Dr.M.G.R.
Educational and Research Institute
(DEEMED TO BE UNIVERSITY)
(An ISO Certified Institution)
University with Graded Autonomy Status
Maduravoyal , Chennai - 600 095

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

CURRICULUM & SYLLABUS

(2018-REGULATION)

MASTER OF TECHNOLOGY

INFORMATION SECURITY AND CYBER FORENSICS

DEPARTMENT

OF

COMPUTER SCIENCE AND ENGINEERING/ INFORMATION TECHNOLOGY

DECLARATION

I, **Dr. S. GEETHA**, Head of Computer Science and Engineering Department, hereby declare that this copy of the syllabus (M.Tech – Information Security and Cyber Forensics - Full Time 2018 Regulation) is the final version which is being taught in the class and uploaded in our University website. I assure that the Syllabi available in our University website is verified and found correct. The Curriculum and Syllabi have been ratified by our Academic Council / Vice Chancellor.

Date: **Signature**

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

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

Curriculum and Syllabus 2018 Regulation - To be implemented from 2018-2019 Batch

I SEMESTER						
S.No	**Sub. Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS18I001	Information Security Management Systems	3	0	0	3
2	MCS18I002	Data Mining and Machine Learning For Information Security	3	1	0	4
3	MCS18I003	Advanced Computer Networks And Security	3	1	0	4
4	MCS18I004	Digital Forensics Investigation	3	0	0	3
5	MCS18I005	Operating System and Forensics	3	1	0	4
6	MCS18I006	Investigation on Cyber Attacks	3	1	0	4
7	MCS18IL01	Cyber Attacks Investigation Lab	0	0	3	1
8	MCS18IL02	Digital Crime Investigation lab	0	0	3	1
		Total	**18**	**4**	**6**	**24**

II SEMESTER						
S.No	**Sub. Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MMA18I007	Mathematics for Information Security and Cyber Forensics	3	1	0	4
2	MCS18I007	Information Security Risk Management and Auditing	3	1	0	4
3	MCS18I008	Applied Cryptography	3	1	0	4
4	MCS18I009	Penetration Testing and Vulnerability Analysis	3	1	0	4
5	MCS18IEXX	Elective - I	3	0	0	3
6	MCS18IL03	Term Project	0	1	3	2
7	MCS18IL04	Cryptography and Cryptanalysis lab	0	0	3	1
8	MCS18IL05	Penetration Testing & Vulnerability Assessment Lab	0	0	3	1
		Total	**15**	**5**	**9**	**23**

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

III SEMESTER						
S.No	**Sub. Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS18I010	Cyber Laws and IPR	3	1	0	4
2	MCS18IEXX	Elective - II	3	0	0	3
3	MCS18IEXX	Elective - III	3	0	0	3
4	MCS18IEXX	Elective - IV	3	0	0	3
5	MCS18IL06	Project Work Phase – I	0	0	6	3
		Total	**12**	**1**	**6**	**16**

IV SEMESTER						
S.No	**Sub. Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS18IL07	Project Work Phase – II	0	0	24	12
		Total	**0**	**0**	**24**	**12**

Summary of Credits:

1st Semester Credits 24
2nd Semester Credits 23
3rd Semester Credits 16
4th Semester Credits 12

TOTAL CREDITS TO BE EARNED FOR THE AWARD OF THE DEGREE: 75

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

ELECTIVE LIST

ELECTIVE – I						
S.No	**Sub. Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1	MCS18IE01	Virtualization and Cloud Security	3	0	0	3
2	MCS18IE02	Database Design and Security	3	0	0	3
3	MCS18IE03	Mobile Forensics	3	0	0	3
4	MCS18IE04	Business Continuity and Disaster Recovery	3	0	0	3

ELECTIVES – II,III, IV						
S.No	**Sub. Code**	**Title of Subject**	**L**	**T**	**P**	**C**
1.	MCS18IE05	Malware Forensics	3	0	0	3
2.	MCS18IE06	Network Forensics	3	0	0	3
3.	MCS18IE07	Intrusion Detection and Prevention Systems	3	0	0	3
4.	MCS18IE08	Threat Modeling and Security Architecture Design	3	0	0	3
5.	MCS18IE09	Internet Security	3	0	0	3
6.	MCS18IE10	Financial Frauds	3	0	0	3
7.	MCS18CE08	Pattern Recognition	3	0	0	3
8.	MCS18CE13	Social Network Analysis	3	0	0	3
9.	MCS18CE14	Principles of Secure Coding	3	0	0	3
10.	MCS18CE15	High Speed Networks and Security	3	0	0	3
11.	MCS18CE03	Secure Network Design	3	0	0	3
12.	MCS18CE17	Research Methodology	3	0	0	3

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I001	INFORMATION SECURITY MANAGEMENT SYSTEMS	3	0	0	3

OBJECTIVES:

- 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 9 Hrs

Information Security concepts - Critical Characteristics of Information - Components of an Information System, balancing information security and access – Systems Development Life Cycle Security SDLC – Security professionals and organization –communities Of interest

UNIT II SECURITY INVESTIGATION 9 Hrs

Need for Security - Business Needs - Threats – Attacks - secure software development - Legal, Ethical and Professional Issues in Information Security

UNIT III PLANNING FOR SECURITY 9 Hrs

Information security planning and governance – policy and practices- blue print for security – training and awareness – continuity strategies

UNIT IV SECURITY TECHNOLOGIES 9 Hrs

Access control – Firewalls – protecting remote connections- IDPS – Honey pots, honey nets and padded cell systems – scanning and analysis tools- biometric access controls

UNIT V IMPLEMENTING SECURITY 9 Hrs

Information Security Project management – technical and nontechnical aspects – certification and accreditations- credentials for security professionals- security management maintenance models

Total Hours: 45

REFERENCES:

1. *Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, New Delhi, 2003*
2. *Micki Krause, Harold F. Tipton, "Handbook of Information Security Management", Vol 1- CRC Press LLC, 2004.*
3. *Stuart Mc Clure, Joel Scram bray, George Kurtz, "Hacking Exposed", Tata McGraw-Hill, 2003*
4. *Matt Bishop, "Computer Security Art and Science", Pearson/PHI, 2002.*
5. *Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series by Jennifer Bayuk Sep 9, 2010.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I002	DATA MINING AND MACHINE LEARNING FOR INFORMATION SECURITY	3	1	0	4

OBJECTIVES:

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

UNIT I INTRODUCTION 12 Hrs

Cyber security, Data Mining, Machine Learning, Review of Cyber security 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 12 Hrs

Machine Learning, Improvements on Machine-Learning Methods, Challenges, Research Directions, Supervised Learning for Misuse/Signature Detection- Misuse/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 12 Hrs

Introduction, Anomaly Detection, Machine Learning in Anomaly Detection Systems, Machine-Learning Applications in Anomaly Detection, Machine 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 12 Hrs

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 12 Hrs

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

Total Hours: 60

REFERENCES:

1. *Data Mining and Machine Learning in Cyber security, Sumeet Dua and Xian Du, CRC Press Taylor and Francis Group,2011.*
2. *Machine Learning and Data Mining for Computer Security: Methods and Applications (Advanced Information and Knowledge Processing), Marcus A. Maloof, Springer; 1st Edition. Edition (September 1, 2005).*
3. *Data Mining: Practical Machine Learning Tools and Techniques, Third Edition (The Morgan Kaufmann Series in Data Management Systems) by Ian H. Witten, Eibe Frank and MarkA.Hall (Jan 20, 2011)*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I003	ADVANCED COMPUTER NETWORKS AND SECURITY	3	1	0	4

UNIT I INTERNETWORKING AND DATA SECURITY 12 Hrs

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

UNIT I I VoIP SECURITY 12 Hrs

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

UNIT III TELECOMMUNICATION SECURITY 12 Hrs

Introduction-Cellular Architecture-Basics of Security—Security problems in Telecommunication And cell network-Vulnerability in telephone, SMS, Data Network **.**

UNIT IV WIRELESS NETWORKS AND SECURITY 12 Hrs

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

UNIT V ADVANCED COMMUNICATION TECHNOLOGY 12 Hrs

Overview - Optical Networks - Advanced intelligent Networks-Home networking – 5G, IoE, Big data, Green Communication, VANET.

Total Hours: 60

REFERENCES:

1. *Walrand.J. Varaiya, High Performance Communication Network, Morgan Kauffman Harcourt Asia Pvt Ltd, 2nd Edition, 2000.*
2. *William Stallings ISDN & Broadband ISDN with frame Relay & ATM, PHI 4th Edtion 2000.*
3. *Uyless Black Emerging Communications Technologies2/e Prentice Hall 1997.*
4. *Bates & Donald W.Gregory Voice & Data Communications Handbook, Mc-Graw Hill, Edition, 3rd edition 2000.*
5. *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures by Peter Thermos and Ari Takanen (Aug 11, 2007).*
6. *Patrick Traynor, Patrick McDaniel, Thomas La Porta, Security for Telecommunication Network-Springer,2008.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I004	DIGITAL FORENSICS INVESTIGATION	3	0	0	3

OBJECTIVES:

- 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 9 Hrs

Foundations of Digital Forensics–

Language of computer crime investigation - digital evidence in the court room- 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 II DIGITAL INVESTIGATION 9 Hrs

Conducting digital investigation – Handling the digital crime scene -investigate reconstruction - Steganography, Data Acquisition and Duplication, Recovering Deleted files and Deleted Partitions,
Image file forensics

UNIT III APPREHENDING OFFENDERS 9 Hrs

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

UNIT IV EVIDENCE MANAGEMENT 9 Hrs

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 INVESTIGATION 9 Hrs

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 Hours: 45

REFERENCES:

1. *Digital Evidence and Computer Crime Forensic science, Computers and Internet - Eoghan Casey – Elsevier Academic Press –Third Edition*
2. *A Electronic Discovery and Digital Evidence in a Nut Shell-Shira A scheindlin, Daniel J Capra, The*
3. *Sedona Conference-Academic Press-Third Edition*
4. *Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk , 2010.*
5. *Handbook of Digital and Multimedia Forensic Evidence John J. Barbara*
6. *Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts Ali Jahangiri October, 2009.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I005	OPERATING SYSTEM AND FORENSICS	3	1	0	4

UNIT I OVERVIEW 12 Hrs

Introduction – evolution on operating System - Process management – states – threads –IPC – Memory – types of memory – Management – files system and file handling.

UNIT II FILE SYSTEM AND DATA RECOVERY 12 Hrs

Introduction – Disk handling – Booting – boot files- master boot record – Firmware - Files System: Windows, Linux, Apple - Hidden files systems. Data Recovery: Data Carving – searching deleted and sparse files - data hiding – Time stamping and lines – Volume shadow copies.

UNIT III MEMORY AND SYSTEM CONFIGURATION 12 Hrs

Memory : Real , Virtual and addressing –layout - capturing, analysis –paging and swapping, System Configuration: Windows- Linux-Mac OS X , Tracking Artifacts – Locating - tracking documents and shortcuts .

UNIT IV LOGS AND EXECUTABLE FILES 12 Hrs

Log files – windows, UNIX, Application, Mac OS X, Security and Auditing; Executable files: Stacks and heaps - Portable - Files formats – windows, Linux, Apple - CLR and JVM – Debugging – System Calls and tracing

UNIT V MOBILE OPERATING SYSTEM AND NEWER TECHNOLOGIES 12 Hrs

Introduction –Android , Blackberry , iOS Windows Mobile ; Newer Technologies - Virtualization, Cloud Computing , Wearables , Drones ; Report – Writing Style , requirements and considerations.

Total no. of Hours: 60

REFERENCES:

1. *Operating System Forensics, 1st Edition by R Messier Publisher: Syngress; 1 edition (27 November 2015)*
2. *Modern Operating System by Andrew S.Tanenbaum 3rd Edition, Pearson Education.*
3. *Security Strategies in Linux Platforms and Applications (Information Systems Security & Assurance) by Michael Jang (Sep 3, 2010)*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I006	INVESTIGATION ON CYBER ATTACKS	3	1	0	4

UNIT I OVERVIEW 12 Hrs

Hacking: Foundation for Ethical Hacking - Introduction to Ethical Hacking – Ethical Hacking framework - Hacking Methodology – Ethical Hacking in Motion- Social Engineering – Physical Security, **Cyber Attacks**: Definition- Factors - Types – Synthetic and Semantic attacks - Virus, Trojans and worms.

UNIT II OS ATTACKS 12 Hrs

Fundamentals of Computer Fraud – Threat concepts – Framework for predicting inside attacks – Managing the threat. Hacking: Windows – Linux and Novell NetWare hacking. Windows hacking : Vulnerabilities - Information gathering – File System – Polices ; Linux Hacking : Vulnerabilities -Information gathering – File System – File permission ; Novel NetWare - NetWare Vulnerabilities – Authentication and NetWare Security Risk management. Keyloggers- types and its Countermeasures; Introduction to Mobiles operating System – Android Windows , iOS and Black Berry.

UNIT III NETWORK ATTACKS 12 Hrs

Network attacks : War Dialing- General telephone-system vulnerabilities – attacks - Network Infrastructure - Scanning, Poking, and Prodding - Wireless LANs – Scanning - Wireless Network Attacks ; TCP / IP – Checksums ; Spoofing- IP, DNS ; Dos attacks – SYN attacks, Smurf attacks, UDP flooding, DDOS – Models. Firewalls – Packet filter firewalls, Packet Inspection firewalls – Application Proxy Firewalls. Intrusion detection system – NIDS, HIDS – Penetrating testing process – Web Services – Reducing transaction risks.

UNIT IV APPLICATION AND MOBILE ATTACKS 12 Hrs

Application attacks: Malware – types – testing – Countermeasures; Messaging Systems – Email – attacks; Web-Application - Vulnerabilities - Web hacking – Strategic Planning Process.- Architecture strategies for computer fraud prevention – Protection of Web sites –Phishing, Session Hijacking, Cross Site Scripting.(XSS) ,Cross Site Request Forgery (CSRF) Countermeasures ; A study on various attacks – Input validation attacks – SQL injection attacks, PHP Injections – Buffer overflow attacks - Privacy attacks. Email Analysis and Spam Mails, Proxy Servers, Spoofing, Banner Grabbing; Introduction to Mobile attacks

UNIT V CASE STUDIES ON ATTACKS 12 Hrs

Accounting Forensics – Computer Forensics; Reporting the results - Plugging Security – Managing security Challenges; Case study on the ethical hacking tools-wire shark, capsa, malware analysis and web data extraction with report.

Total Hours: 60

REFERENCES:

1. *Hacking for Dummies by by Kevin Beaver Published by Wiley Publishing, Inc.2004*
2. *Kenneth C.Brancik "Insider Computer Fraud" Auerbach Publications Taylor & Francis Group– 2008.*
3. *Ankit Fadia " Ethical Hacking" second edition Macmillan India Ltd, 2006*
4. *Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts... by Ali Jahangiri (Oct 21, 2009)*
5. *Ethical hacking countermeasures - An Ultimate Guide For Ethical Hackers [Paperback]Mr. Lomeaskesh kumar (Author), September 1, 2014.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IL01	CYBER ATTACKS INVESTIGATION LAB	0	0	3	1

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

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IL02	DIGITAL CRIME INVESTIGATION LAB	0	0	3	1

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 lab 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. 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

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 reports
- 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.

.

Dr.M.G.R Educational and Research Institute, University, Chennai–95.

MMA18I007	MATHEMATICS FOR INFORMATION SECURITY AND CYBERFORENSICS	L T P C 3 1 0 4

(I yr. / II Sem. M.Tech (Full Time) – CSE (ISCF))

[2013 batch onwards]

UNIT I INTRODUCTION TO ABSTRACT ALGEBRA **(12 hrs)**

Groups (Definition and Examples) – Subgroups – Permutation groups – Homomorphism – Kernel – Cosets – Lagrange's theorem – Rings – Fields (Definition and Examples).

UNIT II COMBINATORICS **(12 hrs)**

Mathematical Induction – Pigeon Hole Principle – Principle of Inclusion and Exclusion – Recurrence Relations – Generating Functions.

UNIT I MATHEMATICAL LOGIC **(12 hrs)**

Statements – Truth Table – Connectives – Normal Forms – Predicate Calculus – Inference Theory.

UNIT IV DISCRETE STRUCTURES I **(12 hrs)**

Basic concepts of Graphs – Sub graphs – Paths and Circuits – Matrix representation of Graphs – Graph Isomorphism – Connected graphs and Components – Euler and Hamiltonian paths – Travelling salesman problem.

UNIT V DISCRETE STRUCTURES II **(12 hrs)**

Basic concepts of Trees– Properties – Pendant vertices – Rooted and Binary trees – Spanning trees – Fundamental circuits – Finding all spanning trees of a graph – Spanning trees in a weighted graph.

Total no. of hrs: 60

Reference Books:

1) Tremblay J.P., Manohar R., *Discrete Mathematical structures with applications to Computer science*, Tata McGraw Hill Publishing Co., (2004).
2) Kenneth Rosen, *Discrete Mathematics and its applications (SIE)*, Tata McGraw Hill Publishing Co., (2007).
3) John C. Martin, *Introduction to languages and the theory of computation (3rd ed.)*, Mcgraw Hill, (2003).
4) Hopcroft J.E., Ullman J.D., *Introduction to Automata theory, Languages and Computation*, Narosa Publishing house, (2002).
5) Narsingh Deo, *Graph theory with applications to Engineering and Computer Science*, Prentice Hall of India, (2004).
6) Robin J. Wilson, *Introduction to Graph theory (4th ed.)*, Pearson, (2002).

applicable to 2016 Reg too
24.2.17

24-2-17

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I007	INFORMATION SECURITY RISK MANAGEMENT AND AUDITING	3	1	0	4

OBJECTIVES:

- The students will be able to gain the knowledge about Information 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 12 Hrs

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

UNIT II RISK ASSESSMENT AND ANALYSIS TECHNIQUES 12 Hrs

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 12 Hrs

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

UNIT IV INFORMATION SECURITY COMPLIANCE 12 Hrs

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

UNIT V IT Infrastructure Audit 12 Hrs

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

Total Hours: 60

REFERENCES:

1. *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Evan Wheeler, 2011 Elsevier Inc.*
2. *Auditing IT Infrastructures for Compliance (Information Systems Security & assurance) by Martin Weiss and Michael G. Solomon, Jones & Bartlett Publishers, September 2010.*
3. *Management of Information Security, Michael E. Whitman (Author), Herbert J. Mattord Course Technology; 3 edition (January 19, 2010)*
4. *Security De-Engineering: Solving the Problems in Information Risk Management, Ian Tibble Auerbach Publications; 1 edition (December 13, 2011)*
5. *Information Security Risk Analysis, Third Edition, Thomas R. Peltier (Author), Auerbach Publications; 3 edition (March 16, 2010)*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I008	APPLIED CRYPTOGRAPHY	3	1	0	4

OBJECTIVES:

- 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 I MATHEMATICAL FOUNDATION 12 Hrs

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 II CRYPTOGRAPHIC PROTOCOLS 12 Hrs

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 III CRYPTOGRAPHIC TECHNIQUES 12 Hrs

Key Length: Symmetric key Length, Public Key Key length-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 IV CRYPTOGRAPHIC ALGORITHMS 12 Hrs

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 V IMPLEMENTATION 12 Hrs

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 Hours: 60

REFERENCES:

1. *Applied Cryptography: Protocols, Algorithms and source code in C, Wiley, Second Edition-Bruce Schneier (OCT 18, 1996)*
2. *Cryptography and Network Security Principles and practices-William Stallings (Jan 24, 2010)*
3. *Foundations of Cryptography: Volume 1, Basic Tools by Oded Goldreich (Jan 18, 2007)*
4. *Encryption: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity... by Kevin Roebuck, Emereo pty Limited, 2011.*
5. *Foundations of Cryptography: Volume 2, Basic Applications by Oded Goldreich (Sep 17, 2009)*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I009	PENETRATION TESTING AND VULNERABILITY ANALYSIS	3	1	0	4

UNIT I PENETRATION TESTING 12 Hrs

Introduction to Kali and Backtrack-Linux tools – Attack Machine- Phases of penetration test- reconnaissance extracting information from DNS-scanning-pings and ping sweeps-port scanning- NMap-Vulnerability scanning

UNIT II EXPLOITATION 12 Hrs

Gaining access to remote services-metasploit-password crackers- local and remote password cracking-password resetting-Wire shark-social engineering-website attack vectors-web based exploitation-interrogating web servers – Spidering- code injection attacks- cross-site scripting- post exploitation- maintaining access with backdoors, root kits and meterpreter

UNIT III DATA COLLECTION REPORTING TOOLS 12 Hrs

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 12 Hrs

Command shell scripting –Python basics – File Manipulation – network communications – Introduction to Perl – Perl Basics- working with Perl- Introduction to Ruby- building classes with ruby- Introduction to Web scripting with PHP – Manipulating windows with Power shell – Scanner Scripting – Exploitation Scripting – Post Exploitation Scripting.

UNIT V TOOLS AND CASE STUDIES 12 Hrs

Penetration Testing Tools: information gathering, web application testing, infrastructure testing Vulnerability Assessment Tools: network security scanners and web security scanners- case studies

Total Hours: 60

REFERENCES:

1. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Engebretson Elsevier Publication, 2nd Edition.*
2. *Penetration Testing: Hacking and Penetration Testing, an Ultimate Security Guide (Python, Ethical Hacking, Basic Security) (Learning Hacking, Penetration Testing and Programming) by D. James Smith, 2015.*
3. *Penetration Tester's Open Source Toolkit, Third Edition by Jeremy Faircloth, 2011.*
4. *Coding for Penetration Testers: Building Better Tools by Jason Andress and Ryan Linn, 2011*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IL03	TERM PROJECT	0	1	3	2

OBJECTIVES:

- 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.

Course Code	Course Title	L	T	P	C
MCS18IL04	CRYPTOGRAPHY AND CRYPTANALYSIS LAB	0	0	3	1

OBJECTIVES:

To implement the following list of 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

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IL05	PENETRATION TESTING & VULNERABILITY ASSESSMENT LAB	0	0	3	1

OBJECTIVES:

To implement the following list of programs

1. Network Mapping & Target Identification
   a. Analysis of output from tools used to map the route between the engagement point and a number of targets.
   b. Network sweeping techniques to prioritize a target list and the potential for false negatives.
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:
   - modifying source ports
   - Spoofing IP addresses
   - Manipulating TTL's
   - Fragmentation
   - Generating ICMP packets
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:
   - Routers
   - Switches
9. Unix Security Assessment
   a. User enumeration- Discovery of valid usernames from network services commonly running by default:
   - rusers
   - rwho
   - SMTP
   - finger

   b. Unix vulnerabilities - Common post-exploitation activities:
   - exfiltrate password hashes
   - crack password hashes
   - check patch levels
   - derive list of missing security patches
   - reversion to previous state

   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 and VRFY

Awareness of recent Send mail vulnerabilities; ability to exploit them if possible.
Mail relaying

10. Web Testing Techniques

a. Web Site Structure Discovery-

- Spidering tools and their relevance in a web application test for discovering linked content.
- Forced browsing techniques to discover default or unlinked content

b. Cross Site Scripting Attacks

- Arbitrary JavaScript execution.
- Using Cross Site Scripting techniques to obtain sensitive information from other users.
- Phishing techniques.

c. SQL Injection

- Determine the existence of an SQL injection condition in a web application.
- Determine the existence of a blind SQL injection condition in a web application.
- Exploit SQL injection to enumerate the database and its structure.
- Exploit SQL injection to execute commands on the target server.

d. Session ID Attacks

- Investigate session handling within a web application.
- Harvest and analyze a number of session identifiers for weaknesses.

e. Data Confidentiality & Integrity

- Identifying weak (or missing) encryption.
- Identifying insecure SSL configurations.

f. Directory Traversal

- Identifying directory traversal vulnerabilities within applications.

g. Code Injection

- Investigate and exploitation of code injection vulnerabilities within web applications

h. Application Logic Flaws

- Assessing the logic flow within an application and the potential for subverting the logic

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18I010	CYBER LAWS AND IPR	3	1	0	4

OBJECTIVES:

- To understand the basic information on cyber security and issues those are specific to IT Act
- To have knowledge on Cyber tribunal
- To acquire specialized knowledge of law and practice relating to IPR

UNIT I INTRODUCTION 12 Hrs

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 II CYBER SPACE 12 Hrs

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 III CYBER TRIBUNAL 12 Hrs

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 IV CYBER CRIMES 12 Hrs

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.

UNIT V IPR 12 Hrs

Patents- Patent databases-patent information system- preparation of patent documents-trademarks- copyrights-industrial designs-geographical indication- protection of trade secrets-management and valuation of intellectual property

Total Hours: 60

REFERENCES:

1. *Cyber Law & IT Protection, Eastern Economy Edition, by Harish Chander.*
2. *Cyber Law: the law of Internet – Jonathan Rose nor, Springer, 1997.*
3. *The Law and Economics of Cyber Security – Mark F Grady, Francesco Parisi, August 2011.*
4. *Cyber law: National and International Perspectives by Roy J. Girasa and 2001*
5. *Intellectual Property Rights – Law and Practice Institute of Company Secretaries of India2014*
6. *Law Relating to Patents, Trademarks, Copyright, Designs and Geographical Indications by B L Wadehra ISBN-13: 978-8175341852 Universal Book Traders; 2nd edition*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IL06	PROJECT WORK PHASE – I	0	0	6	3

OBJECTIVES:

- Title Identification
- Title Confirmation
- Problem Scenario and Definition
- Feasibility Study and Requirement Specification
- Solution Approach
- Architectural Design / Data Flow Design
- Solution Design and Workflow

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IL07	**PROJECT WORK PHASE – II**	**0**	**0**	**24**	**12**

OBJECTIVES:

- Detailed Design and Implementation
- Test Plan
- Partial Demo
- Packaged Demo
- Documentation verification

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE01	VIRTUALIZATION AND CLOUD SECURITY	3	0	0	3

OBJECTIVES:

- 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
- 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 VIRTUALIZATION ARCHITECTURE 9 Hrs

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

UNIT II VIRTUAL NETWORK SECURITY 9 Hrs

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 VIRTUALIZATION MANAGEMENT 9 Hrs

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 CLOUD COMPUTING 9 Hrs

Cloud computing basics - cloud computing services: IaaS, PaaS, SaaS Software plus services - Evolution-Cloud Data Center-Collaboration – SOA- Basic approach to data center based SOA-Role of open source software and usage.

UNIT IV CLOUD SECURITY 9 Hrs

Risk Model- Risk treatment – Security Assessment – Virtual Overlays – Malware – Attacks – cloud data Security and Storage - Security as a Service- Security Management in Cloud. **Total Hours: 45**

REFERENCES:

1. *Virtualization Security: Protecting Virtualized Environments - Dave Shacklef Wiley Publications, December 2012.*
2. *Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability,* ***Forensic Analysis, and... By John Hoopes, 1st Edition.***
3. *Cloud Computing, A Practical Approach, Toby Velte, Anthony Velte, Robert Elsenpeter, McGraw Hill, ISBN: 9780070683518, 2010.*
4. *Cloud Computing Implementation, Management, and Security, John W. Rittenhouse, James F. Ransome, August 2009.*
5. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) by Tim Mather, Subra Kumaraswamy and Shahed Latif, 1st Edition.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE02	DATA BASE DESIGN AND SECURITY	3	0	0	3

OBJECTIVES:

- Students would be able to Design and implement relational database solutions for general applications.
- Develop database scripts for data manipulation and database administration.
- Understand and perform common database administration tasks, such as database monitoring, performance tuning, data transfer, and security.
- To balance the different types of competing resources in the database environment so that the most important applications have priority access to the resources
- 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 TO DATABASES 9 Hrs

Database Environment Database Architectures, The Relational Model, Relational Algebra and Relational Calculus, SQL: Data Manipulation, SQL: Data Definition, Query-By-Example

UNIT II DATABASE ANALYSIS AND DESIGN 9 Hrs

Database System Development Lifecycle ,Entity-Relationship Modeling, Enhanced Entity-Relationship Modeling, Normalization, Conceptual Database Design ,Logical Database Design for the Relational Model, Physical Database Design for Relational Databases

UNIT III TRANSACTION PROCESSING 9 Hrs

Transaction concept, concurrent execution, isolation, testing for serializability, Concurrency control, lock based - time-stamp based - validation based protocols, multi-version schemes, deadlock handling.

UNIT IV DATABASE SECURITY 9 Hrs

Introduction to database security, security models, physical and logical security, security requirements, reliability and integrity, sensitive data, inference, multilevel databases and multilevel security, access control-mandatory and discretionary , security architecture, issues.

UNIT V SECURITY ISSUES 9 Hrs

Application access, security and authorization, authorization in SQL, encryption and authentication, secure replication mechanisms, Audit- logon/logoff, sources, usage and errors, changes, external audit system architecture, archive and secure auditing information **Total Hours: 45**

REFERENCES:

1. *Abraham Silberschatz, Hanry F Korth, Sudarshan S, "Database Systems Concepts", McGraw Hill, 2007.*
2. *Thomas M Connolly, Carolyn E Begg, Database Systems A Practical Approach to Design Implementation and Management, (3rd ed.), Addison Wesley.*
3. *Ron Ben Natan, "Implementing database security and auditing", Elsevier publications, 2005.*
4. *Hassan A. Afyduni, "Database Security and Auditing", Course Technology – Cengage Learning, New Delhi, 2009.*
5. *Raghu Ramakrishnan, "Database Management Systems", McGraw Hill/ Third Edition, 2003*
6. *Ramez Elmasri, Shamkant B. Navathe , "Fundamentals of Database System" Addison Wesley, New Delhi/Fourth Edition 2004*
7. *M. Gertz, and S. Jajodia, Handbook of Database Security- Application and Trends, 2008, Springer.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE03	MOBILE FORENSICS	3	0	0	3

OBJECTIVES:

- To understand the basics of mobile operating systems
- Acquire the data from mobile devices using forensically sound and industry standard tools
- Understand the relationship between mobile and desktop devices in relationship to a criminal and corporate investigations
- Be able to analyze mobile devices, their backup files, and artifacts for forensic evidence

UNIT I INTRODUCTION 9 Hrs

Introduction to mobile forensics – evidence extraction process – removable and external data Storage – phases of examination - using multiple tools and comparing results – forensic Approaches Mobile OS- Mobile forensics tool leveling systems- data acquisition methods

UNIT II iOS 9 Hrs

iOS device: internals, hardware, file system - iOS: architecture, security- iOS data - Acquisition, backups, analysis and recovery

UNIT III ANDROID 9 Hrs

Android: Introduction, model, file systems- Android data: forensic setup, extraction Techniques, backup, recovery and analysis

UNIT IV WINDOWS AND BLACKBERRY 9 Hrs

Windows phone OS - model – data acquisition and extracting – Blackberry OS- architecture – Data acquisition and analysis – backup

UNIT V CASE STUDY 9 Hrs

Mobile investigation: iOS, Android, Windows and Blackberry

Total Hours: 45

REFERENCES:

1. *Practical Mobile Forensics by Satish Bommisetty , Rohit Tamma , Heather Mahalik Packet Publishing Limited (June 2014) ISBN-13: 978-1783288311*
2. *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation by Lee Reiber McGraw-Hill Education (1 March 2016) ISBN-13: 978-0071843638*
3. *File System Forensic Analysis Paperback – Import, 17 Mar 2005 by Brian Carrier Publisher: Addison Wesley ISBN-13: 978-0321268174*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE04	BUSINESS CONTINUITY AND DISASTER RECOVERY	3	0	0	3

OBJECTIVES:

- 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 Management Basics 9 Hrs

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 9 Hrs

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 III Disaster Recovery 9 Hrs

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 9 Hrs

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 9 Hrs

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

Total Hours: 45

REFERENCES:

1. *Business Continuity and Disaster Recovery Planning for IT Professionals Susan Snedaker (Author), (Jul 5, 2007)*
2. *Disaster Recovery and Business Continuity Second Edition, B S Thejendra,(Jan 8,2008)*
3. *Business Continuity and Disaster Recovery for InfoSec Managers, John Rittenhouse PhD CISM James F. Ransome PhD CISM CISSP, (Oct 4, 2004)*
4. *Business Continuity and Disaster Recovery: Getting Started Guide Concepts and Definitions for Common Sense Planning Deborah C. Miller (Nov 12, 2011)*
5 *Guide to Disaster Recovery, Michael Erbschloe, (March 10, 2003)*
6. *Disaster Recovery and Business Continuity IT Planning, Implementation, Management and Testing of Solutions and Services Workbook Gerard Blokdijk Jackie Brewster, Ivanka 2008.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE05	MALWARE FORENSICS	3	0	0	3

OBJECTIVES:

- To analyze the malware and its functionalities
- To analyze the code for malware
- To perform malware forensics

UNIT I MALWARE ANALYSIS 9 Hrs

Basic Static Techniques - Malware Analysis in Virtual Machines - Basic Dynamic Analysis - IDA Pro - Analyzing Malicious Windows Programs – Debugging

UNIT II MALWARE FUNCTIONALITY 9 Hrs

Malware Behavior - Covert Malware Launching -Data Encoding - Malware-Focused Network Signatures.

UNIT III ANTI-REVERSE-ENGINEERING 9 Hrs

Anti-Disassembly-Anti-Debugging - Anti-Virtual Machine Techniques- Packers and Unpacking.

UNIT IV CODE ANALYSIS 9 Hrs

Shell code Analysis - C++ Analysis- 64-Bit Malware – Tools for Malware Analysis

UNIT V MALWARE FORENSICS 9 Hrs

Discovering Alternate Data Streams with TSK - Detecting Hidden Files and Directories with TSK- Finding Hidden Registry Data with Microsoft's Offline API -Bypassing Poison Ivy's Locked Files Bypassing Conficker's File System ACL Restrictions - Scanning for Root kits With GMER - Detecting HTML Injection by Inspecting IE's DOM - Registry Forensics with RegRipper Plug-ins - Detecting Rogue-Installed PKI Certificates - Examining Malware that Leaks Data into the Registry.

Total Hours: 45

REFERENCES:

1. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious by Michael Sikorski, Andrew Honig 1st Edition.*
2. *Malware Analyst's Cookbook: Tools and Techniques for Fighting Malicious Code by Michael Ligh , Steven Adair , Blake Hartstein, Matthew Richard, 2nd Edition.*
3. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh, Kindle Edition.*
4. *Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides by Cameron H. Malin, Eoghan Casey, James M. Aquiline 1st Edition.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE06	NETWORK FORENSICS	3	0	0	3

OBJECTIVES:

- 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 FOUNDATION 9 Hrs

Practical investigative strategies- footprints- concepts in digital evidence- challenges- investigative methodology- sources of network based evidence- principles of internetworking-IP suite- Evidence acquition

UNIT II TRAFFIC ANALYSIS 9 Hrs

Packet analysis: protocol analysis, analysis tools and techniques- flow analysis- higher layer traffic analysis – case studies – Statistical Flow analysis: sensors-flow record export protocols, collection and aggregation-analysis tools and techniques

UNIT III WIRELESS NETWORK FORENSICS 9 Hrs

IEEE Protocol series- WAPs- Wireless traffic capture analysis- common attacks-location wireless devices-NIDS/NIPS functionality- modes of detection-types-evidence acquisition – evidence types-NIPS/NIDS interfaces

UNIT IV NETWORK DEVICES AND SERVERS 9 Hrs

Sources of Logs-Network log architecture- collecting and analyzing evidence- L0ne Sh4rk's Revenge case study – Storage media-switches-routers – firewalls- interface-logging- web proxy functionality- evidence-squid- web proxy analysis – encrypted web traffic

UNIT V ADVANCED TOPICS 9 Hrs

Tunneling for functionality, confidentiality- covert tunneling- trends in malware evolution-network behavior of malware – future of malware and network forensics - Case study: Network Forensics tools

Total Hours: 45

REFERENCES:

1. *Network Forensics : Tracking Hackers Through Cyberspace Sherri Davidoff, Jonathan Ham Pearson Education 2012*
2. *Introduction to Security and Network Forensics William J. Buchanan Auerbach Publications 2012*
3. *Handbook of Digital Forensics and Investigations, Eoghan Casey ed., Elsevier Academic Press, ISBN 13: 978-0-12-374267-4, 1st Edition.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE07	INTRUSION DETECTION AND PREVENTION SYSTEMS	3	0	0	3

OBJECTIVES:

- Understand and implement classes of attack to computer systems
- Have a good grasp of the design and implementation of signature based and anomaly based techniques to solve problems related to intrusion detection and prevention.
- Employ ID&PS specific feature extraction techniques and machine learning skills to applied industry or research problems.
- Collaborate with team members to deliver a solution with limited resources and time.

UNIT I NETWORK ATTACKS 9 Hrs

Network attacks – detection approaches – data collection - Theoretical Foundations Of Detection: Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering

UNIT II ARCHITECTURE AND IMPLEMENTATION 9 Hrs

Centralized – Distributed – Cooperative Intrusion Detection – Alert management and correlation- Evaluation Criteria - Intrusion response – Response type, approach-Survivability and intrusion tolerance- Commercial and Open Source IDS

UNIT III IDP PRINCIPLES 9 Hrs

Intrusion detection and prevention principles- Common detection methodologies: Signature based, anomaly based detection, stateful protocol analysis- types of IDPS technologies-IDPS components and architecture – security capabilities - management

UNIT IV NETWORK BASED IDPS 9 Hrs

Networking overview- components and architecture- security capabilities- Management- Wireless IDPS : WLAN standards, components, sensor locations- information gathering capabilities- logging and detection capabilities-operation and maintenance – Network Behavior Analysis (NBA) systems – Host-based IDPS

UNIT V SECURITY AND IDS MANAGEMENT 9 Hrs

Data correlation – Incident response – policy and procedures – laws, standards and organizations- security business issues – future of intrusion detection and prevention

Total no. of Hours: 45

REFERENCES:

1. *Ali A. Ghorbani, Wei Lu, "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer, 2010.*
2. *Karen Scarf one Peter Mell "Guide to Intrusion Detection and Prevention Systems (IDPS)" NIST Publication*
3. *Carl Enrolf, Eugene Schultz, Jim Millender, "Intrusion detection and Prevention", McGraw Hill, 2004*
4. *Paul E. Proctor, "The Practical Intrusion Detection Handbook ", Prentice Hall, 2001.*
5. *Earl Carter, Jonathan Hogue, "Intrusion Prevention Fundamentals", Pearson Education, 2006.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE08	THREAT MODELING AND SECURITY ARCHITECTURE DESIGN	3	0	0	3

OBJECTIVES:

- The students should understand the security about threat modeling
- Understand the fundamentals of modeling
- 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 9 Hrs

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 9 Hrs

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 9 Hrs

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 9 Hrs

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 9 Hrs

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 Hours: 45

REFERENCES:

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

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE09	INTERNET SECURITY	3	0	0	3

OBJECTIVES:

- 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 Hours: 45

REFERENCES:

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*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18IE10	FINANCIAL FRAUDS	3	0	0	3

UNIT I CORPORATE GOVERNANCE 9 Hrs

Corporate governance structure- definition, role, characteristics, corporate governance functions, global corporate governance. Audit committees, Internal and external audits, Governing bodies.

UNIT II FRAUD IN DIGITAL ENVIRONMENT 9 Hrs

Digital economy, Electronic commerce, Changes in business environment, Electronic financial reporting, Fraud examination, forensic accounting, Anti fraud applications.

UNIT III TYPES OF FRAUD 9 Hrs

Fraud against organization, consumer fraud, Bankruptcy, divorce and tax fraud, fraud in E-Commerce.

UNIT IV PREVENTION AND DETECTION FRAUD 9 Hrs

Nature of fraud, reason to commit fraud, fighting fraud-overview, prevention, recognizing the symptoms, Data driven fraud detection, Financial reporting structure, Taxonomy and schemes.

UNIT V INVESTIGATION AND MANAGEMENT 9 Hrs

Investigating theft acts, investigating concealment, conversion investigation methods, Inquiry methods and fraud reports, financial statement fraud, Liability, asset and inadequate disclosure frauds.

Total Hours: 45

REFERENCES:

1. *Financial Statement Fraud: Prevention and Detection abihollah Rezaee, Richard Riley, 2nd Edition, 2010.*
2. *Fraud Examination W. Steve Albrecht, Chad O. Albrecht, Conan C. Albrecht, Mark F. Zimbelman, 4th edition, 2011.*
3. *Fraud Auditing and Forensic Accounting, Tommie W. Singleton, Aaron J. Singleton, 4th edition.*
4. *Essentials of Corporate Fraud, Tracy L. Coenen, publisher John Wiley &son, 2008.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18CE08	PATTERN RECOGNITION	3	0	0	3

OBJECTIVES:

- To understand the concepts of Pattern recognition and machine learning.
- To appreciate supervised and unsupervised learning and their applications.
- To understand the theoretical and practical aspects of Probabilistic Graphical Models and concepts and algorithms of reinforcement learning and learn aspects of computational learning theory.

UNIT I PATTERN RECOGNITION 9 Hrs

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 CLUSTERING AND CLASSIFICATION 9 Hrs

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

UNIT III STRUCTURAL PATTERN RECOGNITION 9 Hrs

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 9 Hrs

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

UNIT V RECENT ADVANCES 9 Hrs

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 Hours: 45

REFERENCES:

1. *Robert J.Schalkoff (1992), Pattern Recognition : 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*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18CE13	SOCIAL NETWORK ANALYSIS	3	0	0	3

OBJECTIVES:

- To gain knowledge about the current Web development and emergence of Social Web.
- To study about the modeling, aggregating and knowledge representation of Semantic Web.
- To learn about the extraction and mining tools for Social networks.
- To gain knowledge on Web personalization and Web Visualization of Social networks.

UNIT I INTRODUCTION TO SOCIAL NETWORK ANALYSIS 9 Hrs

Introduction to Web - Limitations of current Web – Development of Semantic Web – Emergence of the Social Web - Network analysis - Development of Social Network Analysis - Key concepts and measures in network analysis - Electronic sources for network analysis - Electronic discussion networks, Blogs and online communities, Web-based networks - Applications of Social Network Analysis.

UNIT II MODELLING, AGGREGATING AND KNOWLEDGE REPRESENTATION 9 Hrs

Ontology and their role in the Semantic Web - Ontology-based Knowledge Representation – Ontology languages for the Semantic Web – RDF and OWL - Modeling and aggregating social network data - State-of-the-art in network data representation, Ontological representation of social individuals, Ontological representation of social relationships, Aggregating and reasoning with social network data, Advanced Representations.

UNIT III EXTRACTION AND MINING COMMUNITITES IN WEB SOCIAL NETWROKS 9 Hrs

Extracting evolution of Web Community from a Series of Web Archive - Detecting Communities in Social Networks - Definition of Community - Evaluating Communities - Methods for Community Detection & Mining - Applications of Community Mining Algorithms - Tools for Detecting Communities Social Network Infrastructures and Communities - Decentralized Online Social Networks- MultiRelational Characterization of Dynamic Social Network Communities.

UNIT IV PREDICTING HUMAN BEHAVIOR AND PRIVACY ISSUES 9 Hrs

Understanding and Predicting Human Behaviour for Social Communities - User Data Management, Inference and Distribution - Enabling New Human Experiences - Reality Mining - Context-Awareness - Privacy in Online Social Networks - Trust in Online Environment - Trust Models Based on Subjective Logic - Trust Network Analysis - Trust Transitivity Analysis - Combining Trust and Reputation – Trust Derivation Based on Trust Comparisons - Attack Spectrum and Countermeasures.

UNIT V VISUALIZATION AND APPLICATIONS OF SOCIAL NETWORKS 9 Hrs

Graph Theory- Centrality- Clustering - Node-Edge Diagrams, Matrix representation, Visualizing Online Social Networks, Visualizing Social Networks with Matrix-Based Representations- Matrix + Node-Link Diagrams, Hybrid Representations - Applications - Covert Networks - Community Welfare - Collaboration Networks - Co-Citation Networks.

Total Hours: 45

REFERENCES:

1. *Peter Mika, "Social networks and the Semantic Web", Springer, 1st edition 2007.*
2. *Borko Furht, "Handbook of Social Network Technologies and Applications", Springer, 1st edition, 2010.*
3. *Guangdong Xu, Yanchun Zhang and Lin Li, "Web Mining and Social Networking Techniques and applications", Springer, 1st edition, 2011.*
4. *Dion Goh and Schubert Foo, "Social information retrieval systems: emerging technologies and applications for searching the Web effectively", IGI Global snippet, 2008.*
5. *Max Chevalier, Christine Julien and Chantal Soulé-Dupuy, "Collaborative and social information retrieval and access: techniques for improved user modeling", IGI Global snippet, 2009.*
6. *John G. Breslin, Alexandre Passant and Stefan Decker, "The Social Semantic Web", Springer, 2009*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18CE14	PRINCIPLES OF SECURE CODING	3	0	0	3

OBJECTIVES:

- To learn about the need for secure system.
- To understand the issues in secure coding techniques.
- To understand the socket security.

UNIT I INTRODUCTION 9 Hrs

The Need for Secure Systems: Applications on the World Wild Web, The Need for Trustworthy Computing, **the Proactive Security Development Process:** Process Improvements**,** The Role of Education, Design Phase , Development Phase, Test Phase , **Security Principles to Live By**: SD3: Secure by Design, by Default, and in Deployment, Security Principles, **Threat Modeling:** Secure Design Through Threat Modeling, Security Techniques.

UNIT II CODING TECHNIQUES 9 Hrs

The Buffer Overrun: Stack Overruns, Heap Overruns ,Array Indexing Errors, Format String Bugs, Preventing Buffer Overruns, **Determining Appropriate Access Control :** Why ACLs Are Important, Creating ACLs, NULL DACLs and Other Dangerous ACE Types **Cryptographic Foibles**: Using Poor Random Numbers, Using Passwords to Derive Cryptographic Keys, Key Management Issues, Using the Same Stream-Cipher Encryption Key, Bit-Flipping Attacks Against Stream Ciphers, Reusing a Buffer for Plaintext and Cipher text , Using Crypto to Mitigate Threats.

UNIT III DATABASE AND WEB SPECIFIC INPUT ISSUES 9 Hrs

Protecting Secret Data : Attacking Secret Data, Managing Secrets in Memory, Locking Memory to Prevent Paging Sensitive Data ,Protecting Secret Data in Managed Code, Raising the Security Bar , **Database Input Issues**: The Issue , Pseudo remedy #1: Quoting the Input , Pseudo remedy #2: Use Stored Procedures , Remedy #1: Never Ever Connect as sysadmin, Remedy #2: Building SQL Statements Securely ,**Web-Specific Input Issues:** Other XSS-Related Attacks, XSS Remedies.

UNIT IV SOCKET SECURITY 9 Hrs

Socket Security: Avoiding Server Hijacking, TCP Window Attacks, Choosing Server Interfaces, Accepting Connections, Writing Firewall-Friendly Applications, Spoofing and Host-Based and Port-Based Trust, **Securing RPC**, **ActiveX Controls, and DCOM:** An RPC Primer, Secure RPC Best Practices, Secure DCOM Best Practices, **Protecting against Denial of Service Attacks:** Application Failure Attacks, CPU Starvation Attacks, Memory Starvation Attacks, Resource Starvation Attacks, Network Bandwidth Attacks

UNIT V SECURITY TESTING AND DOCUMENTATON 9 Hrs

Security Testing: The Role of the Security Tester, Building Security Test Plans from a Threat Model, Testing Clients with Rogue Servers , Testing with Security Templates, Determining Attack Surface, **Secure Software Installation:** Using the Security Configuration Editor, Low-Level Security APIs, Using the Windows Installer**, Building Privacy into Your Application:** Major Privacy Legislation, Privacy vs. Security, Building a Privacy Infrastructure**,** Designing Privacy-Aware Applications**, Writing Security Documentation and Error Messages:** Security Issues in Documentation, Security Issues in Error Messages, A Tyspical Security Message, Information Disclosure Issues

Total Hours: 45

REFERENCES:

1. *Michael Howard, David LeBlanc, "Writing Secure Code", Microsoft Press, 2nd Edition, 2003.*
2. *Robert C.Seacord, "Secure Coding in C and C++", Pearson Education, 2nd edition, 2013.*
3. *Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, "Software Security Engineering: A guide for Project Managers", Addison-Wesley Professional, 2008.*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18CE15	HIGH SPEED NETWORKS AND SECURITY	3	0	0	3

OBJECTIVES:

- To learn about the different internet routing protocols and different aspects routing in.
- To understand the issues in ATM networks and the protocols used for the working of ATM networks and how TCP play the role in Network Congestion.
- To understand the mathematical model for security and different aspects of encryption techniques and the role played by authentication in security

UNIT I INTRODUCTION 9 Hrs

Networking history – Need for speed and quality of services – Advanced TCP and ATM networks – Need for the protocol architecture – TCP/IP protocol architecture – OSI model – Internetworking – Transmission control protocol – User datagram protocol – Internet protocol – IPv6.

UNIT II ADVANCED NETWORKS 9 Hrs

Packet switching networks – Frame relay networks – ATM protocol architecture – ATM logical connections – ATM cell – ATM service categories – ATM adoption layer – The emergency of high speed LANs-Ethernet – Fiber channel – Wireless LANs.

UNIT III CONGESTION AND TRAFFIC MANAGEMENT 9 Hrs

Effect of congestion – Congestion and control – Traffic management – Congestion control in packet switching networks – Frame relay congestion control – Need for Flow and error control - Link control mechanisms – ARQ performance – TCP flow control – TCP congestion control – Performance of TCP over ATM – Requirement for ATM traffic and congestion control – ATM traffic Related attributes – Traffic management framework – Traffic control – ABR traffic management – GFR traffic management.

UNIT IV PUBLIC KEY ENCRYPTION 9 Hrs

Attacks - Services - Mechanisms - Conventional Encryption - Classical and Modern Techniques – Encryption Algorithms – Confidentiality - RSA - Elliptic Curve Cryptography - Number Theory Concepts

UNIT V MESSAGE AUTHENTICATION 9 Hrs

Hash Functions - Digest Functions - Digital Signatures - Authentication protocols.

Total Hours: 45

REFERENCES:

1. *William Stallings (2002), "High speed Networks and Internets", (2nd ed.), Pearson Education*
2. *Halsall, "Data Communications Computer Networks and Open Systems", Pearson Education, 4th Edition.*
3. *Wolf Gary Effelsberg, Otto Spaniol, Andre D. (1996), "High Speed Networking for Multimedia applications", Kluwer Academic publishers*
4. *Andrew S.Tanenbaum (1996), "Computer Networks", (3rd ed.), Prentice Hall*
5. *Stallings (1999), Cryptography & Network Security - Principles & Practice, Pearson Education*
6. *Bruce, Schneier (1996), Applied Cryptography (2nd ed.), Toha Wiley & Sons*

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18CE03	SECURE NETWORK DESIGN	3	0	0	3

OBJECTIVES:

- Understand security best practices and how to take advantage of the networking gear that is already available
- Learn design considerations for device hardening, Layer 2 and Layer 3 security issues, denial of service, IPSec VPNs, and network identity
- Understand security design considerations for common applications such as DNS, mail, and web.
- Identify the key security roles and placement issues for network security elements such as firewalls, intrusion detection systems, VPN gateways, content filtering, as well as for traditional network infrastructure devices such as routers and switches.
- Understand the various testing and optimizations strategies to select the technologies and devices for secure network design.

UNIT I NETWORK SECURITY FOUNDATIONS 9 Hrs

Secure network design through modeling and simulation, A fundamental framework for network security, need for user level security on demand, Network Security Axioms, security policies and operations life cycle, security networking threats, network security technologies, general and identity design considerations, network security platform options and best deployment practices, secure network management and network security management.

UNIT II IDENTIFYING SYSTEM DESIGNER'S NEEDS AND GOALS 9 Hrs

Evolution of network security and lessons learned from history, Analyzing top-down network design methodologies, technical goals and tradeoffs – scalability, reliability, availability, Network performance, security, Characterizing the existing internetwork, characterizing network traffic, developing network security strategies.

UNIT III PHYSICAL SECURITY ISSUES AND LAYER 2 SECURITY CONSIDERATIONS 9 Hrs

Control physical access to facilities, Control physical access to data centers, Separate identity mechanisms for insecure locations, Prevent password-recovery mechanisms in insecure locations, awareness about cable plant issues, electromagnetic radiation and physical PC security threats, L2 control protocols, MAC flooding considerations, attack mitigations, VLAN hopping attacks, ARP, DHCP, PVLAN security considerations, L2 best practice policies.

UNIT IV IP ADDRESSING AND ROUTING DESIGN CONSIDERATIONS 9 Hrs

Route summarizations, ingress and egress filtering, Non routable networks, ICMP traffic management, Routing protocol security, Routing protocol authentication, transport protocol management policies, Network DoS/flooding attacks.

UNIT V TESTING AND OPTIMIZING SYSTEM DESIGN 9 Hrs

Selecting technologies and devices for network design, testing network design – using industry tests, Building a prototype network system, writing and implementing test plan, tools for testing, optimizing Network design – network performance to meet quality of service (QoS), Modeling, simulation and Behavior analysis of security attacks, future issues in information system security. **Total Hours: 45**

REFERENCES:

1. Sumit Ghosh, "Principles of secure network system design", Springer-Verlag, NY, 2002. (UNIT I)
2. Sean Convery, "Network security architecture", Cisco Press, 2004.(UNIT III & IV)
3. Priscilla Oppenheimer, "Top-Down network Design", Third edition, Cisco press, 2012. (UNIT II & V).
4. Larry L. Peterson, Bruce S. Davie, "Computer Networks: A Systems Approach", Fourth Edition, Morgan Kauffmann Publishers Inc., 2009, Elsevier.
5. William Stallings, "Cryptography and Network security Principles and Practices", Pearson/PHI, 4th edition, 2006.
6. Wade Trappe, Lawrence C Washington, "Introduction to Cryptography with coding theory", 2nd edition, Pearson, 2007.

M.TECH INFORMATION SECURITY AND CYBER FORENSICS

Course Code	Course Title	L	T	P	C
MCS18CE17	RESEARCH METHODOLOGY	3	0	0	3

OBJECTIVES:

- To understand the need of research
- To explore the types of research design
- To understand the concepts of data collections for the research
- To understand the practical issues in reporting and thesis writing

UNIT I OBJECTIVES AND TYPES OF RESEARCH 9 Hrs

Definition, Motivation and objectives – Research methods vs. Methodology. Types of research – Descriptive vs. Analytical, Applied vs. Fundamental, Quantitative vs. Qualitative, Conceptual vs. Empirical.

UNIT II RESEARCH FORMULATION 9 Hrs

Defining and formulating the research problem -Selecting the problem - Necessity of defining the problem - Importance of literature review in defining a problem – Literature review – Primary and secondary sources – reviews, treatise, monographs-patents – web as a source – searching the web - Critical literature review – Identifying gap areas from literature review - Development of working hypothesis.

UNIT III RESEARCH DESIGN AND METHODS 9 Hrs

Research design – Basic Principles- Need of research design — Features of good design – Important concepts relating to research design – Observation and Facts, Laws and Theories, Prediction and explanation, Induction, Deduction, Development of Models. Developing a research plan - Exploration, Description, Diagnosis, and Experimentation. Determining experimental and sample designs.

UNIT IV DATA COLLECTION AND QUANTITATIVE METHODS FOR PROBLEM SOLVING 9 Hrs

Observation and Collection of data - Methods of data collection – Sampling Methods- Online Databases, Statistical Modeling, Analysis and Inference, Time Series Analysis, Probability Distributions, Multivariate methods, Concepts of Correlation and Regression, Spectral Analysis, Error Analysis, Hypothesis-testing - Generalization and Interpretation.

UNIT V REPORTING AND THESIS WRITING 9 Hrs

Structure and components of scientific reports - Types of report – Technical reports and thesis – Significance – Different steps in the preparation – Layout, structure and Language of typical reports – Illustrations and tables - Bibliography, referencing and footnotes - Oral presentation – Planning – Preparation – Practice – Making presentation , Reproduction of published material – Plagiarism - Citation and acknowledgement - Reproducibility and accountability.

Total Hours: 45

REFERENCES:

1. *Garg, B.L., Karadia, R., Agarwal, F. and Agarwal, U.K., 2002. An introduction to Research Methodology, RBSA Publishers.*
2. *Kothari, C.R., 1990. Research Methodology: Methods and Techniques. New Age International. 418p, 2nd Edition.*
3. *Sinha, S.C. and Dhiman, A.K., 2002. Research Methodology, Ess Ess Publications. 2 volumes.*
4. *Trochim, W.M.K., 2005. Research Methods: the concise knowledge base, Atomic Dog Publishing. 270p.*
5. *Ramez Elmasri, Shamkant B. Navathe, "Fundamentals of Database System" Addison Wesley, New Delhi/Fourth Edition 2004*
6. *M. Gertz, and S. Jajodia, Handbook of Database Security- Application and Trends, 2008, Springer.*