Department of Computer Science and Engineering

NITK, Surathkal

CS851 - Network Security [M. Tech-ISE]

(Syllabus and Assessment Plan)

Semester: II [ISE] **Academic Year:** 2019-20 **Credits:** (3-0-2) 4

A. Theory Syllabus

1. Introduction: **- 6 hrs.**

Attacks, services and mechanisms, TCP/IP – Protocol Stacks.

2. Encryption Algorithms:

Classical Encryption Techniques, Block Ciphers and DES, AES, Block Cipher Operations, Public key Cryptography, RSA, Diffie-Hellman Key Exchange, Elliptic Curve cryptography, Hash Functions, Message Authentication Code, Digital Signature, Key management and distribution, User Authentication. **- 8 hrs.**

3. System Security: **- 5 hrs.**

Backups, integrity management, protecting against programmed threats viruses and worms, physical security, Personnel security.

4. Network security: **- 8 hrs.**

Protection against eavesdropping, Security for modems, IP security, Web security, Electronic mail security, Authentication applications.

5. Security tools: **- 4 hrs.**

Firewalls, Wrappers, proxies, discovering a break-in Denial of service attacks and solutions. Cryptographic security tools: Kerberos, PGP (Pretty Good Privacy), SSH (Secure Shell), SRP (Secure Remote Password), OPIE (One time Passwords In Everything).

Text Books:

a. William Stallings, 'cryptography and network security-principles and practice'. 6th Edition, Pearson Education, 2014.

b. Steve Burnett, Stephene Paine 'rsa security's official guide to cryptography', TMH, 2001

c. E. Nemeth, G. Snyder, S. Seenass, T. R. Hein 'Unix system administration handbook', 3rd ED, PEI.

B. Laboratory Syllabus

Tools: OpenSSL, Wireshark

Module I: Introduction to OpenSSL & exercises using OpenSSL **- 2 Lab Sessions**

Module II: Socket Programming **- 2 Lab Sessions**

a) Design UDP Client and Server to transfer a file.
   Step 1: Client sends "ls" to server
   Step 2: Client select a file
   Step 3: Selected file by the client will be sent to the client (copy-paste)
b) Design TCP Client and Server to transfer a file.
   Step 1: Client sends "ls" to server
   Step 2: Client select a file
   Step 3: Selected file by the client will be sent to the client (copy-paste)
c) Design a TCP concurrent server to convert a given text by client into upper case using multiplexing system call "select".
d) To develop a Client that contacts a given DNS Server (name to ip address mapping is present in dns.txt) to resolve a given host name. (Note: client refer dns.txt locally before request sent to DNS server)
e) Write a client and server program for Signal Handling and Handling Zombie.
f) Design TCP iterative Client and server application to reverse the given input sentence.
g) Write a daytime UDP client program using *gethostbyname* and *getservbyname*, where hostname and service name are passed through the command line.

Module III: Secured Socket Programming using OpenSSL - **4 Lab Sessions**

Module IV: Setting IPSec, TLS/SSL, Secured Mobile IPv6, Kerberos, etc. **- 2 Lab Sessions**

Module V: Security Tools – Tstat, OpenConnect, OpenDPI, Nessus, Metasploit, OpenVAS, Kismet, Zap, W3af, Vega, Bro - **2 Lab Sessions**

Module VI: Mini-Project **- 3 Lab Sessions**

Assessment Plan

(Theory : Laboratory = 75% : 25%)

Sl. No.	Item	Theory	Lab	Remarks
1	End-Semester	45%	-	-
2	Mid-Semester	20%	-	-
3	Quiz	10%	-	Average of two quiz
4	Mini-Project	-	10%	-
5	Mid-Semester	-	05%	-
6	Regular Lab Activity	-	10%	-

Note: Above shown syllabus and assessment plan is applicable even for all Ph. D scholar registered for CS851.

Course Instructor	Secretary	Chairman
(B. R. Chandavarkar)	(DPGC/DRPC)	(DPGC/DRPC)