



**Department of Computer Science and Engineering**  
**National Institute of Technology Tiruchirappalli**

1. Course Outline			
Course Title	Network Security		
Course Code	CS652		
Department	CSE	No. of Credits	3
Pre-requisites Course Code	Advanced Network Principles and Protocols	Faculty Name	Dr. S. Selvakumar
E-mail	ssk@nitt.edu	Telephone No.	0431 - 2503239
Course Type	Elective Course		

**2. 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.

- 3. 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.

4. Course Outcomes (CO)	Aligned Programme Outcomes (PO)							
	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6	PO-7	PO-8
Ability to comprehend fundamental principles	B	S	B	S	B	S	S	B
Ability to apply theoretical concepts in practical scenarios	S	B	M	B	S	S	S	B
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

### 5. Course Teaching and Learning Activities

L.No.	Title	Mode of delivery
<b>UNIT I</b>		
1.	Overview of Network Security	Pen-Board, PPT
2.	Security services, attacks, Security Issues in TCP/IP suite	Pen-Board, PPT
3.	Sniffing, spoofing, buffer overflow	Pen-Board, PPT
4.	ARP poisoning, ICMP Exploits	Pen-Board, PPT
5.	IP address spoofing, IP fragment attack	Pen-Board, PPT
6.	Routing exploits, UDP exploits	Pen-Board, PPT
7.	TCP exploits	Pen-Board, PPT
<b>UNIT II</b>		
8.	Authentication requirements, Authentication functions	Pen-Board, PPT
9.	Message Authentication Codes	Pen-Board, PPT
10.	Hash Functions	Pen-Board, PPT
11.	Security of Hash Functions and MACs	Pen-Board, PPT
12.	MD5 message Digest algorithm	Pen-Board, PPT
13.	Secure Hash Algorithm	Pen-Board, PPT
14.	RIPEMD, HMAC Digital Signatures	Pen-Board, PPT
15.	Authentication protocols-Kerberos, X.509	Pen-Board, PPT
<b>UNIT III</b>		
16.	IP Security	Pen-Board, PPT
17.	AH and ESP	Pen-Board, PPT
18.	SSL/TLS	Pen-Board, PPT
19.	SSH	Pen-Board, PPT
20.	Web Security	Pen-Board, PPT
21.	HTTPS	Pen-Board, PPT
22.	DNS Security	Pen-Board, PPT
23.	Electronic Mail Security (PGP, S/MIME)	Pen-Board, PPT

UNIT IV		
24.	Intruders, Viruses	Pen-Board, PPT
25.	Worms	Pen-Board, PPT
26.	Trojan horses	Pen-Board, PPT
27.	Distributed Denial-Of-Service (DDoS)	Pen-Board, PPT
28.	Firewalls	Pen-Board, PPT
29.	IDS	Pen-Board, PPT
30.	Honey nets, Honey pots	Pen-Board, PPT
UNIT V		
31.	Introduction to wireless network security	Pen-Board, PPT
32.	Risks of Wireless networks	Pen-Board, PPT
33.	Threats of Wireless networks	Pen-Board, PPT
34.	Wireless LAN Security	Pen-Board, PPT
35.	WEP	Pen-Board, PPT
36.	WPA	Pen-Board, PPT

#### 6. Course Assessment Methods

Attendance : 75% mandatory

Evaluation Methods : CT1 – 20%  
 CT2 – 20%  
 Seminar/Term Project – 10%  
 End Sem – 50%

Feedback Methods : i) Before I CT  
 ii) Before II CT  
 iii) Before End Sem

**7. Essential Readings (Textbooks, Reference books, Websites, Journals, etc.)**

**Text Books**

1. Yang Xiao and Yi Pan, "Security in Distributed and Networking Systems", World Scientific, 2007, Chapter 1.
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 Senate's Consideration**

*S. Selvakumar*  
Course Faculty  
02 01 17

*CHS*  
31/1/17  
CC Chairperson

*[Signature]*  
HOD 31/1/2017