses	Pen-Board, PPT
25.	Week 9	Worms	Pen-Board, PPT
26.	Week 9	Trojan horses	Pen-Board, PPT
27.	Week 9	Distributed Denial-Of-Service (DDoS)	Pen-Board, PPT
28.	Week 10	Firewalls	Pen-Board, PPT
29.	Week 10	IDS	Pen-Board, PPT
30.	Week 10	Honey nets, Honey pots	Pen-Board, PPT
		Unit V	
31.	Week 11	Introduction to wireless network security	Pen-Board, PPT
32.	Week 11	Risks of Wireless networks	Pen-Board, PPT
33.	Week 11	Threats of Wireless networks	Pen-Board, PPT
34.	Week 12	Wireless LAN Security	Pen-Board, PPT
35.	Week 12	WEP	Pen-Board, PPT
36.	Week 12	WPA	Pen-Board, PPT

COURSE ASSESSMENT METHODS (shall range from 4 to 6)

S. No.	Mode of Assessment	Week/Date	Duration	% Weightage
1	1st cycle test	5th week	1 hour	20
2	2nd cycle test	9th week	1 hour	20
3	Seminar/Term project	12th week	demo	10
CPA	Compensation Assessment*	12th week	1 hour	20
4	Final Assessment *	13th week	3 hours	50

***mandatory; refer to guidelines on page 4**

COURSE EXIT SURVEY (mention the ways in which the feedback about the course shall be assessed)

Student feedback form will be collected at the end of the course through MIS. Further the feedback from students will be collected in class committee meetings.

COURSE POLICY (preferred mode of correspondence with students, policy on attendance, compensation assessment, academic honesty and plagiarism etc.)

MODE OF CORRESPONDENCE (email/ phone etc)

ssk@nitt.edu
0431 – 2503239

ATTENDANCE

75% mandatory

COMPENSATION ASSESSMENT

Will be given for genuine medical reasons.

ACADEMIC HONESTY & PLAGIARISM

If found to practice any sort of plagiarism severe penal action will be initiated.

ADDITIONAL INFORMATION

Text Books

1. Yang Xiao and Yi Pan, "Security in Distributed and Networking Systems", World Scientific, 2007, Chapter I.
2. W. Stallings, "Cryptography and Network Security: Principles and Practice", 5/E, Prentice Hall, 2013.
3. Aaron E. Earle, "Wireless Security Handbook", Auerbach publications, Taylor & Francis Group, 2006.
4. Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill, 2003.

FOR APPROVAL

S. Selvakumar

Course Faculty S. SELVAKUMAR **CC-Chairperson** S. Selvakumar 31/01/18 **HOD** 31/1/2018