Course Name: M.Sc (Information and Cyber Security) PART TIME

Duration: 3 years (Part Time)

Eligibility: Bachelor degree in Engineering/Science from any University recognised by UGC.

Course Objective: The goal of this course is to cater to the requirements of higher learning in part-time mode of working professionals in areas like legal, civil, defense, IT and cyber security to advance their knowledge and skills to minimize the occurrence and severity of information security incidents. The part-time participants will learn on techniques used to detect, respond to, and prevent network intrusions. The duration of the course is three years and its syllabus is divided into six semesters that would provide in-depth understanding of core concepts with major thrust on functional competencies related to real life situations. The course bear a strong adherence to computer based technological skills and capabilities, and thereby resulting in efficiency to handle a variety of issues related to Information and Cyber Security.

Course Structure:

Summary:

Semester No	Total Credit
1	16
2	16
3	16
4	16
5	16
6	16
Total	96

Semester 1

Theory							
Sl No	Course Code	Topic	Contact hrs/wk				Credit
			L	T	P	Total	
1	MAM105	C Programming and Data Structure	3	1	-	4	4
2	MCS103	Information Systems & Software Engineering	3	1	-	4	4
3	MCLP101	Fundamentals of Information Security and Legal Framework	3	1	-	4	4
		Total of Theory				12	12
Practical							
4	MCLP191	Computer LAB (MATLAB, Excel, Linux Server- Apache)		-	4	4	4
		Total number of Practical				4	4
		Total				16	16

Semester 2

Theory							
Sl No	Course Code	Topic	Contact hrs/wk				Credit
			L	T	P	Total	
1	MCLP201	Introduction to Hardware, Network, the Internet	3	1	-	4	4
2	MCLP202	Cyber Threat and Modelling	3	1	-	4	4
3	MCLP203	Cyber Crimes & Investigation	3	1	-	4	4
4	MCLP204	Network Security(Ref: WBUT MCSE 401C)	3	1	-	4	4
		Total of Theory				16	16
		Total				16	16

Semester 3

1	MCLP301	Application and System Security	3	1	-	4	4
2	MCLP302	Operating System, Database and Infrastructure Security	3	1	-	4	4
3	MCLP303	Cyber Forensics	3	1	-	4	4
		Total of Theory				12	12
Practical							
4	MCLP 391	Cyber Forensics Lab		-	4	4	4
		Total number of Practical				4	4
		Total				16	16

Semester 4

Theory							
Sl No	Course Code	Topic	Contact hrs/wk				Credit
			L	T	P	Total	
1	MCLP401	Information Security & Cryptography	3	1	-	4	4
2	MCLP402	Mobile, Wireless and VoIP Security	3	1	-	4	4
3	MCLP403	Malware Analysis	3	1	-	4	4
		Total of Theory				12	12
Practical							
4	MCL491	Cryptography Lab		-	4	4	4
		Total of Practical				4	4
		Total				16	16

Semester 5

Theory							
Sl No	Course Code	Topic	Contact hrs/wk				Credit
			L	T	P	Total	
1	MCLP501	Cyber Law	3	1	-	4	4
2	MCLP502	Security Architecture and Models	3	1	-	4	4
3	MCLP503	Security Policy & Audit	3	1	-	4	4
4	MCLP504	Block Chain	3	1	-	4	4
		Total of Theory				16	16
		Total				16	16

Semester 6

1	MCLPE601 A/B/C	Elective I	3	1	-	4	4
2	MCLPE602 A/B/C	Elective II	3	1	-	4	4
		Total of Theory				8	8
Sessionals							
5	MCL481	Sessional Project			9	9	6
	MCL482	Grand Viva				3	2
		Total of Sessionals				12	8
		Total				20	16

Elective I

MCLPE601A/MCS E 401A Cloud Computing

MCLPE 601B Mobile & Digital Forensics

MCL E 601C Penetration Testing & Vulnerability Assessment

Elective II

MCLPE 602A Risk Management
MCLPE 602B Hardware Security
MCLPE 602C Biometric Security

Semester 1

MAM-105: C Programming and Data Structure

Introduction to Data Structure and Algorithm. Use of Big O and Small o Big Omega and small omega notations. Efficiency of algorithms. Analysis of recursive programs.Solving recurrence equation, divide and conquer algorithms.Dynamic programming,Greedy algorithms.
Implementation of Abstract Data Types(ADT),list,stack,queue hashing. Tree Structure,binary trees,AVL trees,Red-Black Trees,priority queues,Tree-Traversal Algorithms,Graphs and algorithms.Prim's and Kruskal's algorithms,Dijkstra's method,backtracking minimum spanning trees,Sorting and searching algorithms.
Introduction to NP problem, polynomial time,abstract problems,encoding; NP completeness and reducibility, circuit satisfiability, NP complete problem; Vertex cover,subset-sum,Hamiltonian-cycle,Travelling-Salesman Problem.

Text Books:

1.Data structure using c and c++ - Tanenbaum
2.Fundamentals of Data structure in c++ - E.Horwitz,Sahni,D.Mehta
3.Introduction to Algorithms – T.H.Cormen,C.E.Leiserson & R.L.Riveit
4.The Design and Analysis of Computer Algorithms- A.V.Aho, J.E.Hoperoft & J.D.Ullman

MCS103: Information Systems & Software Engineering

Introduction and IS in Global Business Today. Global E-Business: How Business Use Information System, IT Infrastructure and Emerging Technologies, Foundations of Business Intelligence, Telecommunications, the internet, and wireless Technology,Securing Information Systems, Enterprise Applications, Knowledge Management, Enhancing Decision Making information gathering, requirement and feasibility analysis, data flow diagrams,process specifications, input/output design, process life cycle, software planning and managing the project (single & multi variable model), design, software modularity & metrics, coding, testing, implementation, maintenance, software quality and reliability.

Text Books:

1. Management Information Systems: Managing the Digital Firm - 11th Edition by Kenneth C. Laudon Kenneth C. Laudon
2. Software Engineering: A Practitioner's Approach, 7/e by Roger S Pressman, R. S. Pressman & Associates, Inc.
3. An Integrated Approach to Software Engineering by P. jalote, Springer

MCLP101: Fundamentals of Information Security and Legal Framework

Module I: Introduction. [6L]

The History of Information Security, Balancing Information Security and Access, Introduction and Security Trends, General Security Concepts and introduction to what is an "infosphere", Operational Security and People's Role in Information Security.

Module II: Security Needs. [6L]

The Need for Security, Business Needs, Needs to protect against Threats and Attacks, Security in Emails.

Secure Software Development.

Module III: Cryptography Concepts. [8L]

Concepts of Data encryption, Introduction, Plaintext & Cipher text, Substitution Techniques, Transposition Techniques, Encryption & Decryption, Symmetric & Asymmetric key Cryptography.

Public Key Infrastructure (PKI), Different attacks on Cryptosystems.

Module IV: Internet Standards and Authentication. [8L]

Basic concepts of Internet Standards and Physical Security, Network Security and Infrastructure, Authentication Basics, Password, Authentication Token, Certificate based Authentication, Basics of authentication in Wireless Networks, Need of authentication in Wireless Communication.

Module V: Risk and Disaster Management. [6L]

An Overview of Risk Management and Disaster Planning, Risk Identification, Risk Assessment, Risk Control Strategies, Quantitative Versus Qualitative Risk Control Practices.

Module VI: Remote Access Protection. [6L]

Access Control, Biometric Access Controls, Firewalls, Protecting Remote Connections in Remote Access and Virtual Private Networks (VPNs), Intrusion Detection and Prevention Systems

Module VII: Legal Framework

Indian legal system, federalism and constitutionalism, Legislation, Enforcement of laws and Adjudication, Judicial system in India and hierarchy of courts, Criminal and Civil legal and justice system, Concept of Jurisdiction, Regulatory tribunals and their functions, Principles of administrative law, Alternative dispute resolution mechanism.

Text Books:

1) Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, New Delhi.

2) Micki Krause, Harold F. Tipton, " Handbook of Information Security Management", CRC Press LLC

3) Indian Legal System: S.P. Sharma, Mittal Publication

MCLP191:Computer LAB (MATLAB, Excel, Linux Server- Apache)

Assignment-1
Familiarization with MATLAB Control System tool Box, MATLAB- SIMULINK tool box & p SPICE
Assignment-2
Determination of step response for 1 order & 2 order system with amity feedback on CRO & calculation of control system specifications for variations of system design.
Assignment-3
Simulation of step response & impulse response for Type-I & Type-II system with unity feedback using
MATLAB.
Assignment-4
Determination of root locus, Bode-plot, SyQuest Plot, using MATLAB control system toolbox for a given
2^{nd} order transfer function & determination of different control system specifications.
Assignment-5
Electronic spreadsheet software, spreadsheet design, creating a spreadsheet, updating data & recalculations, Common spreadsheet commands.
Assignment-6
graphics capability, special features , different Formulas Related to database function, logical function, math & Accounting function.
Assignment-7
Linux Install, Network Interface configuration, Basic Linux Commands, Telnet.
Assignment-8
IP Subnet Calculation:-Public & Private IP Address, Classes of IP Address, IP sub netting.
Assignment-9
Packet Monitoring software (tcpdump, snort, ethereal).
Assignment-10
Linux File System Permission, Controlling new file permission & ownership , Trace route, Ping, Finger, Nmap .

Semester 2

MCLP201: Introduction to Hardware, Network, the Internet

Module I: (6L)
Definition of computer system, Block Diagram, Components of a computer system, generations of computers, storage devices, Memory Hierarchy, Software, Classification of software, Operating System and its functionalities
Module II: (6L)
Introduction to networking; Data communications: components, data representation (ASCII,ISO etc.), direction of data flow (simplex, half duplex, full duplex); network criteria, physical structure (type of connection, topology), categories of network (LAN, MAN,WAN);
Internet: brief history, Protocols and standards; Reference models: OSI reference model, TCP/IP reference model, their comparative study.

Overview of data(analog & digital), signal(analog & digital), transmission (analog & digital) & transmission media (guided & unguided);

Module III: (8L)

Local Area Networks and data link protocols, point-to-point links and sliding window flow control, CSMA/CD, Ethernet, wireless LAN, cellular networks, and advanced multi-user communication (CDMA, SDMA/MIMO), mobility

Internetworking using TCP/IP: network programming using socket API, network client/server design

Packet/circuit switching and wide-area networks: store-and-forward networks, source routing, virtual/permanent, circuits and call set-up, LAN/WAN addressing, hop-by-hop vs. end-to-end control

Module IV: (10L)

Routing techniques - intra-domain routing (OSPF, RIP), inter-domain policy routing (BGP) and network connectivity

Transport protocols - TCP and UDP, Congestion control, TCP window control, multimedia streaming

High-level network services - DNS, HTTP, SMTP, network management (SNMP), network security

Module V: (10L)

Introduction and history of Internet, WWW, Markup Language: HTML, XML and tags, Scripting Languages, Client-Server Architecture, websites, Internet security and threats, Firewall, Introduction to e-commerce

Text Books:

1. Fundamental of Computers, V.Rajaraman, Prentice Hall India
2. Computer Networks by AS Tanenbaum, Fourth Edition, 2002, Pearson Education
3. Data Communication and Networking by B. Forouzan
4. Data and Communication by W. Stallings
5. Web Technologies: AchyutGodbole, AtulKahate - McGraw Hill

MCLP 202: Cyber Threat and Modelling

Understanding Intelligence: Intelligence Lexicon and Definitions, Traditional Intelligence Cycle, Sherman Kent and Intelligence Tradecraft, Structured Analytical Techniques

Understanding Cyber Threat Intelligence: Defining Threats, Understanding Risk, Cyber Threat Intelligence and Its Role, Expectation of Organizations and Analysts, Four Methods of Threat Detection

Threat Intelligence Consumption: Sliding Scale of Cybersecurity, Consuming Intelligence for Different Goals, Enabling Other Teams with Intelligence

Positioning the Team to Generate Intelligence: Building an Intelligence Team, Positioning the Team in the Organization, Prerequisites for Intelligence Generation

Planning and Direction (Developing Requirements): Intelligence Requirements, Priority Intelligence Requirements, Beginning the Intelligence Lifecycle, Threat Modeling

Case-Study: Carbanak, "The Great Bank Robbery"

MCLP203: Cyber Crimes and Investigation

Introduction to cyber crime, Data diddling, Data leakage, Eavesdropping, E-mail forgery, E-mail threats,Internet misinformation, Internet terrorism, Password cracking, Round downs, Salami Techniques, Scavenging/Corporate Espionage, Social Engineering, Software Piracy, Spamming, Super zapping, Piggybacking, Trap door, Trojan Horse, Virus, Worm Impersonation, Time bomb, Logic bomb, DOS Attack
Email Hacking& its security ,Social Media Hacking& its Security, Web Hacking& its Security, Mobile Hacking& its Security, Wi-Fi Network Hacking& its Security, Software Hacking, Reverse Engineering Cross site scripting & its Security, Email forgery and E-mail Tracing.

Intrusion Analysis, Intrusion Analysis as a Core Skillset, Methods to Performing Intrusion Analysis, Intrusion Kill Chain, Passively Discovering Activity in Historical Data and Logs, Detecting Future Threat Actions and Capabilities, Denying Access to Threats, Delaying and Degrading Adversary Tactics and Malware, Identifying Intrusion Patterns and Key Indicators

Text Books:

1) Cyber Law Law Of Information Technology And Internet (Lexix Nexis) Anirudh Rastogi
2) Understanding Laws– Cyber Laws And Cyber Crimes (Lexix Nexis)
3) Cyber Crime Manual by Bibhas Chatterjee, Lawman Publication

MCLP204 (Ref: WBUT MCSE 401C): Network Security

Concepts and Terminology:
Threats, Attacks, Services and Mechanisms, Security Attacks, Security Services, Integrity check, digital Signature, authentication, Spoofing, Sniffing, Firewall.
Cryptography:
Techniques, Mathematical foundation, Stream Ciphers, Block Ciphers, Cryptanalysis, Hash Algorithms.
Secret Key Cryptography:
Block Encryption, DES rounds, S-Boxes IDEA: Overview, comparison with DES, Key expansion, IDEA rounds, Uses of Secret key Cryptography; ECB, CBC, OFB, CFB, Multiple encryptions DES.
Hash Functions and Message Digests:

Length of hash, uses, algorithms (MD2, MD4, MD5, SHS) MD2: Algorithm (Padding, checksum, passes.) MD4 and 5: algorithm (padding, stages, digest computation.) SHS: Overview, padding, stages.

Public key Cryptography:

Algorithms, examples, Modular arithmetic (addition, multiplication, inverse, and exponentiation) RSA: generating keys, encryption and decryption. Other Algorithms: PKCS, Diffie-Hellman, El-Gamal signatures, DSS, Zero-knowledge signatures.

Authentication:

Password Based, Address Based, Cryptographic Authentication. Passwords in distributed systems, on-line vs offline guessing, storing. Cryptographic Authentication: passwords as keys, protocols, KDC's Certification Revocation, Inter-domain, groups, delegation. Authentication of People: Verification techniques, passwords, length of passwords, password distribution, smart cards, biometrics.

Security Policies and Security Handshake Pitfalls:

What is security policy, high and low level policy, user issues? Protocol problems, assumptions, Shared secret protocols, public key protocols, mutual authentication, reflection attacks, use of timestamps, nonce and sequence numbers, session keys, one-and two-way public key based authentication.

Network Security:

Electronic mail security, IP security, Network management security.
Security for electronic commerce: E-commerce security analysis, protocol, SSL, SET

System Security:

Intruders and Viruses, Firewalls, Intrusion Detection.

Case Studies

Web threats, E-mail threats, Domain controller threats, Extranet and VPN threats.
Assignment and Project work.

Text Books:

1. Atul Kahate, Cryptography and Network Security, McGraw Hill
2. Kaufman, c., Perlman, R., and Speciner, M., Network Security, Private Communication in a public world, 2nd ed., Prentice Hall PTR., 2002
3. Stallings, W.,.Cryptography and Network Security: Principles and Practice, 3rd ed., Prentice Hall PTR.,2003
4. Stallings, W. Network security Essentials: Applications and standards, Prentice Hall, 2000
5. Cryptography and Network Security; McGraw Hill; Behrouz A Forouzan
6. Information Security Intelligence Cryptographic Principles andApp. Calabrese Thomson
7. D. P. Nagpal, Information Security, S. Chand Complany Limited
8. 7. Securing A Wireless Network Chris Hurley SPD.

Semester 3

MCLP301: Application and System Security

Module I: Introduction. [8L]

Protocols and standards, Hypertext Transfer Protocol (HTTP), Markup languages Hypertext Markup Language (HTML), Cascading Style Sheets (CSS).

Module II: Web Application. [14L]

Extensible Hypertext Markup Language (XHTML), CGI scripts and clickable maps,
JAVA applets, JAVA servlets, Perl. DHTML, XML, Client-side technologies, JavaScript, Server-side technologies , SQL , PHP.

Module III: Software and System Security. [5L]

Control hijacking attacks – buffer overflow, integer overflow, bypassing browser memory protection, Sandboxing and Isolation, Tools and techniques for writing robust application software, Security vulnerability detection tools, and techniques – program analysis, Privilege, access control, and Operating System Security, Exploitation techniques, and Fuzzing.

Module IV: Network Security & Web Security. [8L]

Security Issues in TCP/IP – TCP, DNS, Routing (Topics such as basic problems of security in TCP/IP, IPsec, BGP Security, DNS Cache poisoning etc), Network Defense tools – Firewalls, Intrusion Detection, Filtering, DNSSec, NSec3, Distributed Firewalls, Security architecture of World Wide Web, Security Architecture of Web Servers, and Web Clients, Web Application Security – Cross Site Scripting Attacks, Cross Site Request Forgery, Https, Threat Modeling, Attack Surfaces.

Module V: Security in Mobile Platforms. [3L]

Android security model, threat models, information tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection

Module VI: Introduction to Hardware Security, Supply Chain Security. [2L]

Threats of Hardware Trojans and Supply Chain Security, Side Channel Analysis based Threats, and attacks.

Text Books:

1. Principles of Computer Security: W.A.Coklin, G.White, Fourth Edition, McGrawHill
2. Cryptography and Network Security Principles and Practices,*William Stallings,Seventh Edition,Pearson*
3. Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing
   Achyut S. Godbole,Tata McGraw-Hill Education, 2013

MCLP302: Operating System, Database and Infrastructure Security

Module I: Operating System. [18L]

Introduction to OS-Operating system functions, evaluation of O.S., Different types of O.S.: batch, multi-programmed, time-sharing, real-time, distributed, parallel. Computer system operation, I/O structure, storage structure, storage hierarchy, different types of protections, operating system structure (simple, layered, virtual machine), O/S services, system calls.

Process Management : Concept of processes, process scheduling, operations on processes, co-operating processes, inter-process communication. Process Synchronization,Deadlocks.

Memory Management: background, logical vs. physical address space, swapping, contiguous memory allocation, paging, segmentation, segmentation with paging. Virtual Memory : background, demand paging, performance, page replacement, page replacement algorithms (FCFS, LRU), allocation of frames, thrashing.

File Systems : file concept, access methods, directory structure, file system structure, allocation methods (contiguous, linked, indexed), free-space management (bit vector, linked list, grouping), directory implementation (linear list, hash table), efficiency & performance.

I/O Management : I/O hardware, polling, interrupts, DMA, application I/O interface (block and character devices, network devices, clocks and timers, blocking and nonblocking I/O), kernel I/O subsystem (scheduling, buffering, caching, spooling and device reservation, error handling), performance, Disk Management.

Protection & Security:Goals of protection, domain of protection, security problem, authentication, one time password, program threats, system threats, threat monitoring, encryption.

Module II: Database. [16L]

Introduction Concept & Overview of DBMS, Data Models, Database Languages, Database Administrator, Database Users, Three Schema architecture of DBMS.

Entity-Relationship Model. Relational Model, Relational Algebra, Relational Calculus, Extended Relational Algebra Operations, Views, Modifications Of the Database.

SQL and Integrity Constraints.

Relational Database Design :Functional Dependency, Different anamolies in designing a Database., Normalization using funtional dependencies, Decomposition, Boyce-Codd Normal Form, 3NF, Nomalization using multi-valued depedencies, 4NF, 5NF.

Transaction processing, Concurrency control and Recovery Management : transaction model properties, state serializability, lock base protocols, two phase locking.

File Organization & Index Structures.

Module III :Infrastructure Security. [6L]

IT Infrastructure Management Services, Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement

Data Centre Management: Introduction to DCM, Data Center design, Data Center Security Procedure, Server Security, Storage area network, Virtualization, Introduction of Virtual Private Cloud (VPC), Private Cloud Setup, Automation Using Cloud API Server Orchestration, Cloud Logging and monitoring .

Text Books:

1. Silbersehatz A. and Peterson J. L., "Operating System Concepts", Wiley
2. Henry F. Korth and Silberschatz Abraham, "Database System Concepts", Mc.Graw Hill.
3. Elmasri Ramez and Novathe Shamkant, "Fundamentals of Database Systems", Benjamin Cummings Publishing. Company.
4. Principles of Computer Security: W.A.Coklin, G.White, Fourth Edition, McGrawHill

MCLP303: Cyber Forensics

Digital Forensics Fundamentals: Introduction to Incident response,digital forensics four-step procedure,Concepts: computer/network/Internet forensic and anti-forensics.

Unix/Linux fundamentals: Unix/Linux incident response tools, Unix/Linux file systems (Ext2/Ext3)

Unix/Linux Forensic Investigation: Unix/Linux forensics investigation steps and technologies, Unix/Linux forensics case studies

Windows Incident Response: Memory forensics, Windows incident response tools

Windows fundamentals: Windows file systems, Windows forensics tools

Windows Forensic Investigation: Windows acquisition, Windows forensics analysis – registry and other artifacts

Advanced artifacts: Loadable kernel module rootkits, Steganography hiding, detection and analysis

Text Books:

1. Man Young Rhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", Wiley Publications, 2003.
2. 2. Nelson, Phillips, Enfinger, Steuart, "Computer Forensics and Investigations", Cengage Learning, India Edition, 2008.

MCLP391:Cyber Forensics Lab

Software Tools: CyberCheck 4.0 - Academic Version CyberCheckSuite MobileCheck Network Session Analyser Win-LiFT TrueImager TrueTraveller PhotoExaminer Ver 1.1, CDRAnalyzer

Disk Forensics: 1. Identify digital evidences 2. Acquire the evidence 3. Authenticate the evidence 4. Preserve the evidence 5. Analyze the evidence 6. Report the findings

Network Forensics: • Intrusion detection • Logging (the best way to track down a hacker is to keep vast records of activity on a network with the help of an intrusion detection system) • Correlating intrusion detection and logging

Device Forensics 1. PDA 2. Mobile phone 3. Digital Music 4. Printer Forensics 5. Scanner

Semester 4

MCLP401: Information Security & Cryptography

Information Security: Introduction, History of Information security, What is Security, CNSS Security Model, Components of Information System, Balancing Information Security and Access, Approaches to Information Security Implementation, The Security Systems Development Life Cycle.

Cryptography: Concepts and Techniques, symmetric and asymmetric key cryptography, steganography, Symmetric key Ciphers: DES structure, DES Analysis, Security of DES, variants of DES, Block cipher modes of operation , AES structure, Analysis of AES , Key distribution Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Analysis of RSA, Diffie-Hellman Key exchange

Message Authentication and Hash Functions: Authentication requirements and functions, MAC and Hash Funtions, MAC Algorithms: Secure Hash Algorithm, Whirlpool, HMAC, Digital signatures, X.509, Kerberos UNIT – IV Security at layers(Network, Transport, Application): IPSec, Secure Socket Layer(SSL), Transport Layer Security(TLS), Secure Electronic Transaction(SET), Pretty Good Privacy(PGP), S/MIME

Inruders, Virus and Firewalls: Intruders, Intrusion detection, password management, Virus and related threats, Countermeasures, Firewall design principles, Types of firewalls

Introduction to Cryptoanalysis: Linear Cryptanalysis, Differential Cryptanalysis, Cryptanalysis of DLP

Text Books: 1. Principles of Information Security : Michael E. Whitman, Herbert J. Mattord, CENGAGE Learning, 4th Edition. 2. Cryptography and Network Security : William Stallings, Pearson Education,4th Edition 3. Cryptography and Network Security : Forouzan Mukhopadhyay, Mc Graw Hill, 2nd Edition

MCLP402: Mobile, Wireless and VoIP Security

Module I: Introduction. **[6L]**
Security Features in Wireless Environment, Mobile Network Environment, Limitations of Mobile Environment, Mobility and Security, Attacks in Mobile Environment, Security Issues in Mobile Environment.

Module II: Mobile Networks. **[6L]**
Bluetooth Overview, Architecture and Components, Security of Bluetooth, Overview of GSM, Architecture of the GSM Network, GSM Security Features, Attacks on GSM Security.

Module III: Wireless Systems. **[8L]**
3G Wireless Communications Systems - 3GPP, 4G Wireless Communications Systems, Wireless Application Protocol (WAP), Protocol Stack and security related issues.

Module IV: Security in Wireless Communication. **[8L]**
802.11 Architecture, Wireless LAN Components, Security of 802.11 Wireless LANs, Security Features of 802.11 Wireless LANs per the Standard, Problems With the IEEE 802.11 Standard Security, Security Requirements and Threats, Emerging Security Standards and Technologies, IPSec, SSL.

Module V: VoIP. **[5L]**
Streaming in 3rd generation mobile architecture, Voice and Video over IP (Media over IP), Session Initiation Protocol (SIP) and its use in Media Over IP, Skype as a case study.

Module VI: Security in VoIP. **[6L]**
Attacks against the VOIP network, Challenges against implementing VOIP network, WEP (Wired Equivalent Privacy), Effects of using WEP in VOIP networks, Concepts of WPA and WPA2.

Text Books:

1) William Stallings, "Cryptography and Network Security", 3rd Edition, Pearson Education, New Delhi, 2003.
2) B.A. Forouzan, "Cryptography & Network Security", TaTa McGrawHill, 2007.
3) Tom Karygiannis, Les Owens,"Wireless Network Security 802.11, Bluetooth and Handheld Devices", National Institute of Standards and Technology, US Dept. of Commerce Special Publication 800-48, 2002

MCLP403: Malware Analysis

Introduction: Computer Infection Program- Life cycle of malware- Virus nomenclature- Worm nomenclature- Tools used in computer virology.

Implementationof Covert Channel Non self-reproducing Malware- Working principle of Trojan Horse- Implementation of Remote access and file transfer- Working principle of Logical Bomb- Case Study: Conflicker C worm.

Virus Design And Its Implications :Virus components- Function of replicator, concealer and dispatcher- Trigger Mechanisms- Testing virus codes- Case Study: Brute force logical bomb.

Malware Design Using Open Source :Computer Virus in Interpreted programming language- Designing Shell bash virus under Linux- Fighting over infection- Anti –antiviral fighting – Polymorphism- Case study: Companion virus.

Virus And Worm Analysys Klez Virus- Clone Virus- Doom Virus- Black wolf worm- Sassar worm- Happy worm 99.

TEXT BOOKS:

1. ErciFiliol, "Computer Viruses: from theory to applications", Springer, 1st edition, 2005

2. Mark.A .Ludwig, "The Giant black book of computer viruses,CreateSpace Independent Publishing Platform, 2 nd edition, 2009,ISBN 10: 144140712X

MCLP491: Cryptography Lab

1) Perform Basic Encryption/Decryption(Text only)..
2) Diffie-Hellman key exchange and symmetric key cryptography.
3) Public key cryptography using RSA.
4) Implementing Private key cryptography.
5) Perform Basic Encryption/Decryption
6) Perform Basic Hash Functions(Like MD4,MD5 etc.).
7) Perform Basic Fractal functions(Like Julia set etc.)
8)Generate Asymmetric Key Pair.
9) Generate Web Certificate from Key Pair.
10) Run Secure Web Server Using Web Certificate.
11) An Application On Watermarking Technique.

Semester 5

MCLP501 : Cyber Law

Module I: Introduction Computers and its Impact in Society• Overview of Computer and Web Technology• Need for Cyber Law• Cyber Jurisprudence at International and Indian Level•

Module II: Cyber Law - International Perspectives UN• & International Telecommunication Union (ITU) Initiatives Council of Europe - Budapest Convention on Cybercrime• Asia-Pacific Economic Cooperation (APEC)• Organization for Economic Co-operation and Development (OECD)• World Bank• Commonwealth of Nations

Module III: Constitutional & Human Rights Issues in Cyberspace Freedom of Speech and Expression in Cyberspace• Right to Access Cyberspace – Access to Internet• Right to Privacy• Right to Data Protection

Module IV: Cyber Crimes & Legal Framework Cyber Crimes against Individuals, Institution and State• Hacking• Digital Forgery• Cyber Stalking/Harassment• Cyber Pornography• Identity Theft• & Fraud Cyber terrorism• Cyber Defamation• Different offences under IT Act, 2000

Module V: Cyber Torts Cyber Defamation• Different Types of Civil Wrongs under the IT Act, 2000, Electronic Evidence.

Module VI: Intellectual Property Issues in Cyber Space Interface with Copyright Law• Interface with Patent Law• Trademarks• & Domain Names Related issues

Module VII:Indian Context of Jurisdiction and IT Act, 2000. ,International Law and Jurisdictional Issues in Cyberspace.

Text Books:

1. Chris Reed• & John Angel, Computer Law, OUP, New York, (2007).
2. Justice Yatindra Singh, Cyber Laws, Universal Law Publishing Co, New Delhi, (2012
3. Sudhir Naib, The Information Technology Act, 2005: A Handbook, OUP, New York,• (2011)
4. S. R. Bhansali, Information Technology Act, 2000, University Book House Pvt. Ltd

MCLP502: Security Architecture and Models

Module I: Security Architecture And Information. [7L]

Introduction ,History, Information Security, Critical Characteristics of Information, Components of an Information System, Securing the Components, Balancing Security and Access, Need for security, Business needs,Threats,Attacks,Legal,Ethical and Professional Issues.

Module II: Logical design and physical design. [7L]

Blueprint for security, Information Security policy,NIST Models, VISA International security model, Design of Security Architecture, Planning for continuity,Security Technology,IDS, Crytography,Access Control Devices,Physical Security,Security and Personnel.

Module III: Low-level architecture. [6L]

Security Assessments,Security Architecture Basics,Architecture Patterns in Security,Cryptography,Trusted Code,Secure Communications.

Module IV: Mid-level architecture. [6L]

Middleware Security,Web Security,Application and OS Security,Database Security.

Module V: High-level architecture. [6L]

Security Components, Security and Other Architectural Goals,Enterprise Security Architecture.

Module VI: Business cases and security. [2L]

Business Cases for Security.

MCLP503: Security Policy and Audit

Module I: Introduction. [6L]

Basics of Audit, IT Auditing: What Is It? The Situation and the Problem, Audit Standards, Importance of Audit Independence, Need for IT Audit Function, Auditor: Knowledge, Skills, and Abilities, Role of the IT Auditor, Types of Auditors and Their Duties, Functions, and Responsibilities

Module II: Audit Process in an Information Technology Environment. [7L]

Audit Universe, Risk Assessment, Audit Plan, Developing an Audit Schedule, Audit Budget, Objective and Context, Using the Plan to Identify Problems, Audit Process, Design Audit Procedures, Fieldwork and Implementing Audit Methodology.

Module III: IT Auditing in Modern Era. [7L]

IT Auditing Trends, New Dimension: Information Assurance, IT Audit: The Profession, A Common Body of Knowledge, Certification, Role of the IT Auditor in IT Governance, IT Auditor as Counselor, IT Auditor as Partner of Senior Management.

Module IV: Audit using Computer Assisted Audit Tools. [9L]

Auditor Productivity Tools, Using Computer-Assisted Audit Tools in the Audit Process, Flowcharting Techniques, Flowcharting as an Analysis Tool, Appropriateness of Flowcharting Techniques, Computer-Assisted Audit Tools and Techniques for Application Reviews, Computer-Assisted Audit Tools and Techniques for Operational Reviews, Web Analysis Tools, Web Analysis Software as an, Audit Tool, Computer Forensics.

Module V: Managing IT Audit. [6L]

Evaluating IT Audit, IT Audit Quality, Terms of Assessment, IT Audit and Auditor Assessment Form, Criteria for Assessing the Audit, Criteria for Assessing the Auditor, Applying the Concept, Evaluation of IT Audit Performance.

Module VI: Security Audit Process. [5L]

Pre-planning audit, Audit Risk Assessment, Performing Audit, Internal Controls, Audit Evidence, Audit Testing, Audit Finding, Follow-up activities.

Text Books:

1. Sandra Senft, Frederick Gallegos and Aleksandra Davis, "Information Technology Control and Audit, Fourth Edition", CRC Press.

2. David L. Cannon, “CISA Certified Information Systems Auditor Study Guide”, John Wiley & Sons.

MCLP504 Block Chain & Cryptocurrency

Intro to Blockchain and Cryptocurrency

Internet of money, Public vs. private blockchain technology, Proof of work, consensus verification, Data blocks, Bitcoin and valuation, Ethereum and Blockchain Platforms Clearing and , Introduction to Blockchain API

Open source tools, Algorithms,,Assets and Tokenization and the Value of the Blockchain Credits versus tokens Community currency

Smart Contracts Distributed ledger technology,Regulation and legal frameworks,Consensus Protocols and Byzantine Fault Tolerance (BFT), Scalability and distributed ledgers, ethereum, Regulatory Environment

Use Cases Finance,Security, Social Good, Other alternative uses,

Security: Attacks and Trustless Networks

6th Semester:

MCSE401A/MCLPE601A: Cloud Computing

Introduction: Cloud computing definition, reference model, Characteristics, Benefits,
Challenges, Distributed Systems, Virtualization, Service-oriented computing, Utility-oriented computing, Overview on computing platforms & technologies – AWS,Google AppEngine, MS Azure, Hadoop, Saleforce.com, Manjrasoft Aneka
Parallel & Distributed Computing: Parallel vs. Distributed computing, Elements of parallel computing, Parallel processing - hardware architecture & approaches, Concept & Component of Distributed Computing, RPC, Service-oriented computing Virtualization: Cloud reference model – IaaS, PaaS, SaaS, Types of clouds – Public,Private, Hybrid, Community, Cloud interoperability & standards, scalability & fault tolerance, Security, trust & privacy
Concurrent Computing, High-throughput Computing and Data-Intensive Computing:Programming applications with Threads, Thread API, Parallel computation with Threads,Task computing, Frameworks for Task computing, Task-based application model,
Data-intensive computing, characteristics, technology Cloud Platforms and Applications: Overview on Amazon Web Services, Google AppEngine and Microsoft Azure, Cloud applications in scientific, business and consumer Domain

Text Books:

1. Buyya, Vecciola and Selvi, Mastering Cloud Computing: Foundations and Applications Programming, Tata McGraw Hill
2. Rittinghouse and Ransome, Cloud Computing: Implementation, Management,

and Security, CRC Press
3. Aravind Doss, Cloud Computing, Tata McGraw Hill
4. Kris Jamsa, Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More, Jones & Bartlett Learning

MCLPE601B Mobile & Digital Forensics

Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft.

CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues

Mobile phone forensics: crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques

Digital forensics: Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contaminationUnit V (8 hours) Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locationsSeven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context

Text Books:

1. Gregory Kipper, “Wireless Crime and Forensic Investigation”, Auerbach Publications, 2007
2. Iosif I. Androulidakis, “ Mobile phone security and forensics: A practical approach”, Springer publications, 2012
3. Andrew Hoog, “ Android Forensics: Investigation, Analysis and Mobile Security for Google Android”, Elsevier publications, 2011
4. Angus M.Marshall, “ Digital forensics: Digital evidence in criminal investigation”, John – Wiley and Sons, 2008

MCLPE601C Penetration Testing & Vulnerability Assessment

Introduction Ethical Hacking terminology- Five stages of hacking- Vulnerability Research- Legal implication of hackingImpact of hacking.

Foot printing & Social engineering Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks.

Scanning & Enumeration Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS FingerprintingEnumeration.

System Hacking Password cracking techniques- Key loggers- Escalating privileges- Hiding Files- Steganography technologies- Countermeasures.

Sniffers & SQL Injection Active and passive sniffing- ARP Poisoning- Session Hijacking- DNS Spoofing- Conduct SQL Injection attack - Countermeasures.

TEXT BOOKS:

1. Kimberly Graves, "CEH: Official Certified Ethical Hacker Review Guide", Wiley Publishing Inc., 2007. ISBN: 978-0-7821-4437-6.
2. Shakeel Ali &TediHeriyanto, "Backtrack -4: Assuring security by penetration testing", PACKT Publishing., 2011. ISBN: 978-1-849513-94-4.

MCLPE602A Risk Management

Module I: Introduction to Information Risk Management. [9L]
Introduction to Risk Management, The Business Risk Model, Information and Technology Risk Management, Identifying IT Risks and Controls, Risk Information Processes, Assessing and Mitigating Risk at the Process Level, Managing Project Risk.

Module II: Introduction to Risk Assessments and Risk Semantics. [7L]
Assessing Information Risks and Controls, A Framework for Assessing IT Risks, The Role of IT Audit and Risk Assessments, IT Governance, Non-Technical Security Risks, The Risks Caused by People – Social Engineering & Behavioral Security.

Module III: Risk Issues in IT and Telecommunication. [9L]
The Risks of Connectivity, Risks Surrounding IT and Telecommunication Networks, Organizational Network and Application Security, Internet & Host Security, Firewalls & VPNs, IT Fraud in Organizations, Cyber Crime and Terrorism, Digital and Computer Forensics.

Module IV: Security Management. [6L]
Information Security Management, Corporate Security Policy, The Ongoing Management of Information Security, Measuring Security, Incident Response.

Module V: Incident Analysis. [4L]

Introduction, Log analysis, Event criticality, General log configuration and maintenance, Live Incident Response, Timelines, Other forensics topics

Text Books:

1. Manish Agrawal, Alex Campoe and Eric Pierce, "Information Security and IT Risk Management", Wiley.
2. Michael E. Whitman, "Principles of Information Security", Cengage Learning.

MCLPE 602B Hardware Security

Overview of Different Issues of Hardware Security

Preliminaries: Algebra of Finite Fields, Basics of the Mathematical Theory of Public Key Cryptography, Basics of Digital Design on Field-programmable Gate Array (FPGA), Classification using Support Vector Machines (SVMs)

Useful Hardware Security Primitives: Cryptographic Hardware and their Implementation, Optimization of Cryptographic Hardware on FPGA, Physically Unclonable Functions (PUFs), PUF Implementations, PUF Quality Evaluation, Design Techniques to Increase PUF Response Quality

Side-channel Attacks on Cryptographic Hardware: Basic Idea, Current-measurement based Side-channel Attacks (Case Study: Kocher's Attack on DES), Design Techniques to Prevent Side-channel Attacks, Improved Side-channel Attack Algorithms (Template Attack, etc.), Cache Attacks

Testability and Verification of Cryptographic Hardware: Fault-tolerance of Cryptographic Hardware, Fault Attacks, Verification of Finite-field Arithmetic Circuits

Modern IC Design and Manufacturing Practices and Their Implications: Hardware Intellectual Property (IP) Piracy and IC Piracy, Design Techniques to Prevent IP and IC Piracy, Using PUFs to prevent Hardware Piracy, Model Building Attacks on PUFs (Case Study: SVM Modeling of Arbiter PUFs, Genetic Programming based Modeling of Ring Oscillator PUF)

Hardware Trojans: Hardware Trojan Nomenclature and Operating Modes, Countermeasures Such as Design and Manufacturing Techniques to Prevent/Detect Hardware Trojans, Logic Testing and Side-channel Analysis based Techniques for Trojan Detection, Techniques to Increase Testing Sensitivity Infrastructure Security: Impact of Hardware Security Compromise on Public Infrastructure, Defense Techniques (Case Study: Smart-Grid Security)

Text Books:

Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press

MCLPE 602C BIOMETRIC SECURITY

Introduction to Biometrics, Fingerprint Recognition, Face Recognition, Iris Recognition, Hand Geometry Recognition

Gait Recognition, The Ear as a Biometric, Voice Biometrics, A Palm print Authentication System, and OnLine Signature Verification

3D Face Recognition, Automatic Forensic Dental Identification, Hand Vascular Pattern Technology, Introduction to Multi biometrics, Multispectral Face Recognition

Multi biometrics Using Face and Ear, Incorporating Ancillary Information in Multi biometric Systems, The Law and the Use of Biometrics, Biometric System Security, Spoof Detection Schemes

Linkages between Biometrics and Forensic Science, Biometrics in the Government Sector, Biometrics in the Commercial Sector, Biometrics Standards, Biometrics databases

Text Books:

1. Jain, Anil K.; Flynn, Patrick; Ross, Arun A. (Eds.), Handbook of Biometrics, Springer, 2008.
2. Benjamin Muller, Security, Risk and the Biometric State: Governing Borders and Bodies, 1st Edition, Routledge, 2010.