GUJARAT TECHNOLOGICAL UNIVERSITY, AHMEDABAD, GUJARAT

COURSE CURRICULUM

COURSE TITLE: COMPUTER AND NETWORK SECURITY

(COURSE CODE: 3350704)

Diploma Programmes in which this course is offered	Semester in which offered
Computer Engineering	5th Semester

1. RATIONALE

Present computing era is based on internet and hence networking is an essential part of course. Prime concern is that in current advanced digital world various security threats are increasing day by day posing problems to data confidentiality, integrity and availability. This course aims at learning basic cryptography techniques and applying security mechanisms for operating systems as well as private and public network to protect them from various threats.

2. LIST OF COMPETENCIES:

The course content should be taught and implemented with the aim to develop different types of skills so that students are able to acquire following competencies:

- **Determine appropriate mechanisms for protecting networked systems by applying various cryptographic techniques.**
- **Secure the network by using firewalls on various networks in order to identify various network attacks and resolve them**.

3. COURSE OUTCOMES:

The theory should be taught and practical should be carried out in such a manner that students are able to acquire different learning out comes in cognitive, psychomotor and affective domain to demonstrate following course outcomes.

i. Identify and describe the common types of security threats are risks to the Computer Systems and the nature of common Information hazards.
ii. Identify the potential threats to confidentiality, integrity and availability of Computer Systems.
iii. Describe the working of standard security mechanisms and applied to the external and internal network.
iv. Define cryptography, describe the elements of the encryption process and select best algorithm to encrypt data and protocols to achieve Computer Security.
v. Apply accepted security policies, procedures are necessary to secure Operating Systems and applications.

4. Teaching and Examination Scheme

Teaching Scheme (In Hours)			Total Credits (L+T+P)	Examination Scheme				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	ESE	PA	ESE	PA	200
3	0	4	7	70	30	40	60	

Legends: L-Lecture; **T** – Tutorial/Teacher Guided Theory Practice; **P** -Practical; **C** – Credit **ESE** -End Semester Examination; **PA** - Progressive Assessment.

5. COURSE CONTENT DETAILS

Unit	Major Learning Outcomes (in cognitive domain)	Topics and Sub-topics
Unit – I Introduction and Security Threats:	1a.List and discuss various security terms, recent trends in computer security. 1b. Describe various types of threats that exist for computers and networks.	1.1 Threats to security : Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare
	1c. Describe simple steps to take minimize the possibility if an attack on a system.	1.2 Avenues of Attack, steps in attack
	1d. Define Security Basics.	1.3 Security Basics – Confidentiality, Integrity, Availability
	1e. Describe various types of computer and network attacks 1f. Identify various types of malicious software that exists.	1.4 Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection. Malware : Viruses, Logic bombs
Unit – II Organizational Security	2a.List & Define various human security threats. 2b. Determine ways in which users can aid security.	2.1 Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software /hardware, Access by non employees. 2.2 People as Security Tool: Security awareness, and Individual user responsibilities.
	2c. Describe physical security components that can protect any computer and network.	2.3 Physical security: Access controls Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature and writing patterns, keystrokes, Physical barriers
	2d.List potential threats on password and explain characteristics of a strong password.	2.4 Password Management, vulnerability of password, password protection, password selection strategies, components of a good password.

Unit	Major Learning Outcomes (in cognitive domain)	Topics and Sub-topics
Unit – III Cryptography and Public key Infrastructure	3a. Identify and describe types of cryptography . 3b. List and describe various Encryption Algorithms.	3.1 Introduction to Symmetric encryption & Asymmetric encryption. 3.2 Encryption algorithm / Cifer, Encryption and Decryption using: Caesar's cipher, playfair cipher, shift cipher, shift cipher, Vigenere cipher, one time pad (vermin cipher), hill cipher (for practice use small matrix and apply encryption only).
	3c. Describe transposition techniques and steganography.	3.3 Transposition techniques (rail fence), steganography
	3d. Explain Hashing and SHA-1 mechanism.	3.4 Hashing function : SHA1 (only)
	3e. Distinguish Asymmetric and Symmetric Encryption. 3f. Describe digital signature and concept of key escrow.	3.5 Asymmetric encryption: Digital Signatures, Key escrow
	3g. List the basics of public key infrastructures. 3h. Describe the roles of certificate authorities and certificate repositories. 3i. Describe the role of registration authorities. 3j. Explain the relationship between trust and certificate verification. 3k. Explain use of digital certificates.	3.6 Public key infrastructures : basics, digital signatures, digital certificates, certificate authorities, registration authorities, steps for obtaining a digital certificate, steps for verifying authenticity and integrity of a certificate
	3l. Distinguish centralized and decentralized infrastructures.	3.7 Centralized or decentralized infrastructure, private key protection
	3g. List and describe trust models.	3.8 Trust Models: Hierarchical, peer to peer, hybrid
Unit IV Network security	4a. Explain working principle of FIREWALLs.	4.1 Firewalls: working, design principles, trusted systems, Kerberos.
	4b.Define, classify and	4.2 Security topologies – security zones,

Unit	Major Learning Outcomes (in cognitive domain)	Topics and Sub-topics
	describe various security topologies.	DMZ, Internet, Intranet, VLAN, security implication, tunneling.
	4c. Describe Internet Protocol Security (IPsec) and its use in securing communication.	4.3 IP security : overview, architecture, IPSec configurations, IPSec security
	4d. Explain email security.	4.4 Email security : security of email transmission, malicious code, spam, mail encryption
Unit V **Web Security**	5a. Define & list various types of IDSs. 5b. Distinguish Host-based IDS & Network-based IDS. 5c. List and describe HIDS and NIDS components. 5d. List advantages and disadvantages HIDS, NIDS	5.1 Intruders, Intrusion detection systems (IDS): host based IDS, network based IDS, logical components of IDS, signature based IDS, anomaly based IDS, network IDS components, advantages and disadvantages of NIDS, host based IDS components, advantages and disadvantages of HIDS.
	5e. List & Explain Web Security Threats. 5f. Explain securities in SSL and TLS. 5g. Explain concept of secure electronic transaction.	5.2 Web security threats, web traffic security approaches, Introduction to Secure Socket Layer (SSL) & Transport Layer Security(TLS), Concepts of secure electronic transaction

6. SUGGESTED SPECIFICATIONTABLE WITH HOURS&MARKS (THEORY)

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Introduction and Security Threats	6	4	4	4	12
II	Basics of System Security	6	4	4	4	12
III	Cryptography and Public key Infrastructure	14	6	8	8	22
IV	Network security	8	2	8	2	12
V	Web Security	8	2	8	2	12
	Total	**42**	**18**	**32**	**20**	**70**

Legends: R = Remember; U= Understand; A= Apply and above levels (Bloom's Revised Taxonomy)

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

7. SUGGESTED LIST OF EXERCISES/PRACTICALS

S. No.	Unit No.	Practical Exercises (Outcomes' in Psychomotor Domain)	Approx Hrs. required
1	I	List and practice various "net" Commands on DOS & Linux.	04
2	I	Configure a system for various security experiments.	02
3	I	Configure Web browser security settings.	02
4	I	Draw Diagram of DoS, backdoors, trapdoors.	04
5	I & II	Draw diagrams of sniffing, spoofing, man in the middle & replay attacks.	02
6	I	Draw diagram for Confidentiality, Integrity & Availability.	02
7	III	Write Ceaser's Cipher algorithm & Solve various examples based on Encryption & Decryption.	02
8	III	Write, test and debug Ceaser cipher algorithm in C/C++/Java/Python/Matlab.	02
9	III	Write algorithm/steps for Shift Cipher & solve various examples on it.	02
10	III	Write algorithm/steps for Hill Cipher and solve examples on it.	02
11	III	Write algorithm/steps for playfair cipher and solve examples on it.	02
12	III	Write algorithm/steps for Verman Cipher & solve	02

		various examples on it.	
13	III	Write algorithm/steps for Vignere Cipher & solve various examples on it.	02
14	III	Write algorithm/steps for one time pad & solve various examples on in.	02
11	III	Draw diagram of Public Key Infrastructure.	02
12	III	Draw diagram of Centralized/Decentralized Infrastructure.	02
13	III	Demonstrate cross-scripting.	02
14	IV	Draw various Security Topologies.	02
15	IV	Demonstrate traffic analysis of different network protocols using tool. i.e. Wire-shark. (Atleast one of them should be recorded and included in term work.)	04
16	IV	Demonstrate Sniffing using packet tool i.e. snort.	04
17	IV	Configure your e-mail account against various threats. i.e. spam attack, phising, spoofing etc.	04
18	V	Draw diagram Host-based Intrusion Detection System	02
19	V	Draw diagram Network-based Intrusion Detection System	02
20	V	Demonstration of SQL-Injection.	02
21	V	Demonstration of readymade encryption/decryption code	04
Total			**62**

8. SUGGESTED LIST OF STUDENT ACTIVITIES

Following is the list of proposed student activities like**:**

i. Visit to Internet Service Provider
ii. Study measures are taken by small computer industries
iii. Seminars on various security tools, algorithms from the course content
iv. Seminars on current threats on system/network

9. SPECIAL INSTRUCTIONAL STRATEGIES (if any)

The course activities include Lectures and Practical Exercises as per teaching scheme. The programmes in would be executed during practical's sessions. Following needs attention:

i. Concepts will be introduced in lectures using multimedia projector.
ii. Discussion
iii. Demonstrations
iv. Power point presentation for each of the software tools/algorithms
v. Practical work will be through laboratory sessions.
vi. Debate/Group Discussions for comparison of various tools and algorithms

10. SUGGESTED LEARNING RESOURCES

A) List of Books

Sr.No.	Title of Book	Author	Publication
1.	Principles Of Computer Security CompTIA Security+ And Beyond (Exam SY0-301), 3rd Edition Books	Conklin, Wm. Arthur Gregory White, Dwayne Williams, Roger Davis, Chuck Cothren, Corey Schou	Mc Graw Hill ISBN:9781259061196, 2012
2.	Cryptography and Network Security Principles and Practices	Williams Stallings	Pearson Education, Third Edition
3.	Principles of Computer Security CompTIA Security+ and Beyond Lab Manual	Vincent Nestler, Gregory White, Wm. Arthur Conklin, Matthew Hirsch, Corey Schou	Mc Graw Hill, 2010 , 9780071748568
4.	Cryptography and Network Security Principal and Practices	Atul Kahate	Tata-McGraw-Hill Sixth reprint 2006
5.	Cryptography and Network Security	B A Forouzen	TMH
6.	Computer Security Basics	Deborah Russell G.T. Gangenisr	O'Reilly publication
7.	Computer Security	Dieter Gollman	Wiley India Education, Second Edition

B) List of Major Equipment/ Instrument with Broad Specifications

i. Computer System with latest configuration and memory, laptops, servers
ii. Multimedia projector
iii. High B/W Internet Connection.
iv. Open source Free diagnostic software/tools
v. Access to library resources

C) List of Software/Learning Websites

i. Software: Wireshark Traffic Analysis/Packet Sniffing Tool, Snort Packet Sniffing tool
ii. www.securityplusolc.com.
iii. http://mercury.webster.edu/aleshunas/COSC%205130/COSC%205130%20Home.htm
iv. http://williamstallings.com/Cryptography/
v. http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf
vi. http://nptel.iitm.ac.in/courses.php?disciplineId=106
vii. Network Simulator Tool: GNS3 v0.8.5, NetSimK
viii. http://www.snort.org/docs
ix. http://manual.snort.org/node27.html
x. http://www.wireshark.org/docs/wsug_html_chunked/

xi. http://www.pearsonhighered.com/assets/hip/us/hip_us_pearsonhighered/samplechapter/0131407333.pdf
xii. http://www.cs.nyu.edu/courses/fall04/G22.2262-01/assignments/assignment4_files/Ethereal_TCP.pdf

11. COURSE CURRICULUM DEVELOPMENT COMMITTEE

Faculty Members from Polytechnics

- **Prof. P. P. Kotak,** H. O. D., Computer Department, A. V. P. T. I., Rajkot
- **Prof. K. N. Raval,** H.O.D Computer Department, R. C. Technical Institute, Ahmedabad
- **Prof. Manisha P Mehta**, Sr. Lecturer in Computer Technology, K. D. Polytechnic, Patan.
- **Prof. Sunil R. Solanki**, Lecturer in Computer Engineering, Govt. Polytechnic, Dahod.
- **Prof. Sachin D. Shah,** Lecturer in Computer Engineering, R. C. Technical Institute, Ahmedabad.

Coordinator and Faculty Members from NITTTR Bhopal

- **Dr. M. A. Rizvi,** Associate Professor, Dept. of Computer Engineering and Applications.
- **Dr. Priyanka Tripathi,** Associate Professor, Dept. of Computer Engineering and Applications, NITTTR