Dr.M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
UNIVERSITY

(Decl. U/S 3 of the UGC Act 1956)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

M.Tech – Information Security and Cyber Forensics (Full Time)

Curriculum and Syllabus

2013 Regulation

I SEMESTER						
S.No	**Sub.Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS13I001	Advanced Computer Networks and Security	3	0	0	3
2	MCS13I002	Introduction to Information Security	3	1	0	4
3	MCS13I003	Information Security Standards & Compliances	3	0	0	3
4	MCS13I004	Cyber Forensics Process Design	3	0	0	3
5	MCS13I005	Data Communication& Security	3	0	0	3
6	MCS13I006	Ethical Hacking and Countermeasures	3	0	0	3
7	MCS13IL01	Ethical Hacking Lab	0	0	3	1
8	MCS13IL02	Cryptography and Cryptanalysis Lab	0	0	3	1
		Total	**18**	**1**	**6**	**21**

II SEMESTER						
S.No	**Sub.Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS13I007	Data Mining & Machine Learning for Information Security	3	0	0	3
2	MCS13I008	Threats & Vulnerabilities	3	0	0	3
3	MMA130009	Mathematics for Information Security and Cyber Forensics	3	1	0	4
4	MCS13I009	Applied Cryptography	3	0	0	3
5	MCS13I010	Advanced Penetration Testing	3	0	0	3
6	MCS13IEXX	Elective I	3	0	0	3
7	MCS13IL03	Term Paper & Seminar	0	0	6	1
8	MCS13IL04	Digital Crime Investigation Lab	0	0	3	1
9	MCS13IL05	Penetration Testing & Vulnerability Assessment Lab	0	0	3	1
		Total	**18**	**1**	**12**	**22**

III SEMESTER						
S.No	**Sub.Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS13I011	Digital Forensic Investigation & Evidence Management	3	0	0	3
2	MCS13IEXX	Elective II	3	0	0	3
3	MCS13IEXX	Elective III	3	0	0	3
4	MCS13IEXX	Elective IV	3	0	0	3
5	MCS13IL06	Project Work Phase-I	0	0	6	5
		Total	**12**	**0**	**6**	**17**

IV SEMESTER						
S.No	**Sub.Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS13IL07	Project Work Phase-II	0	0	24	15
		Total	**0**	**0**	**24**	**15**

Summary of Credits:

1st Semester Credits	**21**
2nd Semester Credits	**22**
3rd Semester Credits	**17**
4th Semester Credits	**15**
Total	**75**

Elective I						
S.No	**Sub.Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS13IE01	Business Continuity & Disaster Recovery	3	0	0	3
2	MCS13IE02	Cloud Computing And Security	3	0	0	3
3	MCS13C002	Object Oriented Software Engineering	3	0	0	3
4	MCS13IE04	Unix and Linux Systems Security	3	0	0	3

Elective II						
S.No	**Sub.Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS13IE05	Virtualization Security	3	0	0	3
2	MCS13IE06	Mobile and Multimedia Security	3	0	0	3
3	MCS13IE07	Wireless Network Forensics	3	0	0	3
4	MCS13IE08	Pattern Recognition	3	0	0	3

Elective III						
S.No	**Sub.Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS13IE09	Secure Software Development Life Cycle	3	0	0	3
2	MCS13IE10	TCP / IP Design and Implementation	3	0	0	3
3	MCS13IE11	Storage Management Security	3	0	0	3
4	MCS13IE12	Information Security Risk Management and Auditing	3	0	0	3

Elective IV						
S.No	**Sub.Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS13IE13	Threat Modeling and Security Architecture Design	3	0	0	3
2	MCS13IE14	Cyber Laws	3	0	0	3
3	MCS13IE15	Virus Programming	3	0	0	3
4	MCS13IE16	Advanced Databases and Security	3	0	0	3

MCS13I001 ADVANCED COMPUTER NETWORKS AND SECURITY 3 0 0 3

OBJECTIVE:

- Understand the fundamentals of next generation computer networks,
- Learning the principles of network security
- Handling the issues such as wireless networking, current standards (e.g. Bluetooth, 802.11, UMTS, 3G), and new application areas (e.g. wireless sensor networks).

UNIT I INTERNETWORKING AND DATA SECURITY 9Hrs

Network ownership, service paradigm and performance-protocols and layering- internetworking concepts, architecture and protocols-IP internet protocol addresses-binding protocol addresses(ARP)-IP datagrams and datagrams forwarding- IP Encapsulation, fragmentation and reassembly, UDP-TCP reliable transport service, Security design issues in UDP –TCP-IP protocols.

UNIT-I I VOIP SECURITY 9Hrs

Introduction, VoIP architecture and Protocols, Threats and Attacks, VoIP Vulnerabilities, Signalling protection mechanism, Media protection mechanism, Key Management Mechanism, VoIP and Network security controls.

UNIT-III ATM 9Hrs

Protocols and Security Issues, Addressing Signaling & Routing - Header Structure - ATM Adaptation layer - Management control, Internetworking With ATM**:** LAN - IP over ATM - Multiprotocol over ATM - Frame Relay over ATM – DHCP - DNS

UNIT-IV WIRELESS NETWORKS AND SECURITY 9Hrs

Evolution Of Wireless Networks, Mobile Communications technologies- wireless channel- Network design-Ad hoc Networks-Bluetooth technology-Security aspects of Wireless Networks.

UNIT-V RECENT TRENDS 9Hrs

Optical Networks - Advanced intelligent Networks-Home networking.

Total No of Hours: 45

Reference Books:

1. Walrand.J. Varaiya, (2000) *High Performance Communication Network*, (2nd ed.),Morgan Kauffman – Harcourt AsiaPvt Ltd,

2. William Stallings (2000) *ISDN & Broadband ISDN with frame Relay & ATM*, (4th ed.),PHI.

3. UylessBlack(1997) *Emerging Communications Technologies*,(2nd ed.), Prentice Hall

4. Bates & Donald W.Gregory ,*Voice& Data Communications Handbook*, (3rd ed.),Mc-Graw Hill

5. Peter Thermos and Ari Takanen (2007) *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures.*

MCS13I002 INTRODUCTION TO INFORMATION SECURITY 3 1 0 4

OBJECTIVE:

- Gaining knowledge about information security
- Comprehend the history of computer security and how it evolved into information security.
- Outlines the phases of the security systems development life cycle, the roles of professionals involved in information security within an organization.

UNIT 1 INTRODUCTION 12Hrs

Information Security- Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC

UNIT II SECURITY INVESTIGATION 12Hrs

Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues,

UNIT III LOGICAL DESIGN AND PHYSICAL DESIGN 12Hrs

Blueprint for Security, ISO 17799/BS 7799, NIST Models, VISA International Security Model, Design of Security Architecture, Planning for Continuity, Security Technology, IDS, Scanning and Analysis Tools, Cryptography, Access Control Devices, Physical Security, Security and Personnel.

UNIT IV CYBER FORENSICS 12Hrs

Introduction to Cyber forensics, Information Security Investigations , Corporate Cyber Forensics, Scientific method in forensic analysis, Investigating large scale Data breach cases., Analyzing Malicious software

UNIT V 12Hrs

Types of Computer Forensics Technology –Types of Vendor and Computer Forensics Services

Total No of Hours: 60

Reference Books:

1.Michael E Whitman and Herbert J Mattord, (2003)“*Principles of Information Security*”, Vikas Publishing House, New Delhi

2.Micki Krause, Harold F. Tipton, (2004)“ *Handbook of Information Security Management*”, Vol 1-3 CRC Press LLC

3.Stuart Mc Clure, Joel Scrambray, George Kurtz, (2003)“*Hacking Exposed*”, Tata McGraw-Hill

4. Matt Bishop, (2002)“*Computer Security Art and Science*”, Pearson/PHI

5.*Computer Forensics: Investigating Network Intrusions and Cyber Crime* (Ec-Council Press Series:Computer Forensics)

6.JenniferBayuk (2010)*CyberForensics: Understanding Information Security Investigations* (Springer's Forensic Laboratory Science Series

MCS13I00 INFORMATION SECURITY STANDARDS AND COMPLIANCES 3 0 0 3

OBJECTIVE:

- To understand the security basics and implementation and components of it govemance
- Detailed study of HIPAA.
- Knowledge about PCI & Octave Methods.

UNIT I: INTRODUCTION 9Hrs

Security basics, legal response to security, legal standard for compliance, developing a compliant security program, security controls, role of standards

UNIT II: IT GOVERNANCE 9Hrs

Governance and risk management, IT regulatory Compliance, Information and Continuity risk, Internal control frameworks, Project Governance, Components of IT Governance, ISO/IEC 38500, IT Governance Frameworks and Standards, The Calder- Moir Framework, Implementing IT Governance.

UNIT III: HIPAA 9Hrs

Introduction to HIPAA Essentials, Relationship between Security and Privacy, HIPAA privacy rule requirement overview, Performing a privacy rule gap Analysis and Risk Analysis, Writing effective privacy policies, HIPAA Security rule requirement overview, Performing performance rule risk analysis, Writing effective information security policies.

UNIT IV: PCI 9Hrs

Build and maintain a secure network, Protect Card holder Data, Maintain a vulnerability Management programme, Implement strong access control measures, regularly monitor and test networks, maintain an Information security policy.

UNIT V: OCTAVE 9Hrs

Introduction, The OCTAVE Method, Variations in the OCTAVE approach.

Total No of Hours: 45

Reference Books:

1. Thomas J. Smedinghoff ,*Information Security Law: The Emerging Standard for Corporate Compliance*
2. Kevin Beaver , Rebecca Herold, *The Practical Guide to HIPAA Privacy and Security Compliance*
3. James M Barrow,*PCI Compliance: Level 1 Merchant Guide for DSS* version 2.0
4. Christopher Alberts ,Audrey Dorofee ,*Managing Information Security Risks: The OCTAVE (SM) Approach*
5. *IT Governance: Implementing Frameworks and Standards for the Corporate Governance of IT*

MCS13I004 CYBER FORENSICS PROCESS DESIGN 3 0 0 3

OBJECTIVE:

- Detailed Study of digital evidence management & Network forensics
- Plan & prepare for investigation of data and image files
- Acquire knowledge on the cyber forensics concepts and its tools

UNIT I DIGITAL EVIDENCE MANAGEMENT 9Hrs

Data Recovery – Evidence Collection and Data Seizure – Duplication and Preservation of Digital Evidence – Computer Image Verification and Authentication, Discovery of Electronic Evidence – Identification of Data – Reconstructing Past Events.

UNIT IINETWORK FORENSICS 9Hrs

Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs Investigating network Traffic, Investigating Web attacks, Router Forensics**,** Investigating Wireless Attacks.

UNIT III INVESTIGATING DATA AND IMAGE FILES 9Hrs

Steganography, Data Acquisition and Duplication, Recovering Deleted files and Deleted Partitions, Image file forensics

UNIT IV ADVANCED CYBER FORENSICS CONCEPTS 9Hrs

Fighting against Macro Threats – Information Warfare Arsenal – Tactics of the Military – Tactics of Terrorist and Rogues – Tactics of Private Companies. The Future – Arsenal – Surveillance Tools – Victims and Refugees – Advanced Computer Forensics.

UNIT V TOOLS AND CASE STUDY 9Hrs

Cyber forensics tools and case studies.

Total No of Hours: 45

Reference Books:

1. Christofpaar, Jan Pelzl,.*Understanding Cryptography: A Textbook for Students and Practitioners*
2. Ali Jahangiri ,Live Hacking: *The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts*
3. John J. Barbara, *Handbook of Digital and Multimedia Forensic Evidence*
4. *Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics)*
5. Jennifer Bayuk ,*CyberForensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series)*

MCS13I005 DATA COMMUNICATION AND SECURITY 3 0 0 3

OBJECTIVE :

- Acquire the fundamental knowledge of computer networks
- Learn about the protocol and LAN
- Gain in-depth knowledge on transport & application layer & network security

UNIT-I INTRODUCTION 9Hrs

Introduction - OSI reference model-TCP/IP reference model-Electrical interface-Transmission media-Attenuation-data transmission basics - asynchronous transmission – synchronous transmission – error correction - error detection methods in MAC layers- Analog and Digital transmission

UNIT-II PROTOCOL 9Hrs

Introduction – Error control-Idle RQ - continuous RQ - Character oriented protocols –simplex - half duplex - duplex protocol - Bit oriented protocol – HDLC - SDLC

UNIT-III LOCAL AREA NETWORKS 9Hrs

Introduction – Wired LANs – Ethernet, Token bus Token Ring, FDDI-Wireless LANs- Bridges-Transparent bridges, source routing bridges

UNIT-IV TRANSPORT & APPLICATION LAYER 9Hrs

Transport protocols-connection oriented service-TCP-TCP congestion control-UDP Network security-public key encryption and digital signatures- Application layer- DNS- Remote Logging-SMTP-FTP-HTTP-NFS and attacks in Application layer-Cloud issues

UNIT-V NETWORK SECURITY 9Hrs

Internet protocols – IPV4-IPV6- Routing protocols and security issues- Firewalls – Security Services – Message confidentiality, integrity and authentication – Data loss/ Data leakage prevention schemes- Quantum network security schemes

Total No of Hours: 45

Reference Books:

1. Fred Halsal,(2001)”*Data Communication, Computer Networks and Open Systems*”,Pearson Education
2. William Stalling,(2003)”*Data & Computer Communications*”, (6th ed.), Pearson Education
3. Andrew S. Tanenbaum,(2000)”Computer Networks”, (4th ed.), PHI
4. Douglas E. Comer and Ralph E. Droms,(2001)” *Computer Networks and Internet*”, (3rd ed.), Pearson Education
5. Benrouz A. Forouzan ,”*Data Communication & Networking* “, McgrawHill ,(4th ed.)
6. *www.searchsecurity.co.uk*

MCS13I006 ETHICAL HACKING AND COUNTERMEASURES 3 0 0 3

OBJECTIVE :

- To identify security vulnerabilities and weaknesses in the target applications.
- To identify how security controls can be improved to prevent hackers gaining access to operating systems and networked environments.
- To test and exploit systems using various tools in real time machines.

UNIT I **9Hrs**

Hacking windows – Network hacking – Web hacking – Password hacking. A study on various attacks – Input validation attacks – SQL injection attacks ,PHP Injections– Buffer overflow attacks - Privacy attacks.

UNIT II **9Hrs**

TCP / IP – Checksums – IP Spoofing port scanning, DNS Spoofing. Dos attacks – SYN attacks, Smurf attacks, UDP flooding, DDOS – Models. Firewalls – Packet filter firewalls, Packet Inspection firewalls – Application Proxy Firewalls.

UNIT III **9Hrs**

Fundamentals of Computer Fraud – Threat concepts – Framework for predicting inside attacks – Managing the threat – Strategic Planning Process.- Architecture strategies for computer fraud prevention – Protection of Web sites – Intrusion detection system – NIDS, HIDS – Penetrating testing process – Web Services – Reducing transaction risks. Phishing.

UNIT IV **9Hrs**

Key Fraud Indicator selection process customized taxonomies – Key fraud signature selection process – Accounting Forensics – Computer Forensics – Journaling and it requirements – Standardized logging criteria – Journal risk and control matrix – Neural networks – Misuse detection and Novelty detection

UNIT V **9Hrs**

Footprinting, Scanning, Enumeration, Email Analysis and Spam Mails, Proxy Servers, Spoofing, Banner Grabbing, Social Engineering, Sniffers, Session Hijacking, Defending Virus, Defending Trojans, Backdoor ,Rootkits and Worms, Keyloggers, , Cross Site Scripting.(XSS) ,Cross Site Request Forgery (CSRF)Countermeasures, Expert Levels Hands on OWASP, IP Tracing Hunting Hackers.

Total No of Hours: 45

Reference Books:

1. Kenneth C.Brancik,(2008) "*Insider Computer Fraud*", Auerbach Publications Taylor & Francis

2. Ankit Fadia (2006)"*Ethical Hacking*" ,(2nd ed.), Macmillan India Ltd

3. *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms* Ec-Council Press Series:Certified Ethical Hacker,EC- Council(2009)

4. Ali Jahangiri (2009) *Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers and IT Security Experts...*

5. Lokeshkumar,*Ethical hacking countermeasure ,An Ultimate Guide For Ethical Hackers*

MCS13IL01 ETHICAL HACKING LAB 0 0 3 1

OBJECTIVE :

- To implement the following programs

1. Working with Trojans, Backdoors and sniffer for monitoring network communication
2. Denial of Service and Session Hijacking using Tear Drop, DDOS attack.
3. Penetration Testing and justification of penetration testing through risk analysis, SQL Injection Attacks, XSS, CSRF.
4. Password guessing and Password Cracking.
5. Wireless Network attacks, Bluetooth attacks
6. Firewalls, Intrusion Detection and Honey pots
7. Malware – Key logger, Trojans, Key logger countermeasures
8. Understanding Data Packet Sniffers – Wireshark, CACE Pilot, TCP dump/Win Dump, Network View, The Dude Sniffer, Ace, Capsa Network Analyzer.
9. Windows Hacking – NT LAN Manager, Secure 1 password recovery
10. Implementing Web Data Extractor and Web site watcher. Hacking Web Application
11. Buffer Overflow Attacks.
12. Enumeration – SNMP, SMTP, Unix/Linux, LDAP,NTP.
13. Programming and Reverse Engineering - Basics of coding in Ruby

MCS13IL02 CRYPTOGRAPHY AND CRYPTANALYSIS LAB 0 0 3 1

OBJECTIVE

- To implement the following programs

1. Implementation of S-DES algorithm for data encryption
2. Implementation of Triple - DES algorithm for data encryption
3. Implement RSA asymmetric (public key and private key)-Encryption.
4. Histogram analysis of Caesar Cipher and DES
5. Generate digital signature using Hash code & MAC code
6. Study of MD5 Hash function and implement the hash code using MD5
7. Study of SHA-1 Hash function and implement the hash code using SHA-1
8. Diffie-Hellman Key Exchange Protocol
9. Breaking of Monoalphabetic and Polyalphabetic ciphers
10. Breaking of Columnar transposition Ciphers
11. Implementation of Linear Cryptanalysis of DES
12. Implementation of Interpolation attack and Related key attack

MCS13I007 DATA MINING AND MACHINE LEARNING FOR INFORMATION SECURITY 3 0 0 3

OBJECTIVE

- To Identify key elements of data mining and machine learning algorithms
- Understand how to choose algorithms for different analysis tasks .
- Analyse data in both an exploratory and targeted manner .
- Implement and apply basic algorithms for supervised an d unsupervised learning .

UNIT I INTRODUCTION 9Hrs

Cyber security, Data Mining, Machine Learning, Review of Cybersecurity solutions, Proactive Security Solutions, Reactive Security Solutions, Misuse/Signature Detection, Anomaly detection, Hybrid Detection, Scan Detection, Profiling Modules.

UNIT II CLASSICAL MACHINE-LEARNING PARADIGMS FOR DATA MINING 9Hrs

Machine Learning, Improvements on Machine-Learning Methods, Challenges, Research Directions, supervised learning for misuse/signature detectionMisuse/Signature Detection, Machine Learning in Misuse/Signature Detection, Machine-Learning Applications in Misuse Detection. unsupervised machine learning Kmeans-K nearest- Expectation max-Subspace clustering

UNIT III MACHINE LEARNING FOR ANOMALY DETECTION 9Hrs

Introduction, Anomaly Detection, Machine Learning in Anomaly Detection Systems, Machine-Learning Applications in Anomaly Detectionmachine learning for hybrid detection – Hybrid Detection, Machine Learning in Hybrid Intrusion Detection Systems, Machine-Learning Applications in Hybrid Intrusion Detection.

UNIT IV MACHINE LEARNING FOR SCAN DETECTION, 9Hrs

Scan and Scan Detection, Machine Learning in Scan Detection, Machine-Learning Applications in Scan Detection, Other Scan Techniques with Machine-Learning Methods.machine learning for profiling network traffic-Introduction, Network Traffic Profiling and Related Network Traffic Knowledge, Machine Learning and Network Traffic Profiling, Data-Mining and Machine-Learning Applications in Network Profiling, Other Profiling Methods and Applications.

UNIT V PRIVACY-PRESERVING DATA MINING 9Hrs

Privacy Preservation Techniques in PPDM, Workflow of PPDM, Data-Mining and Machine-Learning Applications in PPDM,emerging challenges in cybersecurity Emerging Cyber Threats, Network Monitoring, Profiling, and Privacy Preservation, Emerging Challenges in Intrusion Detection.

Total No of Hours: 45

Reference books:

1. SumeetDua and Xian Du ,*Data Mining and Machine Learning in Cybersecurity*, , CRC Press Taylor and Francis Group.
2. Marcus A. Maloof ,(2005),*Machine Learning and Data Mining for Computer Security: Methods and Applications (Advanced Information and Knowledge Processing)*,(1st ed.) , Springer
3. Ian H. Witten, Eibe Frank and MarkA.Hall (2011),*Data Mining: Practical Machine Learning Tools and Techniques*, (3rd ed.),(The Morgan Kaufmann Series in Data Management Systems)

MCS13I008 THREATS AND VULNERABILITIES 3 0 0 3

OBJECTIVE:

- Understand the different types of threats
- Describe the prevention of hackers and crackers
- the intrusion detection methods and analysis of recovery methods in security and information system.

UNIT I THREATS AND VULNERABILITIES TO INFORMATION AND COMPUTING INFRASTRUCTURES 9Hrs

Internal Security Threats, Physical Security Threats, Fixed-Line Telephone System Vulnerabilities, E-Mail Threats and Vulnerabilities, E-Commerce Vulnerabilities, Hacking Techniques in Wired Networks , Hacking Techniques in Wireless Networks,Computer Viruses and Worms, Trojan Horse Programs, Hoax Viruses and Virus Alerts,Hostile Java Applets, Spyware

UNIT II WIRELESS THREATS AND ATTACKS 9Hrs

Wireless Threats and Attacks,,WEP Security ,Bluetooth Security,,CrackingWEP,Denial of Service Attacks, Network Attacks, Fault Attacks, Side-Channel Attacks

UNIT III PREVENTION: KEEPING THE HACKERS AND CRACKERS AT BAY 9Hrs

RFID and Security ,Cryptographic Privacy Protection Techniques, Cryptographic Hardware SecurityModules,Smart Card Security,Client-Side Security,Server-Side Security ,Protecting Web Sites,DatabaseSecurity,Medical Records Security,Access Control: Principles and Solutions,Password Authentication ,Computer and Network Authentication,AntivirusTechnology,Biometric Basics and Biometric Authentication

UNIT IV DETECTION AND RECOVERY 9Hrs

Intrusion Detection Systems Basics, Host-Based Intrusion Detection Systems , Network-Based Intrusion Detection Systems, Use of Agent Technology for Intrusion Detection, Contingency Planning Management, Computer Security Incident Response Teams (CSIRTs) , Implementing a Security Awareness Program, Risk Assessment for Risk Management, Security Insurance and Best Practices.Auditing Information Systems Security, Evidence Collection and Analysis Tools, Information Leakage: Detection and Countermeasures

UNIT V MANAGEMENT AND POLICY CONSIDERATIONS 9Hrs

Digital Rights Management , Web Hosting , Managing a Network Environment , E-Mail and Internet Use Policies, Forward Security: Adoptive Cryptography Time Evolution , Security Policy Guidelines , The Asset-Security Goals Continuum: A Process for Security , Multilevel Security, Multilevel Security Models ,Security Architectures , Quality of Security Service: Adaptive Security, Security Policy Enforcement , Guidelines for a Comprehensive Security System

Total No of Hours: 45

Reference Books:

1. HosseinBidgoli, Ph.D.,*Handbook of Information Security, Volume 3, Threats, Vulnerabilities,Prevention,Detection, and Management*
2. Lawrence J Fennelly,*Handbook of Loss Prevention and Crime Prevention*

3.Tipton RuthbeRg,*Handbook of Information Security Management*

4.Mark Egan,*The Executive Guide to Information Security*

MMA130009 MATHEMATICS FOR INFORMATION SECURITY AND CYBER FORENSICS 3 1 0 4

OBJECTIVE:

- Acquire fundamental knowledge on abstract algebra
- Gain an appreciation of the importance and beauty of the basic ideas in combinatorics
- Develop basic understanding of the concepts in Mathematical logic
- Become knowledgeable in the concepts of graphs and trees

UNIT I INTRODUCTION TO ABSTRACT ALGEBRA 12Hrs

Groups(DefinitionandExamples)–Subgroups–Permutationgroups– Homomorphism–Kernel –Cosets–Lagrange's theorem –Rings–Fields (DefinitionandExamples).

UNIT II COMBINATORICS 12Hrs

MathematicalInduction–PigeonHolePrinciple–PrincipleofInclusionandExclusion– RecurrenceRelations–GeneratingFunctions.

UNIT III MATHEMATICAL LOGIC 12Hrs

Statements–TruthTable–Connectives–NormalForms–PredicateCalculus–Inference Theory.

UNITIV DISCRETES TRUCTURES I 12Hrs

Basic conceptsofGraphs–Subgraphs–Paths andCircuits –Matrix representationofGraphs– GraphIsomorphism–ConnectedgraphsandComponents–EulerandHamiltonian paths– Travellingsalesmanproblem.

UNITV DISCRETE STRUCTURES II 12Hrs

Basic conceptsof Trees–Properties–Pendantvertices–Rooted andBinary trees–Spanning trees–Fundamentalcircuits–Findingallspanning trees ofagraph–Spanningtrees ina weighted graph.

Total No. of hrs: 60

Reference Books:

1) TremblayJ.P., ManoharR., (2004) *Discrete Mathematicalstructureswith applications to Computerscience*,TataMcGraw HillPublishingCo.,

2) KennethRosen,(2007)*DiscreteMathematicsand itsapplications(SIE)*,TataMcGraw Hill PublishingCo.,

3) JohnC.Martin,(2003)*Introduction to languagesand the theoryof computation*(3rd ed.), McgrawHill

4) Hopcroft J.E., UllmanJ.D.,*Introduction to Automata theory,Languagesand Computation*,NarosaPublishinghouse,(2002).

5) NarsinghDeo, (2004)*Graphtheorywith applications to Engineering and Computer Science*, PrenticeHallofIndia,

6) RobinJ.Wilson, (2002) *Introduction to Graph theory*(4th ed.),Pearson,

MCS13I009 APPLIED CRYPTOGRAPHY 3 0 0 3

OBJECTIVE:

- Acquire fundamental knowledge on the concepts of finite fields and number theory
- Understand various block cipher and stream cipher models
- Describe the principles of public key cryptosystems, hash functions and digital signature

UNIT 1 MATHEMATICAL FOUNDATION 9Hrs

Number theory: Fermat's and euler's theorem-chinese remainder theorem-Euclidean algorithm-Test for primality-Discrete logarithms, Information theory: entropy, Uncertainity-Complexity theory: pseudo random number generation and generators.

UNIT 2 CRYPTOGRAPHIC PROTOCOLS 9Hrs

Protocol Building Blocks-Basic Protocols: key Exchange-Authentication-Authentication and Key exchange: Wide-mouth frog, Yahalom, Kerberos-Formal Analysis of Authentication and Key Exchange Protocols-Multiple Key Public Key Cryptography-Secret Splitting-Secret Sharing: Secret Sharing with Cheaters-Cryptographic protection of Databases-Intermediate Protocols: Time stamping services, Linking protocol, Distributed Protocol-Proxy Signatures-Group Signatures-Advanced Protocols: Zero knowledge proof, Parallel Zero Knowledge Proof, Zero Knowledge proof of identity: Chess Grandmaster Problem-Blind Signatures-Simultaneous Contract Signing-Digital certified Mail-Simultaneous Exchange of Secrets-Esoteric protocols: Secure Elections-Secure Multiparty Computation.

UNIT 3 CRYPTOGRAPHIC TECHNIQUES 9Hrs

Key Length: Symmetric key Length, Public Key Keylength-Algorithm types and Modes: Electronic Code Book Mode, Block Replay, Cipher Block Chaining Mode-Using Algorithms: Choosing an Algorithm, Public Key Cryptography vs Symmetric Cryptography, Encrypting Communication Channels.

UNIT 4 CRYPTOGRAPHIC ALGORITHMS 9Hrs

Block Ciphers: Lucifer, New Des,RC2-Combining Block Ciphers: Double Encryption, Triple Encryption, Cascading Multiple Algorithms-One Way Hash Functions:Snefru,N-Hash,MD5,SHA-Public Key Algorithms: RSA, Pohlig-Hellman, Rabin, Elliptic Curve Cryptosystems-Public Key Digital Signature Algorithms: Ghost Digital Signature Algorithm, Discrete Logarithm Signature schemes.

UNIT 5 IMPLEMENTATIONS 9Hrs

IBM Secret Key Management-IBM common cryptographic Architecture-ISO Authentication Framework-PEM-Message Security Protocol-Public Key Cryptographic Standard-AT&T model 3600 Telephone security Device-Quantum Cryptography, Tokenization(Data Security)

Total No of Hours: 45

Reference Books:

1. Bruce Schneier (1996) Applied cryptography:Protocols,Algorithms and source code in c,Wiley,(2nd ed.)
2. William Stallings(2010) Cryptography and Network Security priniciples and practices
3.OdedGoldreich (2007)Foundations of Cryptography: Volume 1, Basic Tools
4. Kevin ,Roebuck*Encryption: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity...*
5.OdedGoldreich (2009)*Foundations of Cryptography: Volume 2, Basic Applications*

MCS13I010 ADVANCED PENETRATION TESTING 3 0 0 3

OBJECTIVE:

- To identify security vulnerabilities and weaknesses in the target applications.
- To identify how security controls can be improved to prevent hackers gaining access to operating systems and networked environments.
- To test and exploit systems using various tools.
- To understand the impact of hacking in real time machines.

UNIT I PLANNING AND SCOPING FOR A SUCCESSFUL PENETRATION TEST 9Hrs

Introduction to advanced Penetration testing - Before testing begins – Planning for Action – Exploring Backtrack – Installing Open office- Effectively manage test results advanced reconnaissance techniques Introduction to reconnaissance – DNS Recon – Gathering and validating domain and IP information- Using Search engines to do the job.

UNIT II ENUMERATION 9Hrs

Adding another virtual machine – Nmap – SNMP – Creating network baselines with Scan PBNJ – Enumeration Avoidance Techniques Remote Exploitation -Manual Exploitation – Getting to and from victim machines - Passwords – Metasploit – Web Application Exploitation Detecting Load balancers – Detecting web application firewalls – Web application attack and audit framework .

UNIT III EXPLOITS AND CLIENT SIDE ATTACKS 9Hrs

Buffer Overflows – Fuzzing – Fuzzing tools included in Backtrack – Fast-track post exploitation
Rules of Engagement – Data gathering, Network analysis and pillaging - bypassing firewalls and avoiding detection
Preparation – Stealth scanning through the firewall – Avoiding IDS Cleaning up compromised hosts – Miscellaneous evasion technique - data collection tools and reporting - Record now sort later – The text editor method – Dradis framework for collaboration – Setting up virtual test lab – Putting it all together.

UNIT IV CODING FOR PENETRATION TESTERS 9Hrs

Introduction to command shell scripting – Introduction to Python – Introduction to Perl – Introduction to Ruby.

UNIT V INTRODUCTION TO WEB SCRIPTING WITH PHP 9Hrs

Manipulating windows with Power shell – Scanner Scripting – Exploitation Scripting – Post Exploitation Scripting.

Total No of Hours: 45

Reference Books:

1. Lee Allen(2012) *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide*

2. Jeremy Faircloth (Aug 1, 2011).*Penetration Tester's Open Source Toolkit*, (3rded.)

3. *Penetration Testing: Procedures & Methodologies (Ec-Council/ Certified Security Analyst*) ,EC-Council (2010)

4. Jason Andress and Ryan Linn (2011) *Coding for Penetration Testers: Building Better Tools*

MCS13IL03 TERM PAPER AND SEMINAR (CASE STUDY) 0 0 6 1

OBJECTIVE

- The Students are expected to present a Case Study
- The Students should deliver a presentation on the Case Study.
- Evaluation is done based on the technical strength, presentation & demonstration of the proposed Case Study.
- Students should submit a report and appear for Viva – Voce.

MCS13IL04 DIGITAL CRIME INVESTIGATION LAB 0 0 3 1

OBJECTIVE

- To implement the following programs :

In this course, the students will learn many of the cardinal principles and techniques of digital crime scene investigation. The necessity of a rigorous scientific approach will be stressed. This course uses an intensive, hands-on style to learn the basics of digital crime scene management and the recognition, evaluation, enhancement, documentation, control, and collection of evidence. Students will be introduced to:

- Documentation with notes, sketches, and photography
- Specialized techniques for the recognition and enhancement of physical evidence
- Preparation and maintenance of case folders for records including notes, sketches, photographs, and Contacts/communications.
- Communication of results and preparation formal, typewritten reports2
- Management of scenes and available resources including equipment and personnel Mock crime
- Scenes will be used for demonstrations and to assess knowledge, skills, and abilities of students.

- Conducting Digital Investigation and Investigative reconstruction with Digital Evidence.
- Modus Operandi, Motive and Technology.

Scenes will encompass criminal and non-criminal activities including Computer Intrusions, Cyber stalking, violent crime, crime committed using Mobile devices and Network Related crimes

The primary aim of the course is to introduce students to scientific, philosophy, integrity, scene investigation procedures, criminalities, and the role of the criminalist as they relate to digital crime scene investigation.

MCS13IL05 PENETRATION TESTING AND VULNERABILITY ASSESSMENT LAB 0 0 3 1

OBJECTIVE

To the implement the following programs :

1. Network Mapping & Target Identification

2. Interpreting Tool Output - Interpreting output from port scanners, network sniffers and other network enumeration tools.

3. Filtering Avoidance Techniques - The importance of egress and ingress filtering, including the Risks associated with outbound connections.

4. Packet Crafting - Packet crafting to meet a particular requirement

5. OS Fingerprinting - Remote operating system fingerprinting; active and passive techniques.

6. Network Access Control Analysis - Reviewing firewall rule bases and network access control lists.

7. File System Permissions

a. File permission attributes within Unix and Windows file systems and their security implications.

b. Analyzing registry ACLs

8. Configuration Analysis - Analyzing configuration files from the following types of Cisco equipment:

9. Unix Security Assessment

a. User enumeration- Discovery of valid usernames from network services commonly running by default.

b. Unix vulnerabilities - Common post-exploitation activities

c. FTP - FTP access control   Anonymous access to FTP servers
Risks of allowing write access to anonymous users

d. Send mail / SMTP - Valid username discovery via EXPN
Awareness of recent Sendmail vulnerabilities; ability to exploit them if possible .
Mail relaying

10. Web Testing Techniques

a. Web Site Structure Discovery

b. Cross Site Scripting Attacks

c. SQL Injection

d. Session ID Attacks

e. Data Confidentiality & Integrity

f. Directory Traversal

g. Code Injection

h. Application Logic Flaws

MCS13I011 DIGITAL FORENSIC INVESTIGATION AND EVIDENCE MANAGEMENT 3 0 0 3

OBJECTIVE

- Understand the languages of digital forensics ,and the investigation of digital crime scene
- Learn the basics of computer investigators
- Become knowledgeable in the digital forensics networks and OSI layers

UNIT I DIGITAL FORENSICS 9Hrs

Foundations of Digital Forensics– Language of computer crime investigation - digital evidence in the court room.

UNIT II DIGITAL INVESTIGATION 9Hrs

Conducting digital investigation – Handling the digital crime scene -investigate reconstruction – modus operandi, motive and technology.

UNIT III APPREHENDING OFFENDERS 9Hrs

Violent crime and digital evidence – digital evidence as alibi – Sex offenders on the Internet-Computer intrusions-Cyber stalking.

UNIT IV COMPUTERS 9Hrs

Computer basics for digital investigators – applying forensic science to computers –Digital Evidence on windows system-digital evidence on UNIX system, Digital evidence on Macintosh system, Digital evidence on mobile devices.

UNIT V NETWORKS 9Hrs

Networks basics for digital investigators – applying forensic science to networks – digital evidence on the internet - digital evidence on physical and Data - link layers - digital evidence on network and transport layers.

Total No of Hours: 45

Reference Books:

1. EoghanCasey ,'Digital Evidence and Computer Crime Forensic science, Computers and Internet', (3rd ed.),Elsevier Academic Press
2. Shira A scheindlin, Daniel J Capra ,A Electronic Discovery and Digital Evidence in a Nut Shell, (3rd ed.),The Sedona Conference,Academic Press

MCS13IE01 BUSINESS CONTINUITY & DISASTER RECOVERY 3 0 0 3

OBJECTIVE:

- Develop basic understanding of threat and recovery planning and risk Management
- Analysis of mitigation strategy development.
- Understand the IT and non IT disasters and planning development techniques and understand the testing and auditing methods.

UNIT-I: BUSINESS CONTINUITY AND DISASTER RECOVERY AND RISK MANAGEMENTBASICS 9Hrs

Overview - definition-Components of business-The cost of planning versus the cost of failure-Types of disasters-Electronic data threats- Business continuity and disaster recovery planning – basics

Risk Management Basics-Principle, process, Technology and Infrastructure in Risk Management-IT specific Risk Management-Risk assessment Components-Information gathering methods-Natural and environmental threats-human threats-Infrastructure threats-Threat checklist-Threat Assessment Methodology-Vulnerability assessment.

UNIT II BUSINESS IMPACT ANALYSIS AND MITIGATION STRATEGY DEVELOPMENT 9Hrs

Introduction- Business Impact Analysis Overview-Understanding Impact Critically-Identifying business functions-Marketing and sales-Operations-Research and development-Warehouse- Gathering data for the Business Impact Analysis-Determining the Impact- Business Impact Analysis data points-Preparing the Business Impact Analysis report – mitigation strategy development Introduction-Types of Risk Mitigation strategies-The Risk Mitigation process- Developing your Risk Mitigation Strategy-People, mitigation and infrastructure-IT Risk mitigation-Backup and recovery consideration

UNIT IIIDISASTER RECOVERY 9Hrs

Introduction-Data Disasters-Virus Disasters-Communication System Disaster-Software Disasters-Data centre Disasters-IT Staff Disasters-IT Vendor Disasters-IT Project Failures-Information Security-Disaster Recovery Tools-Introduction to Non-IT Disasters-Disaster Recovery At Home.

UNIT IV PLAN DEVELOPMENT 9Hrs

Introduction-Phase of the Business continuity and disaster recovery-Defining BC/DR teams and key personnel-Defining task and assigning resources-Communication Plans-Event logs,, change controls and appendices-emergency response and recovery Introduction-Emergency management overview response plan-Crisis Management-Disaster Recovery-IT Recovery tasks.

UNIT V TRAINING, TESTING AND AUDITING AND BC/DR PLAN MAINTENANCE 9Hrs

Introduction-Training forBusiness continuity and disaster recovery-Testing the BC/DR plan-Performing IT System and Security auditsBC/DR plan maintenance Introduction-BC/DR Plan Change Management-Strategies for managing change-BC/DR plan Audit-Plan Maintenance Activities-Project close out.

Total No of Hours: 45

Reference Books:

1**.**Susan Snedaker , (2007)*Business Continuity and Disaster Recovery Planning for IT Professionals*

2. B S Thejendra,(Jan 8,2008)*Disaster Recovery and Business Continuity* ,(2nd ed.),

3.John RittinghousePhD ,CISM ,James F. Ransome PhD CISM CISSP,(2004)*Business Continuity and Disaster Recovery for InfoSec Managers*

4. Deborah C. Miller (2011) *Business Continuity and Disaster Recovery: Getting Started Guide Concepts and Definitions for Common Sense Planning*

5Erbschloe**,** (2003)*Guide to Disaster Recovery*,*Michael*

6**.** Gerard Blokdijk Jackie Brewster , Ivanka ,*Disaster Recovery and Business Continuity IT Planning, Implementation, Management and Testing of Solutions and Services Workbook*

MCS13IE02 CLOUD COMPUTING AND SECURITY 3 0 0 3

OBJECTIVE:

- Understand the cloud computing basics ,and evolution of cloud data software ,and analysis of security and virtual attacks,
- Understand the virtual security and maintain secure data storage and understand the service providers in audit and compliance.

UNIT I Introduction 9Hrs

Cloud computing basics – Benefits-limitations- security concerns- regulatory issues –Cloud computing services: IaaS, PaaS,SaaS Software plus services

UNIT II Building Cloud networks 9Hrs

Evolution- Cloud Data Center-Collaboration – SOA- Basic approach to data center based SOA-Role of open source software and usage

UNIT III Cloud Analysis and Environment 9Hrs

Risk Model- Risk treatment – Security Assessment – Virtual Overlays – Malware – Attacks.

UNIT IV Cloud Security 9Hrs

Infrastructure Security - Cloud Data Security and storage – Security as a Service- Security Management in Cloud

UNIT V Audit and Compliance 9Hrs

Privacy- Audit and compliance – cloud service providers- impact of cloud computing on the role of corporate IT

Total No of Hours: 45

Reference Books:

1**.** Toby Velte, Anthony Velte, Robert Elsenpeter ,(2009)*Cloud Computing, A Practical Approach***,**
McGraw Hill, ISBN: 9780070683518

2**.** John W. Rittinghouse, James F. Ransome (2009).*Cloud Computing Implementation, Management, and Security*

3.Tim Mather, SubraKumaraswamy and ShahedLatif (2009)*Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice)*

4 John Rhoton, Jan De Clercq and David Graves (2013)*Cloud Computing Protected: Security Assessment Handbook*

5. Vic (J.R.) Winkler, (2011)*Securingthe Cloud :Cloud Computer Security Techniques and Tactics*,
ISBN: 978-1-59749-592-9, 2011 Elsevier Inc..

.

MCS13C002 OBJECT ORIENTED SOFTWARE ENGINEERING 3 0 0 3

OBJECTIVE:

- Develop basic understanding of classical software engineering
- Describe about planning,estimation and tools
- Explain about modules to objects
- Acquire Knowledge About Different Phases

UNIT I INTRODUCTION TO CLASSICAL SOFTWARE ENGINEERING 9Hrs

Historical, Economic and Maintenance aspects. Introduction to OO Paradigm. Different phases in structured paradigm and OO Paradigm. Software Process and different life cycle models and corresponding strengths and weaknesses.

UNIT II PLANNING, ESTIMATION & TOOLS FOR STEP WISED REFINEMENT 9Hrs

Estimation of Duration and Cost – COCOMO components of software. Project Management plan, Cost - Benefit analysis, Introduction to software metrics and CASE tools. Taxonomy and scope of CASE tools.

UNIT III MODULES TO OBJECTS 9Hrs

Cohesion and Coupling, Data Encapsulation and Information hiding aspects of Objects. Inheritance, polymorphism and Dynamic Binding aspects. Cohesion and coupling of objects. Reusability, Portability and Interoperability aspects.

UNIT IV REQUIREMENT& ANALYSIS PHASES 9Hrs

Rapid Prototyping method, Specification phase, Specification Document, Formal methods of developing specification document, Use case Modeling, Class Modeling, Dynamic Modeling, Testing during OO Analysis.

UNIT V DESIGN PHASE & IIM PHASES 9Hrs

Data oriented design, Object Oriented design, and Formal techniques for detailed design. Challenges in design phase. Implementation, Integration and maintenance phases, OOSE aspects in these phases.

Total No of Hours: 45

Reference Books:

1. Stephen R. Schach ,*Object oriented and Classical Software Engineering*, (7th ed.) , TMH.
2. Timothy Lethbridge, Robert Laganiere ,*Object oriented and classical software Engineering* , TMH.
3. IvicaCrnkovic,*Component-based software engineering*, 7th international symposium, CBSE 2004, Springer.

MCS13IE04 UNIX AND LINUX SYSTEMS SECURITY 3 0 0 3

OBJECTIVE :

- Familiarize students with the Linux environment
- Learn the fundamentals of shell programming
- Acquire the basic knowledge of linux administration and security principles.

UNIT I SECURITY BUILDING BLOCKS 9Hrs

Users, Passwords and Authentication – Users, Groups and Super user – File System and Security - Physical Security for Servers.

UNIT II NETWORK AND INTERNET SECURITY 9Hrs

Modems and Dial up Security – TCP/IP Networks – Securing TCP and UDP services – Network based authentication systems- Network file system.

UNIT III SECURE OPERATIONS 9Hrs

Backups – Defending Accounts – Integrity Management – Auditing, Logging and Forensics .

UNIT IV HANDLING SECURITY INCIDENTS 9Hrs

Discovering a break in – Protecting against program threats- denial of service attacks and solution.

UNIT V 9Hrs

Layered Linux Security Strategy - Managing Security Alerts and Updates – Building and maintaining a security Baseline – Testing and Reporting – Detecting and Responding to security breaches.

Total No of Hours: 45

Reference Books:

1. Simson Garfinkel, Gene Spafford PH.D. and Alan Schwartz PH.D (2003) *Practical Unix and Internet Security*, (3rd ed.)
2. Evi Nemeth, Garth Snyder, Trent R. Hein and Ben Whaley (2010) *UNIX and Linux System Administration Handbook* (4thed.)
3. David A. Curry (1992)*UNIX System Security: A Guide for Users and System Administrators (Addison-Wesley Professional Computing)*
4. Michael Jang (2010)*Security Strategies in Linux Platforms and Applications (Information Systems Security & Assurance)*

MCS13IE05 VIRTUALIZATION SECURITY 3 0 0 3

OBJECTIVE:

- The students will be able to understand the Increased use of hardware resources Reduced management and resource costs
- Improved business flexibility Improved security and reduced downtime and understand the security of virtualization.

UNIT I 9Hrs

Fundamentals of virtualization security- virtualization architecture , threats to virtualized environment , How security must adapt to virtualization , Securing Hypervisors , Hypervisor configuration and security , Configuring VMware ESXi, Configuring Citrix Xenserver.

UNIT II 9Hrs

Designing Virtual Networks for security, Comparing virtual and physical networks , Virtual Network security considerations , Configuring virtual switches for security , Advanced virtual network operations , Network operations in VMware vSphere, Network operations in Microsoft Hyper-V, Network operations in Citrix Xenserver.

UNIT III 9Hrs

Virtualization management and client security , Network architecture for Virtualization Management Servers, VMware vcenter , Microsoft system Center virtual machine manager , Citrix Xencenter, Securing virtual machine – threats and vulnerabilities , Locking down VMware VMs, Locking down XenServer VMs.

UNIT IV 9Hrs

Logging and auditing , Virtualization logs and auditing options , Integrating with existing logging platforms , effective log management , Change and configuration management - best practices , Cloning and templates for improved configuration management .

UNIT V 9Hrs

Disaster recovery and business continuity, high availability and fault tolerance , scripting tricks and tips for automation – need for scripting , VMware scripting , Citrix scripting – shell scripts .

Total No of Hours: 45

Reference Books:

1. Dave Shacklef,(2012)Virtualization Security: Protecting Virtualized Environments ,Wiley Publications
2. John Hoopes (2008)Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and...
3. Virtualization Security (Ec-Council Disaster Recovery Professional (Edrp)), EC-Council (2010)
4. Matthew Portnoy (2012) Virtualization Essentials
5. Edward Haletky (2009)VMware vSphere and Virtual Infrastructure Security: Securing the Virtual Environment

MCS13IE06 MOBILE AND MULTIMEDIA SECURITY 3 0 0 3

OBJECTIVE :

- To understand the basics of wireless technologies and security.
- Become knowledgeable in mobile phone forensics and android forensics. Learn the methods of investigation using digital forensic techniques.

UNIT I MOBILE PLATFORMS 9Hrs

Top mobile issues and development strategies , Physical Security , Tips for secure Mobile Application Development , Android Security , Android Security Model , Apple I -Phone Security , Windows Mobile Security, Blackberry Security, Java Mobile Edition Security , Symbian OS Security , Web OS Security

UNIT II MOBILE SERVICES 9Hrs

WAP and Mobile HTML Security , Bluetooth security – Bluetooth technical architecture , SMS Security – Application attacks , Protocol attacks , Mobile Geolocation , Enterprise Security on the Mobile OS – Device Security Options , Encryption , Application sandboxing , Signing and permissions.

UNIT III FUNDAMENTALS OF MULTIMEDIA SECURITY 9Hrs

Multimedia Encryption, Multimedia Authentication, Key Management for Multimedia Authentication and Distribution, An Overview of Digital Watermarking, Biometrics in Digital Rights Management.

UNIT IV ADVANCED MULTIMEDIA SECURITY 9Hrs

Format- Compliant Content Protection, Secure Media Streaming and Secure Transcoding, Scalable Encryption and Multi-Access control for Multimedia, Broadcast Encryption.

UNIT V WATERMARKING TECHNIQUES FOR MULTIMEDIA 9Hrs

Robust Identification of Audio using Watermarking and Fingerprinting, Multidimensional Watermark for Still Image: Parallel, Embedding and Detection, Fragile Watermarking for Image Authentication, New trends and Challenges in Digital Watermarking Technology: Applications for printed materials, Robust Watermark Detection from quantized MPEG Video Data.

Total No of Hours: 45

Reference Books:

1. HimanshuDwivedi , Chris Clark , David Thiel ,(2010)*Mobile Application Security*,Tata McGraw Hill
2. Stephen Fried (2010)*Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World* ,,Auerbach Publications
3. WenjunZeng (Editor), Heather Yu ,Ching-Yung Lin ,(2006)*Multimedia Security Technologies for Digital Rights Management* (1st ed.),Academic Press
4. DarkoKirovski.,(2006)*Multimedia Watermarking Techniques and Applications (Internet and Communications)* (1st ed.),Auerbach Publications
5. Mario Marques da Silva ,(2012)*Multimedia Communications and Networking*, ,CRC Press;(1st ed.)

MCS13IE07 WIRELESS NETWORK FORENSICS 3 0 0 3

OBJECTIVE :

- To explain the basic information storage and retrieval concepts and issues those are specific to efficient information retrieval.
- To design and implement a small to medium size information storage and Retrieval system.
- To implement security issues while storing and retrieving information.

UNIT I NETWORK FORENSICS AND INVESTIGATING LOGS 9Hrs

Introduction and Investigating Logs-Network Forensics-Log files as Evidence-Why Synchronize Computer Times. network traffic investigations: Introduction -Network addressing Schemes-OSI Reference Model-Overview of Network Protocols-Types of Network Attacks-Evidence gathering at the Physical Layer-DNS Positioning Techniques-Evidence gathering from ARP Table-Evidence Gathering at the Data Link Layer-Gathering Evidence from IDS

UNIT IIWEB ATTACK INVESTIGATIONS 9Hrs

Types of Web Attack-Overview of Web Logs-Investigating a Web Attack-Investigating FTP Server-Investigating IIS Logs- Investigating Apache Logs-Investigating Web Attacks in Windows based Server-Web page defacement-Security Strategies for Web Applications-investigating Static and Dynamic IP Addresses-Tools for Web attack Investigation-Tools for Locating IP Addresses. router forensics: Functions of a Router-Router vulnerabilities-Router Attacks-Router forensics Vs Traditional Forensics-Investigating Router Attacks-Using Specialized E-Mail Forensics Tools-Laws against E-Mail Crime.

UNIT III WEB SECURITY 9Hrs

Web Security, Email Security, Virtual Private Network, Incident response.

UNIT IV WIRELESS ATTACK INVESTIGATIONS: **9Hrs**

Wireless Network technologies-Wireless Attacks-Network Forensics in Wireless Environment PDAforensics: Information stored in PDAs-Palm OS-Windows CE-PDA Generic States-PDA Security Issues-PDA Forensics Steps-PDA Security Counter Measures.

UNIT V IPOD AND IPHONE FORENSICS 9Hrs

iPod and iPhone Forensics-JailBreaking-Tools for iPod and iPhone Forensics blackberry forensics : Blackberry Security-Blackjacking Attacks- Blackberry Forensics-Additional Blackberry Forensics Tools

Total No of Hours: 45

Reference Books:

1. *Computer Forensics : Investigating Network Intrusions and Cyber Crime*, EC-Council, ISBN-13: 978-1-4354-8352-1, ISBN-10: 1-4354-8352-9
2. *Computer Forensics: Investigating Wireless Networks and Devices*, EC-Council, ISBN-13: 978-1-4354-8353-8, ISBN-10: 1-4354-8353-7
3. *Handbook of Digital Forensics and Investigations*, Eoghan Casey ed., Elsevier Academic Press, ISBN 13: 978-0-12-374267-4
4. *Network Defense: Security and Vulnerability Assessment* (Ec-Council Press Series: Network Defense) by EC-Council (Apr 14, 2010)

MCS13IE08 PATTERN RECOGNITION 3 0 0 3

OBJECTIVE:

- To learn about patterns ,functions, algorithms and understand the clustering methods of validity and unsupervised classification and pattern recognition and processing
- The feature extraction methods and discovering recent advances in pattern recognition.

UNIT I. PATTERN RECOGNITION 9Hrs

Overview of pattern recognition - Discriminant functions - Supervised learning - Parametric estimation -Maximum likelihood estimation - Bayesian parameter estimation - Perceptron algorithm - LMSE algorithm -Problems with Bayes approach - Pattern classification by distance functions - Minimum distance pattern classifier.

UNIT II. UNSUPERVISED CLASSIFICATION 9Hrs

Clustering for unsupervised learning and classification - Clustering concept - C-means algorithm - Hierarchical clustering procedures - Graph theoretic approach to pattern clustering - Validity of clustering solutions.

UNITIII.STRUCTURAL PATTERN RECOGNITION 9Hrs

Elements of formal grammars - String generation as pattern description - Recognition of syntactic description - Parsing - Stochastic grammars and applications - Graph based structural representation.

UNIT IV. FEATURE EXTRACTION AND SELECTION 9Hrs

Entropy minimization - Karhunen - Loeve transformation - Feature selection through functions approximation - Binary feature selection.

UNIT V.RECENT ADVANCES 9Hrs

Neural network structures for Pattern Recognition - Neural network based Pattern associates – Unsupervised learning in neural Pattern Recognition - Self organizing networks - Fuzzy logic - Fuzzy pattern classifiers - Pattern classification using Genetic Algorithms.

Total no.of Hours: 45

Reference Books:

1. Robert J.Schalkoff,(1992) *PatternRecognition : Statistical, Structural and Neural Approaches*, John Wiley & Sons Inc., New York
2. Tou and Gonzales, (1974)*Pattern Recognition Principles*, Wesley Publication Company, London
3. Duda R.O., and Hart.P.E., (1973)*Pattern Classification and Scene Analysis*, Wiley, New York
4. Morton Nadier and Eric Smith P.,(1993) *Pattern Recognition Engineering*, John Wiley & Sons, New York

MCS13IE09 SECURE SOFTWARE DEVELOPMENT LIFE CYCLE 3 0 0 3

OBJECTIVE:

- To understand the security ,privacy,hippaandunderstand the software design and providing software implementation meethods .
- Understand the secure computing and understand the deployment of operation maintenance.

UNIT I SECURE SOFTWARE CONCEPTS 9Hrs

Secure software concepts – confidentiality –- Information Security risk management - Software security risk management – System Development life cycle – Regulation – privacy and compliance – FIMA-Information privacy and privacy laws – HIPPA final security rule – PCI data security standard-Software Architecture styles – software development methodology – CLASP – TSP Secure –Intellectual property and privacy legal Issues – Information privacy principles –OWASP –development –code review – testing guide- Information Security models.

UNIT II SECURE SOFTWARE DESIGN 9Hrs

Approaches – software requirement engineering – security policy decomposition – NIST 33 security principles – Information security policy Implementation and Decomposition – Decomposing confidentiality – Integrity – Availability – Authentication – Authorization – Auditing – Identification of data and gathering of thread information.

UNIT III SECURE SOFTWARE IMPLEMENTATION 9Hrs

Software vulnerabilities and countermeasures – Defensive coding practices – Exception handling – configuration management – code analysis – anti tampering techniques – Interface coding

UNIT IVSECURE SOFTWARE TESTING 9Hrs

Testing for security Quality Assurance – functional – performance – security- Integration testing- Test types – penetration testing – fuzzing – Scanning – simulation testing – Testing for failure – cryptographic validation – Impact Assessment- standard for software quality assurance

UNITV SOFTWARE ACCEPTANCE,SOFTWARE DEPLOYMENT 9Hrs
OPERATIONS MAINTENANCE

Pre-release activities – Post-release activities – Certification – BITS –ICSA – FIPS199- FIPS140- Independent testing – Installation and Deployment – operations and maintenance – Monitoring and Auditing – Incident Management – CERT/CC – FedCIRC – End-of-life policies.

Total No of Hours: 45

Reference Books:

1. Ronald L Krutz, Alexander J. Fry,(2009) "*The CSSLP prep Guide*" Wiley Publication
2. Michael Roberts (Oct 8, 2012)*Certified Secure Software Lifecycle Professional (CSSLP) Secrets To Acing The Exam and Successful Finding And .*
3. Michael Howard, Steve Lipner. (2006)"*The security development lifecycle: SDL, a process for developing demonstrably more secure software" ,* Microsoft Press
4. Miller and Peter Gregory (2012),*CISSP For Dummies*

MCS13IE10 TCP/IP DESIGN AND IMPLEMENTATION 3 0 0 3

OBJECTIVE:

- The students will be able to understand the networking concepts and discovery about protocols Routing, user datagram protocol, machine and flow protocol, and understand the gateways, sockets in design method.

UNIT-I **9Hrs**

Internetworking Issues-Routing-Internet Addressing-Address Resolution Protocol (ARP)-Reverse Address Resolution protocol (RARP)-Packet format Routing-IGMP

UNIT-II **9Hrs**

Fragmentation-Reassembly-Error processing-Ipv6-UDP-Basic concepts-TCP data structures

UNIT-III **9Hrs**

Finite state Machine Implementation-Output processing-Timer management Flow control- Urgent Data Processing

UNIT-IV **9Hrs**

Core Gateway System-Autonomous systems and Considerations-Interior Gateway Protocols, Transparent Gateways, DNS.

UNIT-V **9Hrs**

Sockets-RPC Mechanisms-Telnet-Mail systems.

Total No of Hours: 45

Reference Books:

1. Comer .D.E, (2001)"Internetworking with TCP/IP", Volume 1, PHI

2. Comer D.E & Stevens D.L., (1997)"*Internetworking with TCP/IP*" ,Volume 2,(2nd ed.), Prentice Hall of India

3. Comer D.E, (1999)"*Computer Networks and Internet*", PHI

4. Comer D.E & Stevens D.L., (1997)"*Internetworking with TCP/IP* ",Volume 3, PHI

5. Stevens W.R, (1999)"*TCP/IP Illustrated*", Volume 1,2 & 3, Addison Wesley

MCS13IE11 **STORAGE MANAGEMENT SECURITY** **3 0 0 3**

OBJECTIVES:

- To explain the basic information storage and retrieval concepts.
- To understand the issues those are specific to efficient information retrieval and implement a small to medium size information storage and retrieval system.
- To implement security issues while storing and retrieving information.

UNIT 1 **STORAGE SYSTEMS** **9Hrs**

Data Centre elements – ILM strategy – Disk drive architecture and performance- RAID & RAID levels – ISS and its components

UNIT II **STORAGE NETWORKING TECHNOLOGIES** **9Hrs**

Disk architecture – RAID- RAID levels- storage systems: direct attached storage(DAS), storage area networks (SAN) FC-SAN-IP-SAN - network attached storage (NAS) - content attached storage(CAS)

Unit III **BACK UP, REPLICATION AND ARCHIVE** **9Hrs**

Information availability and measurement - causes and consequences of downtime - RTO, and RPO - single points of failure - solutions for its mitigation - backup/recovery purposes and considerations - architecture and backup/Recovery topologies - local replication technologies - remote replication technologies

Unit IV **STORAGE SECURITY** **9Hrs**

Information security - critical security attributes for information systems - storage security domains • common domain threats – security in virtualized and cloud environment.

Unit V **STORAGE MANAGEMENT** **9Hrs**

Parameters and components to monitor in a storage infrastructure - key management activities and examples - storage management standards and initiatives – ILM – Cloud Service Management activities.

Total No of Hours: 45

Reference Books:

1. *Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments*, (2nd ed.), EMC Education Services ISBN: 978-1-1180-9483-9, (2012)
2. Robert Spalding, (2003)“*Storage Networks: The Complete Reference*“, Tata McGraw Hill , Osborne
3. Marc Farley, (2001)“*Building Storage Networks*”, Tata McGraw Hill , Osborne
4. Robert R. Korfhage (1997)*Information Storage and Retrieval*

MCS13IE12 INFORMATION SECURITY RISK MANAGEMENT AND AUDITING 3 0 0 3

OBJECTIVES:

- The students will be able to gain the knowledge about Information Ris and to discovery knowledge in collecting data about organization
- To do various analysis on Information Risk Assessment. to understand IT audit and its activities.

UNIT I INTRODUCTION 9Hrs

Introduction to Risk management, Applying Risk management to Information Security, Risk management Lifecycle.

UNIT II RISK ASSESSMENT AND ANALYSIS TECHNIQUES 9Hrs

Risk Profiling, Formulating a Risk, Risk exposure factors, Security controls and services, Risk Evaluation and Mitigation strategies, Risk Assessment Techniques.

UNIT III BUILDING AND RUNNING A RISK MANAGEMENT PROGRAM 9Hrs

Threat and Vulnerability Management, Security Risk reviews, A Blueprint for security, Building a program from scratch.

UNIT IV INFORMATION SECURITY COMPLIANCE 9Hrs

Need for Information Security Compliance, Scope of IT Infrastructure ,Auditing for compliance - Auditing Standards and Frameworks.

UNIT V IT INFRASTRUCTURE AUDIT 9Hrs

Planning an IT Infrastructure audit for compliance, conducting an IT Infrastructure audit for compliance, writing the IT Infrastructure Audit Report.

Total No of Hours: 45

Reference Books:

1. Evan Wheeler,.*Security Risk Management: Building an Information Security Risk Management Program fromthe Ground Up.*
2. Martin Weiss andMichael G. Solomon.,*Auditing IT Infrastructures for Compliance (Information Systems Security & assurance)*
3. Michael E. Whitman , Herbert J. Mattord,(2010)*Management of Information Security Course Technology*(3rd ed.)
4. Ian Tibble,(2011) *Security De-Engineering: Solving the Problems in Information Risk Management*,(1st ed.),Auerbach Publications
5. Thomas R. Peltier,(2010) *Information Security Risk Analysis*, (3rd ed.),Auerbach Publications

MCS13IE13 THREAT MODELING AND SECURITY ARCHITECTURE DESIGN 3 0 0 3

OBJECTIVE:

- The students should understand the security about threat modelling and Understand the fundamentals of modelling and understand the requirements for an application to be deployed in a cloud and become knowledgeable in the methods to secure cloud.

UNIT I APPLICATION SECURITY & THREAT MODELING TERMINOLOGY 9Hrs

Application security life cycle – elements of Application Security- Roles in Application Security – Threat Modeling process – Determining threats- Organizing a threat Model. Adversary Goals – principles of dataflow application-analyzing entry points – determining the assets- trust level.

UNIT II CONSTRAINING AND MODELING THE APPLICATION 9Hrs

Gathering relevant background information – Modeling the Application through data flow diagrams- Identifying threats – Investigations-threats with threat trees-vulnerability resolution and migration – creating feature level – Application level threat models- reviewing the threat models – reviewing the threat model – modeling the system-testing based on threat models – making threat modeling work.

UNIT III ARCHITECTURE AND SECURITY 9Hrs

Architecture reviews - security Assessments – five-level compliance model - Security Architecture Basics-Architecture Patterns in security- low level Architecture – code review –buffer overflow exploits- cryptography -Toolkits–Hash functions – flaws- trusted code – Java sandbox –Microsoft Authenticode - secure communications.

UNIT IV MID-LEVEL ARCHITECTURE 9Hrs

Middleware security –Assumption of infallibility-CORBA security standard- web security – Issues – securing web clients – connection security – securing web server hosts – web server Architecture extension - Application and OS security –structure of an OS – structure of an application-securing network services- UNIX access control list-Database security- architectural components and security –role-based accessed control-database views – Oracle label security.

UNIT V HIGH-LEVEL ARCHITECTURE 9Hrs

Security components –secure single sign-on- public key infrastructure-firewalls –kerberos- security and other Architectural goals – force diagram around security – performance - portability- Enterprise security Architecture-security as a process –tools for data management – security pattern catalog - Building business cases for security-financial losses for computer theft – break-even analysis – Insurance and computer security.

Total No of Hours: 45

Reference Books:

1. Frank Swiderski, window snyder (2004)“*Threat Modeling*”, Microsoft press
2. Jay Ramachandran (2006)“*Designing Security Architecture Solutions*”, Wiley Publication
3. Marco *Morana*, Tony UcedaVelez “*Application Threat Modeling*” Wiley – 2013.
4. Mark Ciampa (2009)“*Security+ Guide to Network Security Fundamentals*” Cengage Learning

MCS13IE14 CYBER LAWS 3 0 0 3

OBJECTIVES:

- ➢ The students understand the basic information on cyber security andto understand the issues those are specific to amendment rights .
- ➢ To have knowledge on copy right issues of software's and understand ethical laws of computer for different countries

UNIT I 9Hrs

Modern Era : the Scene and Problems – Need for Cyber Laws – Impact of Internet & Information Technology – The Character and Use of Internet Technologies.

UNIT II 9Hrs

Reorganization of Electronic Records - UNICITRAL Model Law, Legal Aspects of Electronic Records / Digital Signatures - UNICITRAL Model Law, UNICITRAL Model Law : relating TO THE retention of Data Messages, Attributes of Data Messages, Acknowledgement of Data Messages, Time and Place receipt of Data Messages – Securing Electronic Record and electronic / Digital Signature in India – Verification of electronic Signature in India.

UNIT III 9Hrs

The Cyberspace – Protection of Copyrights of Cyber Space – Rights of Software Owners – Infringement of Copyright – remedies for infringement of Copyright on Cyberspace – The liabilities of an Internet Service Provider (ISP) in Cyberspace – Cyberspace and the Protection of Patents in India.

UNIT IV 9Hrs

Cyber Appellate tribunal - Its Function and Powers under IT Act – Obscenity and pornography on Cyberspace – Hacking on Cyberspace on Internet – Other Offences – violation of the Right of Privacy on Cyberspace / Internet – Punishment for violation of Privacy, Breach of Confidentiality and Privacy under the IT Act – Terrorism on Cyberspace / Internet.

UNIT V 9Hrs

An Overview of Cyber Crimes – Indian Evidence Act – Examiner of Electronics Act – Amendments Introduced in Indian Evidence Act, 1872 – IT Act as Amended upto 2008 – IT (Certifying Authorities) Rules, 2000 – Ministerial Order on Blocking of Websites – The IT (Use of Electronics Records and Digital Signatures) Rules 2004.

Total No of Hours: 45

Reference Books:

1. Harish Chander ,*Cyber Law & IT Protection*, Eastern Economy Edition
2. Jonathan Rosenor.*Cyber Law : the law of Internet*
3. Mark F Grady, FransescoParisi, *The Law and Economics of Cyber Security*
4. Roy J. Girasa and Roy J. Girasá (2001) ,*Cyberlaw: National and International Perspectives*

MCS13IE15 VIRUS PROGRAMMING 3 0 0 3

OBJECTIVE:

- The students will be able to understand the purpose of computer infection program.
- To implement the covert channel and mechanisms. and to test and exploit various malware in open source environment and to analyze and design the famous virus and worms.

UNIT I 9Hrs

Introduction – Definitions – Malware Defined - Virus Activity and Operation – Virus Mechanisms

UNIT II 9Hrs

Anti-Malware technology – Malware Management – Risk and Incident management – User Management.

UNIT III 9Hrs

Virus Origin and Distribution – Meta viruses, Hoaxes and Related Nuisances – Taxonomy , Techniques and Tools.

UNIT IV 9Hrs

Computer viruses in interpreted programming language – Companion viruses - Worms

UNIT V 9Hrs

Computer Viruses and Applications – BIOS Viruses – Applied Cryptanalysis of Cipher Systems

Total No of Hours: 45

Reference Books:

1. ÉricFiliol (2005) *Computer Viruses: from theory to applications* (Collection IRIS)
2. David Harley, Urs E. Gattiker and Eugene H. Spafford(2001) ,*Viruses Revealed*
3. Michael Sikorski and Andrew Honig (2012)*Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious software*
4. Peter Szor (2005)*The Art of Computer Virus Research and Defense*

MCS13IE16 ADVANCED DATABASES AND SECURITY 3 0 0 3

OBJECTIVE :

- The students should be able to do the following: Understand the role of a database management system in an organization.
- Understand basic database concepts, including the structure and operation of the relational data model Construct simple and moderately advanced database queries using Structured Query Language (SQL).

UNIT I INTRODUCTION 9Hrs

Review of Relational Databases , Special Purpose Databases - Temporal Databases – Active Databases – Spatial and Multimedia Databases – Deductive Databases – Mobile Databases. Introduction to data warehousing

UNIT II DISTRIBUTED DATABASES 9Hrs

Introduction – Architecture- Design – Query Processing – Transaction Management – Concurrency Control – Recovery – Parallel Databases.

UNIT III OBJECT ORIENTED DATABASES 9Hrs

Introduction - Basis OO Concepts – Modeling and Design for Object Oriented Databases – Persistence – Transaction, Concurrency, Recovery and Versioning.

UNIT IV DATABASE ACCESS CONTROL AND COMMUNICATION 9Hrs

Using Granular Access Control - Securing database-to-database communications – Encryption

UNIT V DATABASE SECURITY 9Hrs

The Database as a Networked Server - Authentication and Password Security - Application Security.

Total No of Hours: 45

Reference Books:

1. M. Timer, Ozsu and Patrick Valduriez, (1999)“*Principles of Distributed Database System*”, PHI

2.AbdullahUzTranselet-al, (1993)”Temporal databases-Theory design and implementation”, Benjamin/Cummings publishing co,

3. Ron Ben Natan “*Implementing Database Security and Auditing*” ELSEVIER DIGITAL PRESS.

4. Jennifer Wisdom & Stefano Ceri (Edited), (1996)“*Active Database Systems – Triggers & Rules for Advanced Database Processing*”, Morgan Kaufmann Publishers Inc

5. SetragKhosShafian, (1993)“*Object Oriented Databases*”, John Wiley & Sons IC.

6. SetragKhosshafian,Brad Baker,(1996)” *Multimedia And Imaging databases*”,Morgan Kaufmann