JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY

M. TECH (CYBER FORNENSICS & INFORMATION SECURITY)

I YEAR I SEMESTER

Code	Group	Subject	L	P	Credits
		IPR and Cyber laws	3	0	3
		Information Security and Cryptography	3	0	3
		Ethical Hacking	3	0	3
		Forensics And Incident Response	3	0	3
	Elective –I	Distributed Systems Advanced Problem Solving Network Programming	3	0	3
	Elective -II	Operating Systems Administration and Security Biometric Security Database Security	3	0	3
	Lab	Ethical Hacking & Network Security Lab	0	3	2
		Seminar	-	-	2
		Total Credits (6 Theory + 1 Lab.)			22

I YEAR II SEMESTER

Code	Group	Subject	L	P	Credits
		Advanced Computer Networks	3	0	3
		Mobile and Digital Forensics	3	0	3
		Cyber Forensics	3	0	3
		Information Security Management and Standards	3	0	3
	Elective –III	Storage Area Networks Malware Analysis Penetration Testing and Vulnerability Assessment	3	0	3
	Elective -IV	Cloud Architectures and Security Wireless Networks and Mobile Computing Applications of Network Security	3	0	3
	Lab	Cyber Forensics Lab	0	3	2
		Seminar	-	-	2
		Total Credits (6 Theory + 1 Lab.)			22

II YEAR I SEMESTER

Code	Group	Subject	L	P	Credits
		Comprehensive Viva	-	-	2
		Project Seminar	0	3	2
		Project Work	-	-	18
		Total	-	3	22

II YEAR II SEMESTER

Code	Group	Subject	L	P	Credits
		Project Work and Seminar	-	-	22
		Total	-	-	22

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

INTELLECTUAL PROPERTY RIGHTS AND CYBER LAWS

UNIT-I:

Introduction to Intellectual Property. 12w of Trademarks, Trademark Selection & Searching

IP Law-Types of IP - Agencies for IF Registration - International Treaties. Purpose and Function of Trademarks - Types of marks - Acquisition of Trademark Rights - Categories of marks - Trade names and Business names -proteetable matter. Selection and Evaluation of a mark - Trademark search.

Trademark Registration Process, Post-registration Procedures. Trademark Maintenance, Transfer of Rights to Marks: Preparing and Filing the Application - Docketing Critical Dates - Examination Process - Post- examination Procedure -Registration. Affidavit of Continued Use -Affidavit of Incontestability - Renewal of Registrations - Docketing Requirements - Loss of Trademark Rights -- Trademark Use and Compliance Policies - Trademark Policing and Maintenance - Use of Marks Owned by Third Parties - Transfer of Ownership or Rights in Trademarks.

UNTT-II:

Inter Panes Proceedings, Infringement, Dilution, New Developments in Trademark Law

Inter Partes Proceedings - Infringement of Trademarks - Dilution of Trademarks- Related Trademark Claims. Protecting a Domain Name Other Cyberspace Trademark issues.

Law of Copyright. Subject Matter Of Copyright. Rights Afforded by Copyright Law

Foundations of Copyright Law- Originality of Material - Fixation of Material - Exclusions from Copyright Protection - Compilations, Collections, and Derivative Works. Rights of Reproduction - Rights to Prepare Derivative works - Rights of Distribution - Rights to Perform the Work Publicly - Rights to Display the Work Publicly - Limitations on Exclusive Rights.

UNIT-III:

Copyright Ownership, Transfers, Duration. Registration. and Searching Copyright Ownership Issues -Joint %mks - Ownership in Derivative works -Works Made for hire - Transfers of Copyright - Termination of Transfers of Copyright - Duration of Copyright. Copyright Registart ion Application - Deposit Materials - Application Process and Registration of Copyright - Searching Copyright Office Records- Obtaining Copyright Office Records and Deposit Materials - Copyright Notice.

Copyright Infringement, New Developments in Copyright Law, Semiconductor Chip Protection Act: Elements of Infringement - Contributory Infringement and Vicarious Infringement - Defenses to Infringement- Infringement Actions - Remedies for Infringement. Copyright Protection for Computer Programs - Copyright Protection for Automated Databases - Copyright in the Electronic Age - The Digital Millenium Copyright Act - Recent Developments in Copyright Law - Terms of the Trade - Vessel Hull Protection - Semiconductor Chip Protection.

UNIT-IV:

Law of Patents, Patent Searches, Ownership, Transfer

Patentability - Design Patents - Double Patenting - Patent Searching -- Patent Application Process - Prosecuting the Application, Post-issuance Actions, Term and Maintenance of Patents. Ownership Rights - Sole and Joint Inventors - Disputes over Inventorship - Inventions Made by Employees and Independent Contractors - Assignment of Patent Rights - Licensing of Parent Rights - Invention Developers and Promoters.

UNIT-V:

Patent Infringement. New Developments and International Patent Law

Direct Infringement - Inducement to Infringe - Contributory Infringement - First Sale Doctrine - Claims Interpretation - Defenses to Infringement -- Remedies for Infringement - Resolving an Infringement Dispute - Patent Infringement Litigation. New Developments in Patent Law - International Patent Protection - Paris Convention - Patent Cooperation Treaty - Agreement on Trade Related Aspects of Intellectual Property Rights- Patent Law Treaty.

TEXT BOOK:

1. Intellectual Property Rights by Deborah E. Bouchoux, Cengage Learning

REFERENCES:

1. Managing Intellectual Property- The Strategic Imperative, Second Edition by Vinod V. Sople, PHI Learning Private Limited.

2. Intellectual Property- Copyrights, Trademarks, and Patents by Richard Stim, Cengage Learning

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

INFORMATION SECURITY AND CRYPTOGRAPHY

Objectives:

- Upon completion of this material, you should be able to define information security
- Recount the history of computer security and how it evolved into information security
- Define key terms and critical concepts of information security
- Enumerate the phases of the security systems development life cycle
- Describe the information security roles of professionals within an organization

UNIT – I

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.

UNIT – II

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

UNIT – III

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

UNIT – V

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

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

REFERENCE BOOKS:

1. Cryptography and Network Security : C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
2. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning
3. Cryptography and Network Security : Atul Kahate, Mc Graw Hill, 2nd Edition
4. Principles of Computer Security: WM.Arthur Conklin, Greg White, TMH
5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning
6. Handbook of Security of Networks, Yang Xiao, Frank H Li, Hui Chen, World Scientific, 2011.

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

ETHICAL HACKING

Objectives:

- To learn the ethics and legality of hacking
- To learn about the hacking tools
- To learn the hacking of servers and OS

UNIT I

Introduction to Ethical Hacking, Ethics, and Legality

Ethical Hacking Terminology, Different Types of Hacking Technologies, Different Phases Involved in Ethical Hacking and Stages of Ethical Hacking: Passive and Active Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks, Hacktivism, Types of Hacker Classes, Skills Required to Become an Ethical Hacker, Vulnerability Research, Ways to Conduct Ethical Hacking, Creating a Security Evaluation Plan ,Types of Ethical Hacks, Testing Types, Ethical Hacking Report

Footprinting and Social Engineering

Footprinting, Information Gathering Methodology, Competitive Intelligence ,DNS Enumeration Whois and ARIN Lookups, Types of DNS Records, Traceroute, E-Mail Tracking ,Web Spiders , Social Engineering, Common Types Of Attacks, Insider Attacks, Identity Theft, Phishing Attacks, Online Scams, URL Obfuscation, Social-Engineering Countermeasures.

UNIT II

Scanning and Enumeration

Scanning, types of Scanning , CEH Scanning Methodology ,Ping Sweep Techniques, Nmap Command Switches, SYN, Stealth, XMAS, NULL, IDLE, and FIN Scans, TCP Communication Flag Types, War-Dialing Techniques, Banner Grabbing and OS Fingerprinting Techniques, Proxy Servers, Anonymizers, HTTP Tunneling Techniques, IP Spoofing Techniques , Enumeration, Null Sessions, SNMP Enumeration, Windows 2000 DNS Zone Transfer, Steps Involved in Performing Enumeration

System Hacking

Understanding Password-Cracking Techniques, Understanding the LanManager Hash Cracking Windows 2000 Passwords, Redirecting the SMB Logon to the Attacker SMB Redirection, SMB Relay MITM Attacks and Countermeasures NetBIOS DoS Attacks, Password-Cracking Countermeasures, Understanding Different Types of Passwords Passive Online Attacks, Active Online Attacks, Offline Attacks Nonelectronic Attacks, Understanding Keyloggers and Other Spyware Technologies Understand Escalating Privileges, Executing Applications, Buffer Overflows, Understanding Rootkits Planting Rootkits on Windows 2000 and XP Machines, Rootkit Embedded TCP/IP Stack Rootkit Countermeasures, Understanding How to Hide Files, NTFS File Streaming NTFS Stream Countermeasures, Understanding Steganography Technologies, Understanding How to Cover Your Tracks and Erase Evidence, Disabling Auditing, Clearing the Event Log

UNIT III

Trojans, Backdoors, Viruses, and Worms

Trojans and Backdoors, Overt and Covert Channels, Types of Trojans, Reverse-Connecting Trojans, Netcat Trojan ,Indications of a Trojan Attack, Wrapping, Trojan Construction Kit and Trojan Makers , Countermeasure Techniques in Preventing Trojans, Trojan-Evading Techniques, System File Verification Subobjective to Trojan Countermeasures Viruses and Worms, Difference between a Virus and a Worm, Types of Viruses, Understand Antivirus Evasion Techniques, Understand Virus Detection Methods

Sniffers

Protocols Susceptible to Sniffing, Active and Passive Sniffing, ARP Poisoning, Ethereal Capture and Display Filters, MAC Flooding, DNS Spoofing Techniques, Sniffing Countermeasures

Denial of Service and Session Hijacking

Denial of Service, Types of DoS Attacks, DDoS Attacks, BOTs/BOTNETs, “Smurf” Attack, “SYN” Flooding, DoS/DDoS Countermeasures, Session Hijacking, Spoofing vs. Hijacking, Types of Session Hijacking, Sequence Prediction, Steps in Performing Session Hijacking, Prevention of Session Hijacking

UNIT IV

Hacking Web Servers, Web Application Vulnerabilities, and Web-Based Password Cracking Techniques

Hacking Web Servers, Types of Web Server Vulnerabilities, Attacks against Web Servers, IIS

Unicode Exploits, Patch Management Techniques, Web Server Hardening Methods Web Application Vulnerabilities, Objectives of Web Application Hacking, Anatomy of an Attack, Web Application Threats, Google Hacking, Web Application Countermeasures Web-Based Password Cracking Techniques, Authentication Types, Password Cracker, Password Attacks: Classification ,Password-Cracking Countermeasures

SQL Injection and Buffer Overflows

SQL Injection, Steps to Conduct SQL Injection, SQL Server Vulnerabilities, SQL Injection Countermeasures Buffer Overflows, Types of Buffer Overflows and Methods of Detection, Stack-Based Buffer Overflows, Buffer Overflow Mutation Techniques

UNIT V

Linux Hacking

Linux Basics, Compile a Linux Kernel, GCC Compilation Commands, Install Linux Kernel Modules, Linux Hardening Methods

Penetration Testing Methodologies

Security Assessments, Penetration Testing Methodologies, Penetration Testing Steps, Pen-Test Legal Framework , Automated Penetration Testing Tools ,Pen-Test Deliverables

TEXT BOOKS:

1. CEH official Certfied Ethical Hacking Review Guide, Wiley India Edition
2. Certified Ethical Hacker: Michael Gregg, Pearson Education
3. Certified Ethical Hacker: Matt Walker, TMH.

REFERENCE BOOKS:

1. Computer Security, concepts, issues and implementation: Alfred Basta Wolf Halton, Cengage Learning
2. Hacking Exponsed Web 2.0, by Rich Annings, Himanshu Dwivedi, Zane Lackey, Tata Mcgraw hill Edition
3. Ethical Hacking & Network Defense, Michael T. Simpson, Cengage Learning
4. Hacking Exposed Windows, Joel Scambray, cissp, Stuart Mcclure, Cissp, Third Edition, Tata Mcgraw hill edition
5. Hacking Exposed Window server 2003, Joel Scambray Stuart Mcclure, Tata Mcgraw hill edition

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

FORENSICS AND INCIDENT RESPONSE

UNIT I

Introduction to Incident - Incident Response Methodology – Steps - Activities in Initial Response Phase after detection of an incident

UNIT II

Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system - **Forensic Duplication**: Forensic duplication:Forensic Duplicates as Admissible Evidence,Forensic Duplication Tool Requirements,Creating a Forensic Duplicate/Qualified Forensic Duplicate of a Hard Drive

UNIT III

File Systems: FAT,NTFS - Forensic Analysis of File Systems - **Storage Fundamentals**: Storage Layer, Hard Drives **Evidence Handling:** Types of Evidence,Challenges in evidence handling, Overview of evidence handling procedure

.

UNIT IV

Collecting Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing- Internet Fraud

UNIT V

Data Analysis Techniques - Investigating Live Systems (Windows &Unix) - Investigating Hacker Tools - Ethical Issues - Cybercrime

TEXT BOOKS :

1. Kevin Mandia, Chris Prosise, “Incident Response and computer forensics”,Tata McGrawHill,2006.
2. Peter Stephenson, "Investigating Computer Crime: A Handbook for Corporate Investigations", Sept 1999
3. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, 1st Edition, 2001

REFERENCE BOOKS :

1. Skoudis. E., Perlman. R. Counter Hack: *A Step-by-Step Guide to Computer Attacks and Effective Defenses.*Prentice Hall Professional Technical Reference. 2001.
2. Norbert Zaenglein, "Disk Detective: Secret You Must Know to Recover Information From a Computer", Paladin Press, 2000
3. Bill Nelson,Amelia Philips and Christopher Steuart, “Guide to computer forensics and investigations”,course technology,4th edition,ISBN: 1-435-49883-6

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

DISTRIBUTED SYSTEMS
(ELECTIVE – I)

Objectives:

- To explain what a distributed system is, why you would design a system as a distributed
- system, and what the desired properties of such systems are;
- To list the principles underlying the functioning of distributed systems, describe the problems
- and challenges associated with these principles, and evaluate the effectiveness and
- shortcomings of their solutions;
- To recognize how the principles are applied in contemporary distributed systems, explain how
- they affect the software design, and be able to identify features and design decisions that may
- cause problems;
- To design a distributed system that fulfills requirements with regards to key distributed
- systems properties (such as scalability, transparency, etc.), be able to recognize when this is
- not possible, and explain why;
- To build distributed system software using basic OS mechanisms as well as higher-level
- middleware and languages.

UNIT I

Characterization of Distributed Systems- Introduction, Examples of Distributed systems, Resource sharing and web, challenges, System models- Introduction, Architectural and Fundamental models, Networking and Internetworking, Interprocess Communication.
Distributed objects and Remote Invocation-Introduction, Communication between distributed objects, RPC, Events and notifications, Case study-Java RMI.

UNIT II

Operating System Support- Introduction, OS layer, Protection, Processes and Threads, Communication and Invocation, Operating system architecture, Distributed File Systems-Introduction, File Service architecture, case study- SUN network file systems.
Name Services-Introduction, Name Services and the Domain Name System, Case study of the Global Name Service, Case study of the X.500 Directory Service.

UNIT III

Peer to Peer Systems-Introduction, Napster and its legacy, Peer to Peer middleware, Routing overlays, Overlay case studies-Pastry, Tapestry, Application case studies-Squirrel, OceanStore.
Time and Global States-Introduction, Clocks, events and Process states, Synchronizing physical clocks, logical time and logical clocks, global states, distributed debugging.
Coordination and Agreement - Introduction, Distributed mutual exclusion, Elections, Multicast communication, consensus and related problems.

UNIT IV

Transactions and Concurrency control - Introduction, Transactions, Nested Transactions, Locks, Optimistic concurrency control, Timestamp ordering, Comparison of methods for concurrency controls. Distributed Transactions - Introduction, Flat and Nested Distributed Transactions, Atomic commit protocols, Concurrency control in distributed transactions, Distributed deadlocks, Transaction recovery, Replication-Introduction, System model and group communication, Fault tolerant services, Transactions with replicated data.

UNIT V

Security - Introduction, Overview of Security techniques, Cryptographic algorithms, Digital signatures, Case studies-Kerberos, TLS, 802.11 WiFi.
Distributed shared memory, Design and Implementation issues, Sequential consistency and Ivy case study, Release consistency and Munin case study, other consistency models, CORBA case study-Introduction, CORBA RMI, CORBA Services.

TEXT BOOKS:

1. Distributed Systems Concepts and Design, G Coulouris, J Dollimore and T Kindberg, Fourth Edition, Pearson Education.
2. Distributed Systems, S.Ghosh, Chapman & Hall/CRC, Taylor & Francis Group, 2010.

REFERENCE BOOKS:

1. Distributed Computing, S.Mahajan and S.Shah, Oxford University Press.
2. Distributed Operating Systems Concepts and Design, Pradeep K.Sinha, PHI.
3. Advanced Concepts in Operating Systems, M Singhal, N G Shivarathri, Tata McGraw-Hill Edition.
4. Reliable Distributed Systems, K.P.Birman, Springer.
5. Distributed Systems – Principles and Paradigms, A.S. Tanenbaum and M.V. Steen, Pearson Education.
6. Distributed Operating Systems and Algorithm Analysis, R.Chow, T.Johnson, Pearson.
7. Distributed Operating Systems, A.S.Tanenbaum, Pearson education.
8. Distributed Computing, Principles, Algorithms and Systems, Ajay D. Kshemakalyani & Mukesh Singhal, Cambrigde, rp 2010

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

ADVANCED PROBLEM SOLVING
(ELECTIVE – I)

Unit I

OOP Using Java - Class and Objects, Variables, Operators, Expressions, Methods, Decision statements,Loops,Arrays,OOP concepts- Encapsulation, Inheritance, Polymorphism, Abstraction, Modularity, Exception handling, Input and Output,Java and Pointers,Interfaces,Packages, Abstract classes,Casting in Inheritance hierarchy,Casting with Interfaces,Vectors in java.util,Data Structures and OOP,Writing a java program-Design,coding,testing and debugging.

Basic concepts(Review)- Abstact Data Types, Data structures, Algorithms- Characteristics of Algorithms, Performance analysis- Time complexity and Space complexity,Asymptotic Analysis- Big O, Omega and Theta notations.

Unit II

Linear data structures- The List ADT, Array and Linked Implementations,Singly Linked Lists-Operations-Insertion,Deletion,Traversals,DoublyLinkedLists-Operations-Insertion,Deletion,SkipLists-implementation, StackADT,definitions,operations, Array and Linked implementations,applications-infix to postfix conversion, recursion implementation,tail recursion,nontail recursion,indirect recursion, QueueADT, definitions and operations ,Array and Linked Implementations,Priority Queue ADT,Deque ADT,Implementation using doubly linked lists,Stacks and Queues in java.util.

Unit III

Non Linear data structures-Trees-Basic Terminology, Binary tree ADT,array and linked representations,iterative traversals,threaded binary trees,Applications-Disjoint-Sets,Union and Find algorithms,Huffman coding,General tree to binary tree conversion, Realizing a Priority Queue using Heap.

Search Trees- Binary Search Tree ADT, Implementation, Operations- Searching, Insertion and Deletion, Balanced Search trees-AVL Trees, Operations – Insertion and Searching,B-Trees, B-Tree of order m,Operations- Insertion,Deletion and Searching,Introduction to Red-BlackTrees, Splay Trees,B*-Trees,B+-Trees(Elementary treatement), Comparison of Search Trees,Trees in java.util.

Unit IV

Searching- Linear Search,Binary Search, Hashing-Hash functions,Collision-Handling schemes,Hashing in java.util,Dictionary ADT,Linear list representation,Skip list representation,Hash table representation,Comparison of Searching methods.

Sorting- Bubble Sort,Insertion Sort,Shell sort,Heap Sort,Radix Sort,Quick sort,Merge sort, Comparison of Sorting methods,Sorting in java.util.

Unit V

Graphs–Basic Terminology, Graph Representations- Adjacency matrix,Adjacency lists,Adjacency multilists,Graph traversals- DFS and BFS, Spanning trees-Minimum cost spanning trees,Kruskal's Algorithm for Minimum cost Spanning trees, Shortest paths- Single Source Shortest Path Problem,All Pairs Shortest Path Problem.

Text Processing **-** Pattern matching algorithms- The Knuth-Morris-Pratt algorithm,The Boyer-Moore algorithm,Tries- Standard Tries, Compressed Tries, Suffix tries.

TEXT BOOKS :

1. Data structures and Algorithms in Java,Adam Drozdek,Cengage Learning.
2. Data structures and Algorithms in Java,Michael T.Goodrich and R.Tomassia , Wiley India edition.
3. Data structures , Algorithms and Applications in Java,S.Sahani, Universities Press.

REFERENCE BOOKS :

1. Data structures and algorithms in Java,Robert Lafore,Pearson Education.
2. Data structures with Java,W.H.Ford and W.R.Topp,Pearson Education.

3. Classic Data structures in Java,T.Budd,Pearson Education.
4. Data Structures using Java,D.S. Malik and P.S.Nair, Cengage Learning,
5.An Introduction to Data structures and Algorithms,J.A.Storer,Springer.
6.Data structures and Java Collections Frame Work,W.J.Collins,Mc Graw Hill.
7.Data structures with Java,J.R.Hubbard and A.Huray,PHI.
8.Data Structures using Java,Y.Langsam,M.Augenstein,A.Tanenbaum,Pearson Education.
9.Data structures with Java,J.R.Hubbard,Schaum's Outlines,TMH.

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

NETWORK PROGRAMMING
(ELECTIVE –I)

Objectives:

- To understand to Linux utilities
- To understand file handling, signals
- To understand IPC, network programming in Java
- To understand processes to communicate with each other across a Computer Network.

UNIT – I

Linux Utilities- File handling utilities, Security by file permissions, Process utilities, Disk utilities, Networking utilities, Filters, Text processing utilities and Backup utilities.

Bourne again shell(bash) - Introduction, pipes and redirection, here documents, running a shell script, the shell as a programming language, shell meta characters, file name substitution, shell variables, command substitution, shell commands, the environment, quoting, test command, control structures, arithmetic in shell, shell script examples.

Review of C programming concepts-arrays, strings (library functions), pointers, function pointers, structures, unions, libraries in C.

UNIT - II

Files- File Concept, File types File System Structure, Inodes, File Attributes, file I/O in C using system calls, kernel support for files, file status information-stat family, file and record locking-lock and fcntl functions, file permissions- chmod, fchmod, file ownership-chown, lchown, fchown, links-soft links and hard links – symlink, link, unlink.

File and Directory management – Directory contents, Scanning Directories- Directory file APIs.

Process- Process concept, Kernel support for process, process attributes, process control – process creation, replacing a process image, waiting for a process, process termination, zombie process, orphan process.

UNIT - III

Signals- Introduction to signals, Signal generation and handling, Kernel support for signals, Signal function, unreliable signals, reliable signals, kill, raise , alarm, pause, abort, sleep functions.

Interprocess Communication - Introduction to IPC mechanisms, Pipes- creation, IPC between related processes using unnamed pipes, FIFOs-creation, IPC between unrelated processes using FIFOs(Named pipes), differences between unnamed and named pipes, popen and pclose library functions, Introduction to message queues, semaphores and shared memory.

Message Queues- Kernel support for messages, UNIX system V APIs for messages, client/server example.

Semaphores-Kernel support for semaphores, UNIX system V APIs for semaphores.

UNIT – IV

Shared Memory- Kernel support for shared memory, UNIX system V APIs for shared memory, client/server example.

Network IPC - Introduction to Unix Sockets, IPC over a network, Client-Server model ,Address formats(Unix domain and Internet domain), Socket system calls for Connection Oriented - Communication ,Socket system calls for Connectionless - Communication, Example-Client/Server Programs- Single Server-Client connection, Multiple simultaneous clients, Socket options - setsockopt , getsockopt , fcntl.

UNIT-V

Network Programming in Java-Network basics, TCP sockets, UDP sockets (datagram sockets), Server programs that can handle one connection at a time and multiple connections (using multithreaded server), Remote Method Invocation (Java RMI)-Basic RMI Process, Implementation details-Client-Server Application.

TEXT BOOKS:

1. Unix System Programming using C++, T.Chan, PHI. (Units II, III, IV)
2. Unix Concepts and Applications, 4th Edition, Sumitabha Das, TMH.(Unit I)
3. An Introduction to Network Programming with Java, Jan Graba,Springer, rp 2010.(Unit V)
4. Unix Network Programming ,W.R. Stevens, PHI.(Units II,III,IV)
5. Java Network Programming,3rd edition, E.R. Harold, SPD, O'Reilly.(Unit V)

REFERENCE BOOKS:

1. Linux System Programming, Robert Love, O'Reilly, SPD.
2. Advanced Programming in the UNIX environment, 2nd Edition, W.R.Stevens, Pearson Education.
3. UNIX for programmers and users, 3rd Edition, Graham Glass, King Ables, Pearson Education.
4. Beginning Linux Programming, 4th Edition, N.Matthew, R.Stones,Wrox, Wiley India Edition.
5. UNIX Network Programming The Sockets Networking API, Vol.-I, W.R.Stevens, Bill Fenner, A.M.Rudoff, Pearson Education.
6. UNIX Internals, U.Vahalia, Pearson Education.
7. UNIX shell Programming, S.G.Kochan and P.Wood, 3rd edition, Pearson Education.
8. C Programming Language, Kernighan and Ritchie, PHI

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

OPERATING SYSTEMS ADMINISTRATION AND SECURITY

(ELECTIVE –II)

UNIT I

Introduction- Computer system Organization and Architecture- Operating System structure and operations- Protection and Security- Process Management- Process Scheduling – Inter process communication- Multi threading models- Semaphores- Deadlocks- Mutexes- Critical Section problem

UNIT II

Memory Management: Swapping, Segmentation, Page replacement algorithms- File Systems: File system mounting and sharing, File system implementation and allocation methods- Device management: Disk structure, scheduling and management, I/O hardware and kernel I/O subsystem

UNIT III

Open source operating system- Linux Kernel architecture- User administration in Linux- Services offered by Linux OS- Configuration of email service, web service, NFS, DNS in Linux- Syntactical Interpretation of various files related to different services in Linux

UNIT IV

Secure operating systems- Security goals- Trust model- Threat model- Access Control fundamentals: Lampson's access matrix, mandatory protection systems, Reference monitor- Secure operating system definition- Assessment criteria

UNIT V

Security in Windows and Unix: Protection system, authorization, security analysis and vulnerabilities- The security kernel- Secure communications processor – Retrofitting security into operating systems

TEXT BOOKS :

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, *Operating System Concepts*, John Wiley & Sons ,Inc., 9th Edition,2012
2. William Stallings, *Operating System: Internals and Design Principles*, Prentice Hall, 7th Edition,2012 Technology", Academic Press, 1st Edition, 2001

REFERENCE BOOKS :

1. Tom Adelstein and Bill Lubanovic, *Linux System Administration*, O'Reilly Media, Inc.,1st Edition, 2007
2. Trent Jaeger, Operating Systems Security, Morgan & Claypool Publishers, 2008
3. Michael J.Palmer, Guide to Operating Systems Security, Thomson/Course Technology, 2004

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

BIOMETRIC SECURITY
(ELECTIVE – II)

UNIT I

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

UNIT II

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

UNIT III

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

UNIT IV

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

UNIT V

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.

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

DATABASE SECURITY
(ELECTIVE – II)

Objectives:

- To learn the security of databases
- To learn the design techniques of database security
- To learn the secure software design

UNIT I

Introduction

Introduction to Databases Security Problems in Databases Security Controls Conclusions

Security Models -1

Introduction Access Matrix Model Take-Grant Model Acten Model PN Model Hartson and Hsiao's Model Fernandez's Model Bussolati and Martella's Model for Distributed databases

UNIT II

Security Models -2

Bell and LaPadula's Model Biba's Model Dion's Model Sea View Model Jajodia and Sandhu's Model The Lattice Model for the Flow Control conclusion

Security Mechanisms

Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation Criteria

UNIT III

Security Software Design

Introduction A Methodological Approach to Security Software Design Secure Operating System Design Secure DBMS Design Security Packages Database Security Design

UNIT IV

Statistical Database Protection & **Intrusion Detection Systems**

Introduction Statistics Concepts and Definitions Types of Attacks Inference Controls evaluation Criteria for Control Comparison .Introduction IDES System RETISS System ASES System Discovery

UNIT V

Models For The Protection Of New Generation Database Systems -1

Introduction A Model for the Protection of Frame Based Systems A Model for the Protection of Object-Oriented Systems SORION Model for the Protection of Object-Oriented Databases

Models For The Protection Of New Generation Database Systems -2

A Model for the Protection of New Generation Database Systems: the Orion Model Jajodia and Kogan's Model A Model for the Protection of Active Databases Conclusions

TEXT BOOKS:

1. Database Security and Auditing, Hassan A. Afyouni, India Edition, CENGAGE Learning, 2009.
2. Database Security, *Castano,* Second edition, Pearson Education.

REFERENCE BOOK:

1. Database security by alfred basta, melissa zgola, CENGAGE learning.

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – I Sem.**

ETHICAL HACKING & NETWORK SECURITY LAB

ETHICAL HACKING:
The following exercises have to be performed using various software tools/utilities

1. **Web Based Email Attacks & Security**
   Working of Email
   E-mail Server
   - E-mail Server Setup
   - Sending mails through Email Server

   E-mail Forgery
   - What is E-mail Forgery – Fake Mail
   - Sending fake E-mails

   Using Websites
   Using Scripts
   E-mail Bombing
   Attacking E-mail Password
   - Introduction to Various Attacks

   Phishing
   Desktop Phishing
   Cookies Stealing
   Non-Technical Attacks
   Social Engineering
   Shoulder Surfing
   Investigating an E-mail
   - Analysing E-mail Header
   - Tracing E-mail

   Defensive-measures
   Electronic Transaction Security
2. **Windows OS Hacking**
   Cracking Windows Login Password – Various Attacks
   - Password Guessing
   - Dictionary Attack
   - Brute-force Attack
   - Rainbow Table Attack

   Creating Backdoors
   - Bootkits
   - Hidden User Account in Windows
   - Bypassing the Login Screen

   Introduction to Steganography
   Hiding Files behind an Image
   Creating File and Folder Locks
   Defensive measures
   - Restricting Files & Folders Access
   - Strong Password Configuration
   - BIOS Boot Order
   - BIOS Security Options
   - Physical Security

   Windows Tips & Tricks
   - Account Privilege Escalation
   - Browser Hacks
   - Registry Tweaks
   - Customizing Login Screen
   - Multiple GTalk & Yahoo Messenger
3. **Understanding Malwares Working & Detection**
   Trojan Working Methods
   - Direct Connection

- Reverse Connection

Viruses Working
- Why Viruses are created?
- Introduction to Batch Programming
- Viruses through Batch Programming

Spyware Working
- Introduction to Keyloggers
- Password Cracking using Keylogger
- Types of Keyloggers

Detection & Removal of Malwares
- Automatic Process

Using Anti-Malware Software
- Manual Process

Using TCP View

Monitoring Process

4. **Networking Attacks & Security**

Tips & Tricks
- Netstat
- Tracert
- Telnet

Firewall & IDS

5. **Wi-Fi Attacks & Security**

Accessing Wireless Network
- WEP Key Cracking

Wireless Attack Methods
- War Driving
- War Walking
- MAC Address Spoofing
- Creating Rouge Wireless Access Point

Defensive-measures
- MAC Filtering
- Configuring Strong Key
- Setting up a Proxy Server

6. **Web Server Attacks & Security**

Web Server Attack Vectors
- Breaking into Database using SQL Injection
- Web Ripping
- Directory Traversal attack
- PHP Remote Code Execution

Defensive Measures
- Input Validation
- Controlling Directory Access
- Monitoring of Web Server

7. **Hacking Using Google**

Google as a Hacking Tool.
- Digging Websites

Defensive Measures
- Restricting Google to Website

8. **Software Reverse Engineering**

Software Assembly Code Analysis

Software Disassembling

Software Key Phishing

Software Patching
- Generating Patch
- Executing the Patch

Software Manipulation
- Finding the Decisive Code
- Modifying the Software Code

Defensive Measures
- Encrypting Application
- Setup Encrypters

- Serial Key Algorithms

9. VOIP & Mobile Hacking

Call Forgery

- Making Fake Calls

SMS Forgery

- Sending Fake SMSs to Any Phone

NETWORK SECURITY :

Objectives:

- The Network Security Lab tries to present several hands-on exercises to help reinforce the
- students knowledge and understanding of the various network security aspects.
- The lab exercises are divided into two parts A & B.
- Part A deals with the implementation of cryptographic algorithms.
- Part B deals with usage of various security attacks/defenses related tools and utilities.

PART – A

The following exercises are based on the cryptographic algorithms. They can be implemented using C, C++, Java, etc.

1. Write a C program that contains a string(char pointer) with a value 'Hello world'. The program should XOR each character in this string with 0 and displays the result.
2. Write a C program that contains a string(char pointer) with a value 'Hello world'. The program should AND or and XOR each character in this string with 127 and display the result.
3. Write a Java program to perform encryption and decryption using the following algorithms
a. Ceaser cipher
b. Substitution cipher
c. Hill Cipher
4. Write a C program to implement the DES algorithm logic.
5. Write a JAVA program to implement the DES algorithm logic.
6. Write a Java program that contains functions, which accept a key and input text to be encrypted/decrypted. This program should use the key to encrypt/decrypt the input by using the triple Des algorithm. Make use of Java Cryptography package.
7. Write a C/JAVA program to implement the Blowfish algorithm logic.
8. Write a C/JAVA program to implement the Rijndael algorithm logic.
9. Write the RC4 logic in Java
10. Using Java cryptography, encrypt the text "Hello world" using Blowfish. Create your own key using Java keytool.
11. Implement DES-2 and DES-3 using Java cryptography package.
12. Write a Java program to implement RSA algorithm.
13. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties(Alice) and the JavaScript application as the other party(Bob)
14. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.
15. Calculate the message digest of a text using the MD5 algorithm in JAVA.
16. Explore the Java classes related to digital certificates.
17. Create a digital certificate of your own by using the Java keytool.
18. Write a Java program to encrypt users passwords before they are stored in a database table, and to retrieve them whenever they are to be brought back for verification.
19. Key generation(public and private key pair) can be performed using Java. Write a program which can do this.
20. Write a program in java, which performs a digital signature on a given text.
21. Study phishing in more detail. Find out which popular bank sites have been phished and how.

PART - B

The following exercises have to be performed using various software tools/utilities mentioned

1) Passive Information Gathering
   a) IP Address and Domain Identification of log entries – DNS, RIR, etc tools
   b) Information Gathering of a web site: WHOIS, ARIN, etc tools
   c) Banner Grabbing: Netcat, etc tools
2) Detecting Live Systems

a) Port Scanning : Nmap,SuperScan
b) Passive Fingerprinting: Xprobe2
c) Active Fingerprinting: Xprobe2

3) Enumerating Systems
   a) SNMP Enumeration: SolarWinds IP Network Browser,
4) www.solarwinds.com/downloads
   a) Enumerating Routing Protocols: Cain & Abel tool, www.oxid.it
5) Automated Attack and Penetration Tools
   a) Exploring N-Stalker, a Vulnerability Assessment Tool, www.nstalker.com
6) Defeating Malware
   a) Building Trojans, Rootkit Hunter: www.rootkit.nl/projects/rootkit_hunter.html
   b) Finding malware
7) Securing Wireless Systems
   a) Scan WAPs: NetStumbler, www.netstumbler.com/downloads
   b) Capture Wireless Traffic: Wireshark, www.wireshark.org

TEXT BOOK:

1. Build Your Own Security Lab, Michael Gregg, Wiley India.

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

ADVANCED COMPUTER NETWORKS

Objectives:

- The objective of this course is to build a solid foundation in computer networks concepts and design
- To understand computer network architectures, protocols, and interfaces.
- The OSI reference model and the Internet architecture network applications.
- The course will expose students to the concepts of traditional as well as modern day
- computer networks - wireless and mobile, multimedia-based.
- Students completing this course will understand the key concepts and practices employed in modern computer networking

Course description: This course will enable the student to refresh the fundamentals of Computer Networks in Unit I. Unit II describes the architecture, components, and operation of routers, and explains the principles of Routing and Routing protocols. Especially the Routing protocols need to be understood thoroughly with the help of any freely downloadable simulator tool. Through Unit III a student can learn the technologies and protocols needed to design and implement a converged switched network. This section explains how to configure a switch for basic functionality and how to implement Virtual LANs, VTP, and Inter-VLAN routing in a converged network. Students need to develop the necessary skills to implement a WLAN in a small-to-medium network. This course in Unit IV discusses the WAN technologies and network services required by converged applications in enterprise networks. Unit V makes the student to implement networking using Java programs.

Suggested Simulator tools: NS-2/*NS-3, OPNET, Packet Tracer, Boson, Wireshark.*

UNIT I: Review

Computer Networks and the Internet: History of Computer Networking and the Internet, Networking Devices, The Network edge, The Network core, Access Networks and Physical media, ISPs and Internet Backbones.

Networking Models: 5-layer TCP/IP Model, 7-Layer OSI Model, Internet Protocols and Addressing, Equal-Sized Packets Model: ATM.

UNIT II: Network Routing

Routing and its concepts: Structure of a Router, Basic Router Configuration, Building a Routing Table, Static Routing, Dynamic Routing – Distance Vector Routing Protocol (RIPv1, RIPv2, EIGRP), Link State Routing Protocols (OSPF).

UNIT III: LAN Switching

Switching and its concepts: Structure of a Switch, Basic Switch Configuration, Virtual LANs (VLANs), VLAN Trunking Protocol (VTP), Spanning Tree Protocol (STP), Inter-VLAN Routing.

UNIT IV: Wide Area Networks (WANs)

Introduction to WANs, Point-to-Point Protocol (PPP) concepts, Frame Relay concepts, Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT), IPv6.

UNIT V: Network Programming using Java

TCP sockets, UDP sockets (datagram sockets), Server programs that can handle one connection at a time and multiple connections (using multithreaded server), Remote Method Invocation (Java RMI) - Basic RMI Process, Implementation details - Client-Server Application.

TEXT BOOKS:

1. Computer Networking: A Top-Down Approach Featuring the Internet, *James F. Kurose, Keith W.Ross*, Fifth Edition, Pearson Education, 2012.
2. Network Fundamentals, Mark Dye, Pearson Education.
3. Routing Protocols & Concepts, Rick Graziani, Pearson Education.
4. LAN Switching & Wireless, Wayne Lewis, Pearson Education.
5. Accessing the WAN, Bob Vachon, Pearson Education.
6. An Introduction to Network Programming with Java, Jan Graba, Springer, rp 2010.

REFERENCE BOOKS:

1. Computer Networks: A Systems approach, *Larry L. Peterson & Bruce S. Davie,* Fifth edition, Elsevier, rp2012.
2. Computer Networks: A Top-Down Approach, *Behrouz A. Forouzan, Firoz Mosharaf*, Tata McGraw Hill, 2012.
3. Java Network Programming,3rd edition, *E.R. Harold*, SPD, O'Reilly.(Unit V)
4. An Engineering Approach to Computer Networking*, S.Keshav,* Pearson Education, 1997.
5. Computer Networks: Principles, Technologies And Protocols For Network Design, *Natalia Olifer, Victor Olifer*, Wiley India, 2006.
6. Computer Networks, *Andrew S. Tanenbaum*, Fifth Edition, Prentice Hall.
7. Computer and Communication Networks, *Nader F. Mir,* Pearson Education, 2007
8. Data Communications and Networking, *Behrouz A. Forouzan*, Fourth Edition, Tata McGraw Hill, 2007.
9. Computer Networks, *Bhushan Trivedi,* Oxford University Press, 2011.
10. Fundamentals of Business Data Communications, *Jerry FitzGerald and Alan Dennis*, Tenth Edition, Wiley, 2009.
11. Internetworking with TCP/IP: Principles, Protocols and Architecture, Volume 1, *Douglas E. Comer,* 4th edition, PHI, 2005.
12. Next-Generation Internet: Architectures and Protocols, Byrav Ramamurthy et al, Cambridge, 2011.

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

MOBILE AND DIGITAL FORENSICS

Objectives:

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

Unit I (9 hours)

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.

Unit II (9 hours)

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

Unit III (**12 hours)**

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

Unit IV (7 hours)

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 contamination-

Unit V (8 hours)

Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locations- Seven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context

References

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

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

CYBER FORENSICS

UNIT-I

Computer Forensics Fundamentals: What is Computer Forensics?, Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources/Employment Proceedings, Computer Forensics Services, Benefits of Professional Forensics Methodology, Steps taken by Computer Forensics Specialists

Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement - Computer Forensic Technology - Types of Business Computer Forensic Technology

Computer Forensics Evidence and Capture: Data Recovery Defined -Data Back-up and Recovery-The Role of Back-up in Data Recovery - The Data- Recovery Solution

UNIT-II

Evidence Collection and Data Seizure: Why Collect Evidence? Collection Options obstacles-- Types of Evidence - The Rules of Evidence-Volatile Evidence - General Procedure - Collection and Archiving - Methods of Collection -Artifacts - Collection Steps - Controlling Contamination: The Chain of Custody

Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene - Computer Evidence Processing Steps - Legal Aspects of Collecting and Preserving Computer Forensic Evidence

Computer Image Verification and Authentication: Special Needs of Evidential Authentication - Practical Consideration -Practical Implementation

UNIT-III

Computer Forensics analysis and validation: Determining what data to collect and analyze, validating forensic *data.* addressing data-hiding techniques, performing remote acquisitions

Network Forensics: Network forensics overview, performing live acquisitions, developing standard procedures for network forensics, unsing network tools, examining the honeynet project.

Processing Crime and Incident Scenes: Identifying digital evidence. collecting evidence in private-sector incident scens, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, seizing digital evidence at the scene, storing digital evidence, obtaing a digital hash, reviewing a case

UNIT—IV

Current Computer Forensic tools: evaluating computer forensic tool needs, computer lOrensics software tools, computer forensics hardware tools, validating and testing forensics software

E-Mail Investigations: Exploring the role of e-mail in investigation, exploring the roles of the client and server in e-mail, investigating e-mail crimes and violations, understanding e-mail servers, using specialized e-mail forensic tools

Cell phone and mobile device forensics: Understanding mobile device forensics, understanding acquisition procedures for cell phones arid mobile devices.

UNIT— V

Working with Windows and DOS Systems: understanding file systems, exploring Microsoft File Structures.

Examinig NTH disks. Understanding whole disk encryption, windows registry. NI icrosoft startup tasks. MS-DOS

startup tasks, virtual machines.

TEXT BOOK:

1. Computer Forensics, Computer Crime Invistigation by Jhon R. Vacca, Firewall Media, New Delhi.
2. Computer Forensics and Investigations by Nelson. Phillips Enfinger.Steuart, CENGAGE Learning

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

INFORMATION SECURITY MANAGEMENT AND STANDARDS

Objectives:

- Compile, analyze, and assess the applicability of best practices in addressing information
- security issues relevant to the cybersecurity community
- Evaluate the impact of business constraints and processes on the implementation of
- information security programs
- Integrate principles and techniques of risk analysis, project planning and change
- management in the development of information security strategies
- Demonstrate secondary research skills in the investigation and selection of best practice
- solutions to address information security challenges
- Demonstrate mastery of theory, concepts and skills in addressing specialized aspects of
- information security management

UNIT I

Information Security Management in Organizations: Security Policy, Standards, Guidelines and Procedures, Information Security Management System (ISMS), Organizational responsibility for Information Security Management, Information Security Awareness Scenario in Indian Organizations, Building Blocks of Information Security

UNIT II

Risk Management: Overview of Risk Management, Risk Identification, Risk Assessment, Risk Control, Quantitative and Qualitative Approaches, Introduction to OCTAVE and COBIT approach.

UNIT III

Finding Networking vulnerabilities, Firewalls – Processing modes, Categorization, Architectures, Selecting the right firewall, managing the firewalls. Intrusion Detection and Prevention Systems (IDS & IPS), Protecting Remote Connections – Virtual Private Networks for security

UNIT IV

Introduction to security audits, need for security audits, organizational roles, Auditor's roles, Types of security audits, Audit approaches, Technology based audits. Business Continuity and Disaster Recovery Planning.

UNIT V

Overview of ISO 17799/ISO 27001 Standards, System Security Engineering Capability Maturity Model (SSE-CMM). Legal, Ethical, and professional Issues in Information Security.

TEXT BOOKS:

1. Information Systems Security, *Nina Godbole*, Wiley India, 2009
2. Principles and Practices of Information Security. *Michael E. Whitman, Herbert J. Mattord*, Cengage Learning,

REFERENCES:

1. Microsoft Security Risk Management Guide
2. Risk Management Guide for Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
3. OCTAVE approach http://www.cert.org/octave/
4. COBIT http://www.isaca.org/
5. Guide to Firewalls and Policies (Unit 3) http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
6. Firewalls and Network Security, Micheal E.Whitman, et al. Cengage Learning, 2008
7. Audit Trails (Unit 7) http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter18.html
8. Information Security Management Handook, Harold F. Tipton, CRC Press, 2012
9. Information Security Policies and Procedures, 2nd Edition, Thomas R. Peltier, Auerbach, 2004

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

STORAGE AREA NETWORKS
(ELECTIVE – III)

UNIT I:

Introduction to Storage Technology Review data creation and the amount of data being created and understand the value of data to a business, challenges in data storage and data management, Solutions available for data storage, Core elements of a data center infrastructure, role of each element in supporting business activities

UNIT II:

Storage Systems Architecture Hardware and software components of the host environment, Key protocols and concepts used by each component ,Physical and logical components of a connectivity environment ,Major physical components of a disk drive and their function, logical constructs of a physical disk, access characteristics, and performance Implications, Concept of RAID and its components , Different RAID levels and their suitability for different application environments: RAID 0, RAID 1, RAID 3, RAID 4, RAID 5, RAID 0+1, RAID 1+0, RAID 6, Compare and contrast integrated and modular storage systems ,High-level architecture and working of an intelligent storage system

UNIT III:

Introduction to Networked Storage Evolution of networked storage, Architecture, components, and topologies of FC -SAN, NAS, and IP-SAN, Benefits of the different networked storage options, understand the need for long-term archiving solutions and describe how CAS fulfills the need, understand the appropriateness of the different networked storage options for different application environments

UNIT IV:

Information Availability & Monitoring & Managing Datacenter List reasons for planned/unplanned outages and the impact of downtime, Impact of downtime, Differentiate between business continuity (BC) and disaster recovery (DR) ,RTO and RPO, Identify single points of failure in a storage infrastructure and list solutions to mitigate these failures ,Architecture of backup/recovery and the different backup/recovery topologies , replication technologies and their role in ensuring information availability and business continuity, Remote replication technologies and their role in providing disaster recovery and business continuity capabilities Identify key areas to monitor in a data center, Industry standards for data center monitoring and management, Key metrics to monitor for different components in a storage infrastructure, Key management tasks in a data center

UNIT V:

Securing Storage and Storage Virtualization Information security, Critical security attributes for information systems, Storage security domains, List and analyzes the common threats in each domain, Virtualization technologies, block -level and file - level virtualization technologies and processes Case Studies The technologies described in the course are reinforced with EMC examples of actual solutions. Realistic case studies enable the participant to design the most appropriate solution for given sets of criteria.

TEXT BOOK:

1.EMC Corporation, Information Storage and Management, Wiley.

REFERENCE BOOKS:

1.Robert Spalding, “Storage Networks: The Complete Reference“, Tata McGraw Hill, Osborne, 2003.
2.Marc Farley, “Building Storage Networks”, Tata McGraw Hill ,Osborne, 2001.
3.Meeta Gupta, Storage Area Network Fundamentals, Pearson Education Limited, 2

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

MALWARE ANALYSIS
(ELECTIVE – III)

Objectives:

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

UNIT I INTRODUCTION

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

UNIT II 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.

UNIT III VIRUS DESIGN AND ITS IMPLICATIONS

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

UNIT IV 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.

UNIT V 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. ISBN 10: 2-287-23939-1

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

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

PENETRATION TESTING & VULNERABILITY ASSESSMENT
(ELECTIVE – III)

Objectives:

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

Unit I Introduction
Ethical Hacking terminology- Five stages of hacking- Vulnerability Research- Legal implication of hacking- Impact of hacking.
Unit II Foot printing & Social engineering
Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks.
Unit III Scanning & Enumeration
Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting- Enumeration.
Unit IV System Hacking
Password cracking techniques- Key loggers- Escalating privileges- Hiding Files- Steganography technologies- Countermeasures.
Unit V 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.

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

CLOUD ARCHITECTURES AND SECURITY
(ELECTIVE – IV)

Objectives:

- Understand the fundamentals of cloud computing.
- Understand the requirements for an application to be deployed in a cloud.
- Become knowledgeable in the methods to secure cloud.

Unit I

Cloud Computing Fundamental: Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture.

Unit II

Cloud Applications: Technologies and the processes required when deploying web services-Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages- Development environments for service development; Amazon, Azure, Google App.

Unit III

Security Concepts: Confidentiality, privacy, integrity, authentication, non-repudiation, availability, access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud;

Unit IV

Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud provider can provide this- Virtualization System Security Issues: e.g. ESX and ESXi Security, ESX file system security- storage considerations, backup and recovery- Virtualization System Vulnerabilities

Unit V

Security management in the cloud – security management standards- SaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud

TEXT BOOKS:

1. GautamShroff, *Enterprise Cloud Computing Technology Architecture Applications* [ISBN: 978-0521137355]
2. Toby Velte, Anthony Velte, Robert Elsenpeter, *Cloud Computing, A Practical Approach* [ISBN: 0071626948]
3. Tim Mather, SubraKumaraswamy, ShahedLatif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance* [ISBN: 0596802765]
4. Ronald L. Krutz, Russell Dean Vines, *Cloud Security* [ISBN: 0470589876]

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

WIRELESS NETWORKS AND MOBILE COMPUTING
(ELECTIVE – IV)

Objectives:
The main objective of this course is to provide the students with the competences required for understanding and using the communications component of an universal communications environment. Students will be provided, in particular, with the knowledge required to understand

- emerging communications networks,
- their computational demands,
- the classes of distributed services and applications enabled by these networks, and
- the computational means required to create the new networks and the new applications.

UNIT I
WIRELESS NETWORKS: Wireless Network, Wireless Network Architecture, Wireless Switching Technology, Wireless Communication problem, Wireless Network Reference Model, Wireless Networking Issues & Standards. **MOBILE COMPUTING:** Mobile communication, Mobile computing, Mobile Computing Architecture, Mobile Devices, Mobile System Networks, Mobility Management
UNIT II
WIRELESS LAN: Infra red Vs radio transmission, Infrastructure and Ad-hoc Network, IEEE 802.11: System Architecture, Protocol Architecture, 802.11b, 802.11a, Newer Developments, HIPERLAN 1, HIPERLAN 2, Bluetooth : User Scenarios, Architecture.
UNIT III
GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS (GSM): Mobile Services, System Architecture, Protocols, Localization & Calling, Handover, Security. **GPRS:** GPRS System Architecture, **UMTS**: UMTS System Architecture. **LTE**: Long Term Evolution
UNIT IV
MOBILE NETWORK LAYER: Mobile IP: Goals, Assumptions, Entities and Terminology, IP Packet Delivery, Agent Discovery, Registration, Tunneling and Encapsulation, Optimizations, Dynamic Host Configuration Protocol (DHCP)
UNIT V
MOBILE TRANSPORT LAYER: Traditional TCP, Indirect TCP, Snooping TCP, Mobile TCP, Fast retransmit/fast recovery, Transmission /time-out freezing, Selective retransmission, Transaction oriented TCP, TCP over 2.5G/3G Wireless Networks.
TEXT BOOKS:
1. Jochen Schiller, “Mobile Communications”, Pearson Education, Second Edition, 2008.
2. Dr. Sunilkumar, et al “Wireless and Mobile Networks: Concepts and Protocols”, Wiley India.
3. Raj Kamal, “Mobile Computing”, OXFORD UNIVERSITY PRESS.

REFERENCE BOOKS:
1. Asoke K Talukder, et al, “Mobile Computing”, Tata McGraw Hill, 2008.
2. Matthew S.Gast, “802.11 Wireless Networks”, SPD O’REILLY.
3. Ivan Stojmenovic, “Handbook of Wireless Networks and Mobile Computing”, Wiley, 2007.
4. Kumkum Garg, “Mobile Computing”, Pearson.
5. Handbook of Security of Networks, Yang Xiao, Frank H Li, Hui Chen, World Scientific, 2011.

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

APPLICATIONS OF NETWORK SECURITY
(ELECTIVE – IV)

Objectives:

- To understand the latest technologies related to network security
- To understand the IEEE 802.11 security
- To understand the GSM and UMTS security
- To understand IDS, IPS
- To understand Computer Forensics

UNIT – I

IEEE 802.11 Wireless LAN Security: Background, Authentication: Pre- WEP Authentication, Authentication in WEP, Authentication and key agreement in 802.11i, Confidentiality and Integrity: Data protection in WEP, Data protection in TKIP and CCMP

UNIT –II

Cell Phone Security: Preliminaries, GSM(2G) Security, Security in UMTS(3G)

UNIT – III

Non-Cryptographic Protocol Vulnerabilities: DoS and DdoS, Session Hijacking and Spoofing, Pharming Attacks, Wireless LAN Vulnerabilities **Software Vulnerabilities:** Phishing, Buffer Overflow, Format String Attacks, Cross-Site Scripting(XSS), SQL Injection **Access Control in the Operating System:** Preliminaries, Discretionary Access Control – Case Studies: Windows/ Unix, Mandatory Access Control, Role-Based Access Control, SELinux and Recent Trends

UNIT –I V

Intrusion Prevention and Detection: Introduction, Prevention versus Detection, Types of Intrusion Detection systems, DdoS Attack Prevention/Detection, Malware Defense

Web Services Security: Motivation, Technologies for Web Services: XML, SOAP, WSDL and UDDI, SSl, WS-Security, SAML, Ws-Trust, WS-Security Policy

UNIT – V

Computer and Network Forensics: Definition, Computer Forensics: History of Computer Forensics, Elements of Computer Forensics, Investigative Procedures, Analysis of Evidence, Network Forensics: Intrusion Analysis, Damage Assessment, Forensic Tools: Computer Forensic tools, Network Forensic Tools

TEXT BOOKS:

1. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning
2. Computer Network Security: Joseph Migga Kizza, Springer link

REFERENCE BOOKS:

1. Cyber Security: Nina Godbole, Sunit Belapure, Wiley India.
2. Network Security Hacks: Andrew Lockhart, O'Reilly, SPD.
3. Cryptography and Network Security : Forouzan Mukhopadhyay, Mc Graw Hill, 2nd Edition
4. Principles of Computer Security: WM.Arthur Conklin, Greg White, TMH
5. Wireless Security-Models, Threats, and Solutions: Randall K.Nichols, Panos C.Lekkas, TMH
6. Computer Security: Dieter Gollman, 2nd Edition, Wiley India
7. Computer Evidence: Collection & Preservation, Christopher L.T.Brown, Firewall Media

M. TECH. CYBER FORENSICS AND INFORMATION SECURITY-R13 Regulations

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech (CF&IS) **I Year – II Sem.**

CYBER FORENSICS LAB

The following exercises have to be performed using various software tools/utilities mentioned

Software Tools:

CyberCheck 4.0 - Academic Version

CyberCheckSuite

MobileCheck

Network Session Analyser

Win-LiFT

TrueImager

TrueTraveller

PhotoExaminer Ver 1.1

CDRAnalyzer

Forensics Exercises:

I) 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

II) 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

III) Device Forensics

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

IV) Hardware Forensics

References:

3. http://www.cyberforensics.in/default.aspx