

COURSE NAME : COMPUTER ENGINEERING / COMPUTER TECHNOLOGY
COURSE CODE : CO/CM/CD
SEMESTER : FIFTH FOR CO/CM AND SIXTH FOR CD
SUBJECT TITLE : COMPUTER SECURITY
SUBJECT CODE : 9114

Teaching and Examination Scheme:

Teaching Scheme			Examination Scheme						
TH	TU	PR	PAPER HRS	TH	TEST	PR	OR	TW	TOTAL
03	--	--	03	80	20	--	--	--	100

Rationale:

Computer security, one of the most important and relevant area of computing today. The requirement to address security in computer system design is an important design consideration in many of today's systems. It is essential to understand various threats to secure computing and the basic security design principles and techniques developed to address these threats. The student will achieve a firm intuition about what computer security means, be able to recognize potential threats to confidentiality, integrity and availability.

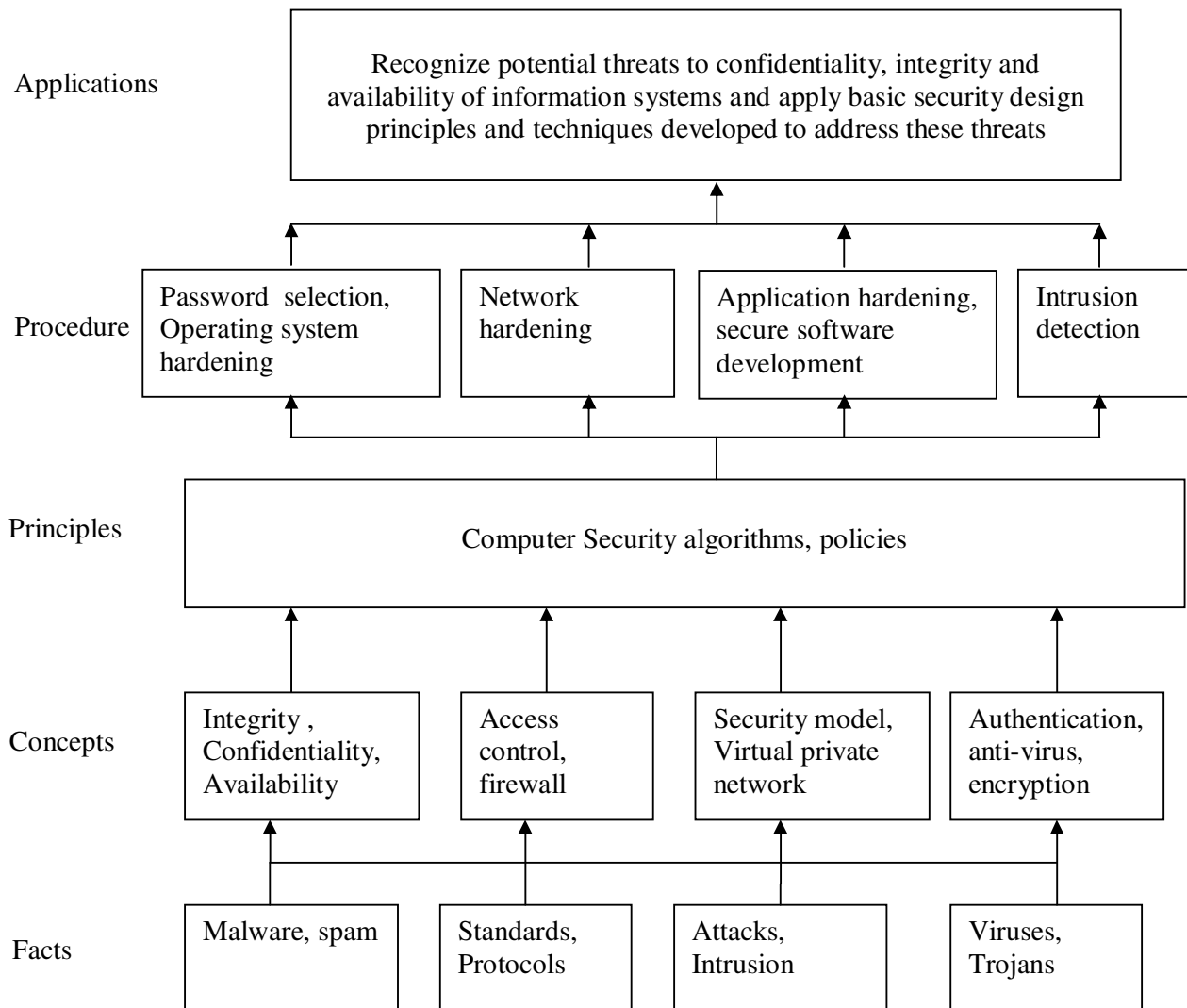
This course will introduce basic cryptography, fundamentals of computer/network security, risks faced by computers and networks, security mechanisms, operating system security, secure systems design principles, and network security principles. It will develop knowledge for security of information and information systems within organizations. It focuses on concepts and methods associated with planning, managing, and auditing security at all levels including networks

Objectives:

The students will be able to:

1. Understand the risks faced by Computer Systems and the nature of common Information hazards.
2. Identify the potential threats to confidentiality, integrity and availability of Computer Systems.
3. Understand the working of standard security mechanisms.
4. Use cryptography algorithms and protocols to achieve Computer Security.
5. Understand the threats and security mechanisms for Computer Networks.
6. Build systems that are more secure against attacks.
7. Apply security principles to secure Operating Systems and applications.

Learning Structure:



Contents: Theory

Chapter	Name of the Topic	Hours	Marks
01	<p>Introduction and Security trends</p> <p>1.1 Threats to security : Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare</p> <p>1.2 Avenues of attack, steps in attack</p> <p>1.3 Types of attack : Denial of service, backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, encryption attacks.</p> <p>Malware : Viruses, Logic bombs</p> <p>1.4 Security Basics – Confidentiality, Integrity, Availability, Operational model of Computer Security, Layers of security</p> <p>1.5 Access control : Discretionary, Mandatory, Role based</p> <p>Authentication : Certificates Tokens, Multifactor</p>	08	14
02	<p>Organizational/ Operational security</p> <p>2.1 Role of people in security : Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software / hardware, Access by non employees, Security awareness, Individual user responsibilities</p> <p>2.2 Security policies, standards, procedures and guidelines</p> <p>2.3 Physical security : Access controls</p> <p>Biometrics : finger prints, hand prints, Retina, patterns, voice patterns, signature and writing patterns, keystrokes, Physical barriers</p> <p>2.4 Social Engineering</p>	08	14
03	<p>Cryptography and Public key Infrastructure</p> <p>3.1 Encryption algorithm/Cifer, Caesar’s cipher, shift cipher, substitution software, Vigenere cipher</p> <p>3.2 Transposition techniques, Steganography</p> <p>3.3 Hashing, SHA</p> <p>3.4 Symmetric encryption, DES (Data encryption standard), Asymmetric encryption, Digital signatures, Key escrow</p> <p>3.5 Public key infrastructures : basics, digital certificates, certificate authorities, registration authorities, steps for obtaining a digital certificate, steps for verifying authenticity and integrity of a certificate</p> <p>3.6 Centralized or decentralized infrastructure, private key protection</p> <p>3.7 Trust models : Hierarchical, peer to peer, hybrid</p>	10	14

04	Network security 4.1 Firewalls : working, design principles, trusted systems, Kerberos 4.2 Security topologies – security zones, DMS, Internet, Intranet, VLAN, security implication, tunneling 4.3 IP security : overview, architecture, IPSec, IPSec configurations, IPSec security 4.4 Virtual Private Network 4.5 Email security : security of email transmission, malicious code, spam, mail encryption	08	12
05	System security 5.1 Intruders, Intrusion detection systems (IDS), host based IDS, network based IDS 5.2 Password Management, vulnerability of password, password selection strategies, components of a good password 5.3 Operating system security : Operating system hardening, general steps for securing windows operating system, Hardening Unix/Linux based operating system, updates : hotfix, patch, service pack	08	14
06	Application and web security 6.1 Application hardening, application patches, web servers, active directory 6.2 Web security threats, web traffic security approaches, secure socket layer and transport layer security, secure electronic transaction Software development : secure code techniques, buffer overflows, code injection, least privilege, good practices, requirements, testing	06	12
Total		48	80

Learning Resources:

Books:

Sr. No.	Author	Title	Publication
01	Wm. Arthur Conkin Dwayne Williams Gregory B. White Roger L. Davis Chuck Cothren	Principles of Computer Security Security + and Beyond	Mc Graw Hill Technology Education International Edition 2005
02	Dieter Gollman	Computer Security	Wiley India Education, Second Edition
03	Deborah Russell G.T.Gangenisr	Computer Security Basics	O'Reilly publication
04	William Stallings	Cryptography and Network Security Principles and Practices	Pearson Education, Third Edition
05	Atul Kahate	Cryptography and Network Security	Tata-McGraw-Hill Sixth reprint 2006