COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

M.TECH. INFORMATION SECURITY

Course of Study & Scheme of Examination
2016-17

Maulana Azad National Institute of Technology,
Bhopal

SCHEME
M.Tech (Information Security)

First Semester

Course number	Subject	Schemes of Studies Periods per week			Credits
		L	T	P	
IS511	Mathematical foundations of Information Security	3	-	-	3
IS 512	Computer and network security	3	-	-	3
IS 513	Cyber crime and information warfare	3	-	-	3
IS 531 – IS 539	Elective 1	3	-	-	3
IS 531 – IS 539	Elective 2	3	-	-	3
IS 551- IS 554	Open Elective 1	3	-	-	3
IS 514	Laboratory 1 (Network & Cyber security Lab)	-	-	2	1
IS515	Laboratory 2 (Based on Elective)			2	1
IS516	Seminar 1	-		4	2
					Total credit
22					

Second Semester

Course number	Subject	Schemes of Studies Periods per week			Credits
		L	T	P	
IS 521	Cryptography	3	-	-	3
IS 522	Database security and access control	3	-	-	3
IS 523	Digital forensics	3	-	-	3
IS 541- IS 548	Elective 3	3	-	-	3
IS 541- IS 548	Elective 4	3	-	-	3
IS 556- IS 560	Open Elective 2	3	-	-	3
IS 524	Laboratory 3 (Data base security and Digital Forensics)	-	-	2	1
IS 525	Laboratory 4 (Based on Elective)			2	1
IS 516	Seminar 2	-	-	4-	2
					Total credit
22					

Departmental Elective

Course Number Elective – 1/2 Sem – I	Elective 1 & 2	Course Number Elective – 3/4 Sem – II	Elective 3 & 4
IS 531	Data Mining And Warehousing	IS 541	Secure software engineering
IS 532	Advanced data structures	IS 542	Graph theory and network algorithms
IS 533	Advanced Computer Networks	IS 543	Simulation and Modelling
IS 534	Operating System Design	IS 544	Security threats and modelling
IS 535	Advanced Computer Architecture	IS 545	Malware analysis and reverse engineering
IS 536	Wireless Network	IS 546	Web search and information retrieval
IS 537	Stochastic Process & Query Theory	IS 547	Secure cloud computing
IS 538	TCP/IP Networking	IS 548	Embedded system
IS 539	Steganography and Digital Watermarking	HUM XXX	Professional communication

Open Elective

Course number Open Elective-1 Sem-I	Open Elective 1	Course number OpenElective-2 Sem-II	Open Elective 2
IS 551	Distributed Computing	IS556	CAD OF Digital System
IS 552	Information Theory and Coding	IS557	Digital Image Processing
IS 553	Optimization Techniques	IS558	Technical Foundation for E- Commerce
IS 554	Biometrics	IS559	Cloud Computing
		IS-560	Statistical Methods

Third Semester

Course No.	Subject	Scheme of Studies Periods Per Week			No. of Duration of Theory Paper		Credits			Total
		L	T	P	No.	HR	L.	Tut.	Prac.	
	Dissertation I								23	23
TOTAL									23	23

Fourth Semester

Course No.	Subject	Scheme of Studies Periods Per Week			No. of Duration of Theory Paper		Credits			Total
		L	T	P	No.	HR	L.	Tut.	Prac.	
	Dissertation II								23	23
TOTAL									23	23
GRAND TOTAL I TO IV SEMESTER										90

SYLLABUS

IS511 MATHEMATICAL FOUNDATION OF INFORMATION SECURITY

Topics in elementary number theory: O and Ω notations – time estimates for doing arithmetic divisibility and the Euclidean algorithm – Congruence's: Definitions and properties – linear congruence's, residue classes, Euler's phi function – Fermat's Little Theorem – Chinese Remainder Theorem – Applications to factoring – finite fields – quadratic residues and reciprocity: Quadratic residues – Legendre symbol – Jacobi symbol.

Primality and Factoring: Pseudo primes – the rho (γ) method – Format factorization and factor bases – the continued fraction method – the quadratic seieve method.

Number Theory and Algebraic Geometry: Elliptic curves – basic facts – elliptic curve cryptosystems – elliptic

Mathematical logic: validity, soundness, completeness, compactness, Skolemization and Herbrand domain, Axiomatic theory

References:

1.Neal Koblitz, "A Course in Number Theory and Cryptography", 2nd Edition, Springer, 2002.

2. Johannes A. Buchman, "Introduction to Cryptography", 2nd Edition, Springer, 2004.

3. Serge Vaudenay, "Classical Introduction to Cryptography – Applications for Communication Security", Springer, 2006.

4. Victor Shoup, "A Computational Introduction to Number Theory and Algebra", Cambridge University Press, 2005.

5. A. Manezes, P. Van Oorschot and S. Vanstone, "Hand Book of Applied Cryptography", CRC Press, 1996.

6. S.C. Coutinho, "The Mathematics of Ciphers – Number Theory and RSA Cryptography",A.K. Peters, Natick, Massachusetts, 1998.

IS512 COMPUTER AND NETWORK SECURITY

Introduction to computer and network security. Basic concepts, threat models, common security goals, Cryptography and cryptographic protocols, including encryption, authentication, message authentication codes, hash functions, one1way functions, public1ke y cryptography, secure channels, zero knowledge in practice, models and methods for security protocol analysis. Malicious code analysis and defense. Viruses, Worms, spyware, rootkits, botnets, etc. and defenses against them, Detecting Attackers. Software security. Secure software engineering, defensive programming, buffer overruns and other implementation flaws. Language1based security: analysis of code for security errors, safe languages, and sandboxing techniques. Operating system security. Memory protection, access control, authorization, authenticating users, enforcement of security, security evaluation, trusted devices, digital rights management. Network security. Network based attacks, Kerberos,X.509, firewalls, intrusion detection systems, DoS attacks and defense. Case studies: DNS, IPSec. Web security. Securing Internet Communication, XSS attacks and defenses, etc. Advanced topics. Security monitoring, surreptitious communication, data remanence, trusted devices, privacy and security of

low1powered devices (RFID) electronic voting, quantum cryptography, penetration analysis, digital rights management and copy protection, security and the law.

References:

1.William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall, New Jersey.

2.Computer Security: Dieter Gollman, 2nd Edition, Wiley India

IS 513 CYBER CRIME AND INFORMATION WARFARE

Introduction of cyber crime, challenges of cyber crime, categorizing cyber crime, cyber terrorism, virtual crimes, perception of cyber criminals: hackers, insurgents and extremist groups, Interception of data, surveillance and protection, criminal copy right infringement, cyber stalking. Hiding crimes in cyberspace and methods of concealment. Anonymity and markets, privacy and security at risk in the global information society. Privacy in cyber space, web defacements and semantic attacks, DNS attacks, code injection attacks.

Risk management- Importance, Process overview, asset identification, threat identification and assessment, the risk assessment Effective and qualitative Risk analysis, value analysis, Facilitated Risk Analysis Process (FRAP)

Information Warfare concept, information as an intelligence weapon, attacks and retaliation, attack and defense. An I-War risk analysis model, implication of I-WAR for information managers, Perceptual Intelligence and I-WAR, Handling Cyber Terrorism and information warfare, Jurisdiction.

References:

1. Principles of Cyber crime, Jonathan Clough Cambridge University Press

2. Information Warfare : Corporate attack and defense in digital world, William Hutchinson,

Mathew Warren, Elsevier.

Electives

IS531 DATA MINING AND WAREHOUSING

Data Mining : Introduction, Relational Databases, Transactional databases, Advanced database Systems and Application, Data Mining Functionalities, Classification of Data Mining Systems, Major Issues in Data Mining.

Data Processing : Data Cleaning, Data Integration and Transformation, Data Reduction, Discretization and concept Hierarchy Generation.

Data Mining Primitives, Languages and System Architecture : Data Mining Primities, DMQL, Architectures of Data Mining Systems.

Concept Description: Data Generalization & Summarization – Based Characterization, Analytical Characterization, Mining class Comparisons, Mining Descriptive Statistical Measures in Large Databases.

Mining Association Rules in Large Databases : Association Rule Mining, Single – Dimensional Boolean Association Rules, Multilevel Association Rules from Transaction Databases, Multi Dimensional Association Rules from Relational Databases, From Association Mining to Correlation Analysis, Constraint – Based Association Mining.

Classification and Prediction : Classification & Prediction, Issues Regarding Classification & Prediction, Classification by decision Tree Induction, Bayesian Classification, Classification by Back propagation, Classification based on concepts & Association Rule, Other Classification, Prediction, Classification Accuracy.

Cluster Analysis : Types of Data in Cluster Analysis, Partitioning methods like KMedioid, CLARA, CLARANS, Hierarchical methods, DBSCAN, BIRCH, CURE, Grid – Based Methods, Model – Based Clustering Methods, categorical clustering algorithms , STIRR, ROCK,CACTUS ,Outlier Analysis.

Advance DM and application:

Web Mining. Web content mining, Web structure mining. Web usage Mining , User behavior analysis, Web Applications (including advertising, recommendation, and summarization)

Temporal DM: Temporal association rules, Sequence mining, GSP, SPADE, SPIRIT, and WUM algorithms, Episode Discovery, Event prediction, Time series analysis.

Spatial Mining ,Spatial Mining tasks. Spatial clustering, Spatial Trends.

Data Mining of Image and Video, Image and Video representation techniques, feature extraction, motion analysis, content based image and video retrieval, clustering and association paradigm, knowledge discovery.

Large-scale Data Mining, Similarity Search (including minwise hashing and locality sensitive hashing), Mining Data Streams, Mining Social Networks, relational Data Mining, Tree/Graph Mining Knowledge Graph mining , Privacy-preserving Data Mining, High-Dimensional Data Clustering .

Text mining and its application in Natural Language Processing, Named Entity Recognition, Wikification , semantic document representation Opinion Mining , Sentiment analysis , Machine learning ,

References:

Text Books :

1. Ian H Witten – Introduction of data mining
2. Jiawei Han & Micheline Kamber - Data Mining Concepts & Techniques
3. Publisher Harcout India. Private Linited.

Reference Books :

1. G.K. Gupta – Introduction to Data Mining with case Studies, PHI, New Delhi – 2006.
2. Berson & S.J. Smith – Data Warehousing Data Mining, COLAP, TMH, New Delhi – 2004
3. H.M. Dunham & S. Sridhar – Data Mining, Pearson Education, New Delhi, 2006.

IS532 ADVANCED DATA STRUCTURES

Review of algorithm analysis, Optimal Binary search trees, Balanced binary search trees, Binary heaps, Advanced heap structures, Binomial heaps, Fibonacci heaps. Amortized analysis, Splay trees. Dictionaries, Disjoint set structures. Data Structures for External Memory, External sorting, String matching. Introduction to Randomized Data structures and algorithms.

References:

1. Introduction to algorithms Cormen and Rivest.
2. Randomized algorithms R.Motwani and P. Raghavan

IS533 ADVANCED COMPUTER NETWORKS

Review of networking concepts: Network models, Addressing, Data rate limits, Bandwidth, throughput, Latency, Data link control, Multiple Access,Wired LAN, Wireless LAN, VLAN, SONET, ATM, QoS in ATM, ATM applications, IP addressing, forwarding, and routing, IPv4, IPv6, IP Security, Virtual Private Networks, Transport layer protocol, congestion control, Multimedia Networks: Voice/Video over IP, IP Telephony, Voice over ATM, AAL2, Network management, Optical Networks

References:

1. Jawin, “Networks Protocols Handbook”, Jawin Technologies Inc., 2005.
2. Bruce Potter and Bob Fleck, “802.11 Security”, O’Reilly Publications, 2002.
3. Lawrence Harte, “Introduction to WCDMA”, Althos Publishing, 2004.
4. Ralph Oppliger “SSL and TSL: Theory and Practice”, Arttech House, 2009.
5. Lawrence Harte, “Introduction to CDMA- Network services Technologies and Operations”, Althos Publishing, 2004.
5. Lawrence Harte, “Introduction to WIMAX”, Althos Publishing, 2005.

IS534 OPERATING SYSTEM DESIGN

Computer system and operating system overview, Operating system functions and design issues, Design approaches, Types of advanced operating systems, Process abstraction, Process management, system calls, Threads, Symmetric multiprocessing and microkernels. Scheduling: Uniprocessor, Multiprocessor and Real time systems, concurrency, classical problems, mechanisms for synchronization: semaphores, monitors, Process deadlock and deadlock handling strategies, Memory management, virtual memory concept, virtual machines, I/O management, File and disk management, Operating system security.

Distributed Operating system: architecture, Design issues, Distributed mutual exclusion, distributed deadlock detection, shared memory, Distributed scheduling. Multiprocessor operating systems: architecture, operating system design issues, threads, process synchronization, process scheduling, memory management, reliability and fault tolerance.

References:

1. Advanced concept in operating system M. Singhal, N.G Shivratri.
2. Operating system internal and design princilples William stallings.

IS535 ARCHITECTURE OF LARGE SYSTEMS

Pipeline processor principles and design, Instruction set architecture; Memory addressing; Instruction composition; Instruction-level parallelism. Hazards: dynamic scheduling, branch prediction; Memory hierarchy; Processor case studies; Multiprocessor introduction: Shared-

memory architectures and their synchronisation and consistency issues, Advanced multi-core topics; Transactional Memory; Interconnection networks.

References:

1. Computer Architecture: A Quantitative Approach, J. L. Hennessy and D. A. Patterson. ,
2. Parallel Computer Architecture: A Hardware/Software Approach
3. David Culler, J.P. Singh and Anoop Gupta,
4. Advanced Computer Architecture: Parallelism, Scalability, Programmability Kai Hwang.

IS536 WIRELESS NETWORK

Introduction to wireless communication, and future trends, Wireless Generations and Standards, Wireless Physical Layer Concepts, fundamentals of antennas, Cellular Concept and Cellular System Fundamentals.Spread Spectrum Modulation Techniques, Coding and Error Control, Multiple Access Technique for Wireless Communications, OFDM.Wireless LAN Technologies, Wireless IEEE Standards, Mobile Network Layer (Mobile IP). Mobile Transport Layer (Mobile TCP), Mobile Data network (GPRS), WAP Model and architecture, Introduction to Ad hoc networks, Sensor networks, Bluetooth networks and Wireless Mesh networks.

References:

1. Wireless Communications and Networking William Stallings
2. Wireless communication: Principles and Practice, T. S. Rappaport,
3. Mobile Communications Schiller
4. Principles of Wireless Networks: A Unified Approach Pahalvan, K. and Krishnamurthy

IS537 STOCHASTIC PROCESS & QUERY THEORY

The objective of this course is to provide the students basic knowledge about probability and stochastic process with applications.

The course will include permutation and combinations, probability theory, Random variable, probability mass function, Binomial, poisson, exponential, normal, uniform distributions ,stochastic process and Markov chains.

Introduction of basic Queuing Theory, Markov Chains and Markov Processes, Birth-Death Processes, Simple Queuing Models (M/M/-/- Queues), Queues with Batch Arrivals, M/G/1 Queue with Residual Life and Imbedded Markov Chain Approach, Queues with Vacations, Bulk Arrivals and Priorities, Discrete Time Queues, Delay Analysis of Queues. Fundamental of Queuing Networks, Open and Closed Queuing Networks, Open Networks of M/M/m type queues. Approximate Models for Open and Closed Queuing Networks, Queuing System Applications, Simulation Modelling of Queuing Systems.

References:

1. Donald Gross, James M. Thompson, John F. Shortle and Carl W. Harris, Fundamentalsof Queueing Thoery, Wiley 2008.
2. Sanjay K. Bose, An Introduction to Queueing Systems, Springer 2002.

3. T.G. Robertazzi, Computer Networks and Systems - Queueing Theory and Peformance Evaluation, Springer 2000.
4. L. Kleinrock, Queueing Systems Volume 1 : Theory, Wiley 1975.

IS538 TCP/IP

Layered communication architecture: layers, services, protocols, layer entities, service access points, protocol functions. Advanced Routing algorithms Advanced Network Congestion Control algorithms Quality of service Real Time Transport Protocol Internetworking Performance Issues Overview on VPN networks Overview on Wireless Networks and Mobile Networks: LAN, PAN, Sensor Networks, Ad_hoc Networks Mobile IP, Mobile TCP, IP Security.

References:

1- William Stallings, Wireless Communications & Networks, 2nd edition, Prentice-Hall Pearson, 2005
2- Jochen Schiller, Mobile Communication, (Latest edition), Addison Wesley
3- G. Wright and W. Stevens, TCP/IP Illustrated, Volume 2, Addison-Wesley, 1996.

IS539 STEGANOGRAPHY AND DIGITAL WATERMARKING

UNIT I

Introduction to Information hiding – Brief history and applications of information hiding – Principles of Steganography – Frameworks for secret communication – Security of Steganography systems –Information hiding in noisy data – Adaptive versus non adaptive algorithms – Laplace filtering – Using cover models – Active and malicious attackers – Information hiding in written text – Examples of invisible communications.

UNIT II

Survey of steganographic techniques – Substitution system and bitplane tools – Transform domain techniques – Spread spectrum and information hiding – Statistical Steganography - Distortion and code generation techniques – Automated generation of English text.

UNIT III

Steganalysis – Detecting hidden information – Extracting hidden information - Disabling hidden information – Watermarking techniques – History – Basic Principles – applications – Requirements of algorithmic design issues – Evaluation and benchmarking of watermarking system.

UNIT IV

Survey of current watermarking techniques – Cryptographic and psycho visual aspects – Choice of a workspace – Formatting the watermark bets - Merging the watermark and the cover – Optimization of the watermark receiver – Extension from still images to video – Robustness of copyright making systems.

UNIT V

Fingerprints – Examples – Classification – Research history – Schemes – Digital copyright and watermarking – Conflict of copyright laws on the internet.

References:

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, “Information hiding techniques for Steganography and Digital Watermarking”, ARTECH House Publishers, January 2004.

2. Jessica Fridrich, “Steganography in Digital Media: Principles, Algorithms, and Applications”, Cambridge university press, 2010.
3. Steganography, Abbas Cheddad, Vdm Verlag and Dr. Muller, “Digital Image” Aktienge sells chaft & Co. Kg, Dec 2009.
4. Ingemar Cox, Matthew Miller,Jeffrey Bloom,Jessica Fridrich and Ton Kalker, “Digital Watermarking And Steganography”, Morgan Kaufmann Publishers, Nov 2007.

IS551 DISTRIBUTED COMPUTING

Introduction to Distributed System: Goals, Hardware concepts, Software concepts, and Client-Server model. Example of distributed systems. Communication: Layered protocols, Remote procedures call, Remote object invocation, Message-oriented communication, Stream-oriented communication. Inter process communication in UNIX/LINUX. Processes: Threads, Clients, Servers, Code Migration, Software agent.Naming: Naming entities, locating mobile entities, removing un-referenced entities. Synchronization: Clock synchronization, Logical clocks, Global state, Election algorithms, Mutual exclusion, Distributed transactions. Consistency and Replication: Introduction, Data centric consistency models, Client centric consistency models, Distribution protocols, Consistency protocols. Fault Tolerance: Introduction, Process resilience, Reliable client server communication, Reliable group communication. Distributed commit, Recovery. Security: Introduction, Secure channels, Access control, Security management. Distributed File System: Sun network file system, CODA files system, Google File System.

References:

1. Distributed Systems: Principles and Paradigms. A. Taunenbaum,
2. Distributed Systems: Concepts and Design G. Coulouris, J. Dollimore, and T. Kindberg,

IS552 INFORMATION THEORY AND CODING

Information and entropy information measures, Shannon’s concept of information. Channel coding, channel mutual information capacity (BW) , theorem for discrete memory less channel, information capacity theorem , error detecting and error correcting codes, Types of codes: block codes, hamming and Lee metrics, description of linear block codes , parity check codes ,cyclic code. Masking techniques.

Compression : loss less and lossy, Huffman codes, LZW algorithm, Binary image compression schemes, run length encoding, CCITT group 3 1-D compression, CCITT group 3 2D compression, CCITT group 4 2D Compression. Convolutional codes, sequential decoding. Video image compression: CITT H 261 Video coding algorithm, audio (speech) compression. Cryptography and cipher.

References:

1. Information Theory, Coding and Crptography R Bose.
2. Multimedia system Design Prabhat K Andleigh and Kiran Thakrar
3. Multimedia Communications Fred Halsall.

IS553 OPTIMIZATION TECHNIQUES

Introduction: Engineering application of Optimization, Formulation of design problems as mathematical programming problems, General Structure of Optimization Algorithms ,Constraints, The Feasible Region, Branches of Mathematical Programming ,Gradient Information, The Taylor Series, Types of Extrema, Necessary and Sufficient Conditions for Local Minima and Maxima, Classification of Stationary Points , Convex and Concave Functions, Optimization of Convex Functions, General Properties of Algorithms ,An Algorithm as a Point-to-Point Mapping,An Algorithm as a Point-to-Set Mapping Closed Algorithms , Descent Functions, Global Convergence, Rates of Convergence.

Unconstrained Optimization: One dimensional optimization techniques: Dichotomous Search, Fibonacci Search ,Golden-Section Search, Quadratic Interpolation Method ,Cubic Interpolation, The Algorithm of Davies, Swann, and Campey, Inexact Line Searches , Multidimensional Gradient Methods ,Steepest- Descent Method, Newton Method Gauss-Newton Method, Conjugate-Direction Methods: Conjugate Directions, Basic Conjugate-Directions Method, Conjugate-Gradient Method, Minimization of Nonquadratic Functions, Fletcher-Reeves Method, Powell's Method, Partan Method. Quasi-Newton Methods: The Basic Quasi-Newton Approach, Generation of Matrix Sk ,Rank-One Method, Davidon-Fletcher- Powell Method, Broyden-Fletcher-Goldfarb-Shanno Method, Hoshino Method, The Broyden Family, The Huang Family, Practical Quasi-Newton Algorithm, Applications of Unconstrained Optimization, Nonlinear Least Squares Problem and Algorithms.

Linear Programming: Graphical method, Simplex method, Duality in linear programming (LP), Sensitivity analysis, Interior-Point Methods, Primal-Dual Solutions and Central Path, Primal Affine-Scaling Method, Primal Newton Barrier Method, Primal-Dual Interior-Point Methods.

Nonlinear Constrained Optimization: Constrained Optimization, Constraints, Classification of Constrained Optimization Problems, Simple Transformation Methods ,Lagrange Multipliers , First-Order Necessary Conditions, Second-Order Conditions, Convexity , Duality Quadratic And Convex Programming: Convex QP Problems with Equality Constraints, Active-Set Methods for Strictly Convex QP Problems , Interior-Point Methods for Convex QP Problems, Cutting-Plane Methods for CP Problems, Ellipsoid Methods.

Minimax Methods: Minimax Algorithms, Improved Minimax Algorithms,

References:

1. Practical Optimization Algorithms And Engineering Applications, Andreas Antoniou
2. An Introduction To Optimization Edwin K. P. Chong & Stanislaw h. Zak,

IS554 BIO METRICS

Introduction: Definitions, biometric modalities, benefits of biometric versus traditional authenticated methods. Key biometric terms and processes. Authenticationtechnologies: storage tokens, dynamic tokens, token usability. Design of a Biometric System: Building blocks, Modes of operation Biometric technologies: Passive & active biometric. user acceptance Ease of use ,technology cost, depoyability,Invasivness of the technology , maturity of the technology. Fingerprint verification: Minutiae Based Fingerprint Matching, Non-minutiae Based Representations,finger print component, algorithms for interpretion.Fingerprint Enhancement, and Fingerprint Classification. Face Recognition:- Introduction, Authentication vs. Identification,

Challenges in Face recognition, Algorithms for face recognitions. Iris Recognition: Introduction, devices for capturing Iris, Iris representation schemes, Iris recognition algorithms. Hand Geometry Recognition , Gait Recognition, The Ear as a Biometric, Voice Biometrics, A Palmprint Authentication System. On-Line Signature Verification.3D Face Recognition. Automatic Forensic Dental Identification, DNA. Introduction to Multibiometrics.- Multispectral Face Recognition.- Multibiometrics Using Face and Ear.- Incorporating Ancillary Information in Multibiometric Systems. Multimodal Biometrics: Limitations of unimodal systems, multibiometric scenarios, levels of fusion, system design, score fusion techniques, score normalization, user-specific parameters, and soft biometrics. The Law and the Use of Biometrics.- Biometric System Security.- Spoof Detection Schemes.- Linkages between Biometrics and Forensic Science.- Biometrics in Government Sector.- Biometrics in the Commercial Sector.- Biometric Standards.- Biometrics Databases Case Study Presentations: Biometrics in Banking Industry, Biometrics in Computerized, Patient Records, Biometrics in Credit Cards, Biometrics in Mass Disaster Victim, Identification Forensic Odontology.

References:

1. Biometrics for network security PaulReid,
2. Handbook of Fingerprint Recognition D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar,
3. BIOMETRICS: Personal Identification in Networked Society A. K. Jain, R. Bolle, S. Pankanti,
4. Biometric Systems: Technology, Design and Performance Evaluation,
J. Wayman, A.K. Jain, D. Maltoni, and D. Maio

Semester II

IS521 CRYPTOGRAPHY

Simple Cryptosystems: Enciphering Matrices – Encryption Schemes – Symmetric and Asymmetric Cryptosystems – Cryptanalysis – Block ciphers –Use of Block Ciphers – Multiple Encryption – Stream Ciphers –Affine cipher – Vigenere, Hill, and Permutation Cipher – Secure Cryptosystem.

Public Key Cryptosystems: The idea of public key cryptography – The Diffie–Hellman Key Agreement Protocol - RSA Cryptosystem – Bit security of RSA – ElGamal Encryption - Discrete Logarithm – Knapsack problem – Zero-Knowledge Protocols – From Cryptography to Communication Security - Oblivious Transfer.

Symmetric Techniques: Stream Cipher: A5, RC4

Asymmetric Techniques: Cryptography in Embedded Hardware

Different type of attack: CMA, CPA, CCA.

References:

1. Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C” John Wiley & Sons, Inc, 2nd Edition, 1996.
2. Wenbo Mao, “Modern Cryptography Theory and Practice”, Pearson Education, 2004
3. Atul Kahate, “Cryptography and Network Security”, Tata McGrew Hill, 2003

IS522 DATABASE SECURITY AND ACCESS CONTROL

Introduction to Access Control, Purpose and fundamentals of access control, brief history, Policies of Access Control, Models of Access Control, and Mechanisms, Discretionary Access Control(DAC), Non- Discretionary Access Control , Mandatory Access Control (MAC). Capabilities and Limitations of Access Control Mechanisms: Access Control List (ACL) and Limitations, Capability List and Limitations, Role-Based Access Control (RBAC) and Limitations, Core RBAC, Hierarchical RBAC, Statically Constrained RBAC, Dynamically Constrained RBAC, Limitations of RBAC. Comparing RBAC to DAC and MAC Access control policy, Biba'sintrigity model, Clark-Wilson model, Domain type enforcement model , mapping the enterprise view to the system view, Role hierarchies- inheritance schemes, hierarchy structures and inheritance forms, using SoD in real system, Temporal Constraints in RBAC, MAC AND DAC. Integrating RBAC with enterprise IT infrastructures: RBAC for WFMSs, RBAC for UNIX and JAVA environments Case study: Multiline Insurance Company. Smart Card based Information Security, Smart card operating system-fundamentals, design and implantation principles, memory organization, smart card files, file management, atomic operation, smart card data transmission ATR,PPS Security techniques- user identification , smart card security, quality assurance and testing , smart card life cycle-5 phases, smart card terminals.

References:

1. Role Based Access Control David F. Ferraiolo , D. Richard Kuhn , Ramaswamy Chandramouli

IS523 DIGITAL FORENSICS

Introduction to legal issues, context, and digital forensics. Digital Evidence - Sources of digital evidence, evidence gathering methods: - Imaging, Forensics copy, selection and extraction, auditing logging, evidence correlation and preservation. Evidence analysis techniques: keyword searches, timelines, hidden data. Computer Forensics and investigations as a profession, understanding computer investigations, Data Acquisition, processing Crime and Incident Scenes Digital Forensics Models. Working with Windows and DOS Systems, Current Computer Forensics Tools, Macintosh and Linux Boot Processes and Disk Structures, Computer Forensics Analysis and Validation Recovering Graphics Files, Network Forensics, E-Mail Investigations, Cell Phone and Mobile Devices

References:

1. Computer Forensics and Investigations Nelson Phillips, Enfinger,Steuart
2. Computer Evidence Collection and Preservation Christopher L.T.Brown, Firewall
3. Media Software Forensics Robert M. Slade.

Elective

IS 541 SECURE SOFTWARE ENGINEERING

UNITI

Problem, Process, and Product - Problems of software practitioners – approach through software

reliability engineering- experience with SRE – SRE process – defining the product – Testing acquired software – reliability concepts- software and hardware reliability. Implementing

Operational Profiles - Developing, identifying, crating, reviewing the operation – concurrence rate – occurrence probabilities- applying operation profiles.

UNIT II

Engineering “Just Right” Reliability - Defining “failure” for the product - Choosing a common measure for all associated systems. - Setting system failure intensity objectives –Determining user needs for reliability and availability., overall reliability and availability objectives, common failure intensity objective., developed software failure intensity objectives. – Engineering software reliability strategies. Preparing for Test - Preparing test cases. - Planning number of new test cases for current release. -Allocating new test cases. - Distributing new test cases among new operations - Detailing test cases. - Preparing test procedures.

UNIT III

Executing Test - Planning and allocating test time for the current release. - Invoking test identifying identifying failures - Analyzing test output for deviations. – Determining which deviations are failures. Establishing when failures occurred. Guiding Test - Tracking reliability growth - Estimating failure intensity. - Using failure intensity patterns to guide test – Certifying reliability. Deploying SRE - Core material - Persuading your boss, your coworkers, and stakeholders. - Executing the deployment - Using a consultant.

UNIT IV

Using UML for Security - UM L diagrams for security requirement -security business processphysical security - security critical interaction - security state. Analyzing Model - Notation - formal semantics - security analysis - important security opportunities. Model based security engineering with UML - UML sec profile- Design principles for secure systems – Applying security patterns.

UNIT V

Applications - Secure channel - Developing Secure Java program- more case studies. Tool support for UML Sec - Extending UML CASE TOOLS with analysis tools - Automated tools for UML SEC. Formal Foundations - UML machines - Rely guarantee specifications- reasoning about security properties.

References:

1. John Musa D, “Software Reliability Engineering”, 2nd Edition, Tata McGraw-Hill, 2005(Units I, II and III).
2. Jan Jürjens, “Secure Systems Development with UML”, Springer; 2004 (Unit IV and V)

IS542 GRAPH THEORY AND NETWORK ALGORITHMS

Mathematical Background: Convex Optimization, Stability of Dynamical Systems and Discrete-time Markov Chains, Utility Maximization and Resource Allocation in the Internet, Statistical Multiplexing and queues, delay and packet loss analysis in queues. Graph Theory: graphs and digraphs, Spanning Trees, Connectivity and Flow, Planar Graphs, Graph Coloring, factorizations, eulerian and hamiltonian graphs, Minimum Connector Problem, Marriage Problem, Assignment Problem, Network Flow Problem , Committee Scheduling Problem, Four Color Problem, Traveling Salesman Problem. Scheduling in High-Speed Switches: Switch Architectures and Crossbar Switches, Head-of-Line (HOL) Blocking and Virtual Output Queues, Capacity Region and Max Weight Scheduling. Scheduling in Wireless Networks: Scheduling in

Wireless Networks, Channel-Aware Scheduling in Cellular Networks, The MaxWeight Algorithm for the Cellular Downlink , MaxWeight Scheduling Ad Hoc P2P Wireless Networks. Network Flow Algorithms : Introduction, Distance Network algorithms, Computational analysis and Optimality conditions of Distance Network Algorithms, Maximum flow algorithms, Minimum Cost Flow algorithms, Cycle canceling and Out of-kilter algorithm, Network Utility Maximization: Utility Maximization for Joint Congestion Control, Routing and Scheduling , Stability and Convergence, Ad Hoc P2P Wireless Networks, Internet versus Wireless Formulations. Distributed Algorithms for Network Communications: Data distribution algorithms, Request-Reply algorithms, Search and traversal algorithms, breaking symmetry and election algorithms, Topology discovery. Routing, Building and aintaining trees, Synchronization. Fault tolerance and recovery, Complexity of distributed algorithms.

References:

1. R. Balakrishnan, K. Ranganathan “A Textbook of Graph Theory”- 2012
2. Alen gibbons “Algorithmic Graph Theory”.

IS543 SIMULATION AND MODELLING

Introduction: Systems, modelling, general systems theory, Concept of simulation, Simulation as a decision making tool, types of simulation. Random Numbers and Queuing Theory: Pseudo random numbers, methods of generating random variables, discrete and continuous distributions, testing of random numbers, Concepts of Queuing theory. Design of Simulation Experiments :Problem formulation, data collection and reduction, time flow mechanism, key variables, logic flow chart, starting condition, run size, experimental design consideration, output analysis and interpretation validation. Simulation Languages: Comparison and selection of simulation languages, study of these simulation language.

Case studies: Development of simulation models using simulation language studied for systems like queuing systems, Production systems, Inventory systems, maintenance and replacement systems and Investment analysis.

References:

1. System Simulation Geoffrey Gordon,
2. System Simulation with Digital Computer Narsingh Deo

IS544 SECURITY THREATS AND MODELLING

UNIT I

Introduction: Security threats, its sources, Target Assets and vulnerabilities, Consequences of threats, Active/ Passive Threats, Web-threats, Network Threats, E-mail threats, Sabotage- Internal treats- Environmental threats - Threats to Server security, Insider threats,

Cyber crimes, hackers and Intruders

UNIT II

Attack Tree, Attack Graphs, Types of Attack Scenarios and Detection Approaches, Threat exploitation and analysis: Session Hijacking – Phishing – DNS Pharming – Tab-nabbing – Clickjacking – XSS – SQL – Command Injection – IP Spoofing, Email-Spoofing, Information Hiding (Stenography), Buffer Overflow

Virology- Worms, Virus, Spam’s, Ad ware, Spy ware, Trojans, Backdoors, Bots, Malware

UNIT III

Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation – Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools - Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning.

Footprinting- Scanning-Enumeration - basic banner grabbing, Enumerating Common Network services.

UNIT IV

Security models – Access Control Matrix Model, Take-Grant Protection Model

Secure Web Engineering Privacy - Privacy Issues, Privacy in social networks, Privacy Models, Privacy preserving Data Mining techniques, Privacy enhancing technology, Web Privacy

Security Policies – Security Policies and Procedures, Writing Security Policies, Sample Security Policies, Types: Integrity policies, Confidentiality policies, WWW Policies, Same Origin Policy, E-mail Security Policies, etc.

Security certification – Security monitoring and auditing, Forensics Investigator,

UNIT V

Security protocols – Transport layer protocols – SSL – Electronic mail security – PEM and S/MIME security protocol – Pretty Good Privacy – Web Security - Firewalls design principles – Trusted systems – Electronic payment protocols. Intrusion detection – password management – Viruses and related Threats – Virus Counter measures, Virtual Private Networks.

Application Level Security: HTTP Vs HTTPS, SSL, IPV6 Security Requirements Specifications: Antivirus, Firewalls, IDS, IPS, Log Files, Honey Pots, Honey Net Secure Software Engineering: Need for secure systems, Software security issues, Secure Software Life Cycle, Secure Programming Vs Defensive Programming, Proactive security development process, Secure design principles and Patterns, Insecure Code Samples, Code Reviews and Static Analysis, Security Testing, Creating a Software Security Programs

References:

1. Joseph M Kizza, “Computer Network Security”, Springer Verlag, 2005
2. Swiderski, Frank and Syndex, “Threat Modeling”, Microsoft Press, 2004.
3. William Stallings and Lawrie Brown, “Computer Security: Principles and Practice”, Prentice Hall, 2008.
4. Thomas Calabres and Tom Calabrese, “Information Security Intelligence: Cryptographic Principles & Application”, Thomson Delmar Learning, 2004.
5. Chapter 9: Legal, Privacy, and Ethical Issues in Computer Security;

IS 545 MALWARE ANALYSIS AND REVERSE ENGINEERING

Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) 3.1 Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAV Signatures, Creating Custom Clam A V Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser’s REMnux , SANS SIFT , Sandbox Setup and Configuration New Course Form , Routing TCP/IP Connections, Capturing and Analyzing

Network Traffic, Internet simulation using INetSim , Using Deep Freeze to Preserve Physical Systems , Using FOG for Cloning and Imaging Disks , Using MySQL Database to Automate FOG Tasks , Introduction to Python , Introduction to x86 Intel assembly language , Scanners: VirusTotal, Jotti, and NoVirusThanks , Analyzers: ThreatExpert, CWSandbox, Anubis, Joebox , Dynamic Analysis Tools: Process Monitor, Regshot, HandleDiff , Analysis Automation Tools: VirtualBox, VMWare, Python , Other Analysis Tools

Malware Forensics: Using TSK for Network and Host Discoveries , Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD , Registry Forensics with RegRipper Plug-ins : , Bypassing Poison Ivy's Locked Files , Bypassing Conficker's File System ACL Restrictions , Detecting Rogue PKI Certificates

Malware and Kernel Debugging:Opening and Attaching to Processes ,Configuration of JIT Debugger for Shellcode Analysis ,Controlling Program Execution ,Setting and Catching Breakpoints ,Debugging with Python Scripts and PyCommands ,DLL Export Enumeration, Execution, and Debugging ,Debugging a VMware Workstation Guest (on Windows) ,Debugging a Parallels Guest (on Mac OS X) ,Introduction to WinDbg Commands and Controls , Detecting Rootkits with WinDbg Scripts , Kernel Debugging with IDA Pro

Memory Forensics and Volatility : Memory Dumping with MoonSols Windows Memory Toolkit , Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps , Code Injection and Extraction , Detecting and Capturing Suspicious Loaded DLLs , Finding Artifacts in Process Memory , Identifying Injected Code with Malfind and YARA .

Researching and Mapping Source Domains/IPs : Using WHOIS to Research Domains , DNS Hostname Resolution , Querying Passive DNS , Checking DNS Records , Reverse IP Search New Course Form , Creating Static Maps , Creating Interactive Maps

References:

1. Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher william Pollock.

IS546 WEB SEARCH AND INFORMATION RETRIEVAL

Information retrieval model, Searching the web, Document Representation, Query languages and query operation, Indexing and searching, Scoring and ranking feature vectors, domain specific search, Information retrieval evaluation, Probabilistic information retrieval, Text classification and Naive Bayes, clustering, Matrix decompositions and latent semantic.

References:

1. Manning, C., Raghavan, P., and Schutze, H. (2007), An introduction to Information Retrieval, Cambridge University Press.
2. Chakrabarti, S. (2002). Mining the web: Mining the Web: Discovering knowledge from hypertext data. Morgan-kaufman.

IS547 SECURE CLOUD COMPUTING

Cloud computing fundamental: Definition of Cloud computing, Cloud computing models, cloud computing architecture, essential characteristic, Virtualization basic, server consolidation, automatic computing, horizontal scaling, high performance computing. Cloud security: cloud

security fundamental, cloud information security objective, cloud security services, End-user access to the cloud computing, identity management and access control, cloud computing risk, cloud computing security challenges, security analysis, real time risk management in cloud computing, trusted cloud computing, hardware based security to ensure data privacy, virtualization system-specific attacks, guest hopping, attacks on the VM (delete the VM, attack on the control of the VM, virtual thread, VM security recommendation, VM migration attack, hyperjacking. Legal and compliance issues responsibility, ownership of data, right to penetration test, local law where data is held, examination of modern Security Standards (eg PCIDSS), how standards deal with cloud services and virtualization, compliance for the cloud provider vs. compliance for the customer, VM specific security technique.

References:

1. Anothony T Velte, Toby J Velte, Robert Elsenpeter, Cloud Computing: A Practical Approach, MGH, 2010.
2. Gautam Shroff, Enterprise Cloud Computing, Cambridge, 2010.
3. Ronald Krutz and Russell Dean Vines, Cloud Security, 1st Edition, Wiley, 2010.
4. Cloud Security: A Comprehensive Guide to Secure Cloud Computing By Ronald L. Krutz, Russell Dean Vines, 2011.

IS 548 EMBEDDED SYSTEM

Trust models for secure embedded hardware and software, Isolation techniques for secure embedded hardware, hyperaware, and software, System architectures for secure embedded systems, Metrics for secure design of embedded hardware and software, Security concerns for medical and other applications of embedded systems, Support for intellectual property protection and anti-counterfeiting, Specialized components for authentication, key storage and key generation, Support for secure debugging and troubleshooting, Implementation attacks and countermeasures, Design tools for secure embedded hardware and software, Hardware/software code sign for secure embedded systems, Specialized hardware support for security protocols.

References:

1. Raj Kumal “Embedded Systems 2E” Tata McGraw-Hill Education

Open Elective

IS556 CAD OF DIGITAL SYSTEMS

Basic Mathematical Concepts, Introduction to design methodologies, Design automation tools, Algorithmic graph theory and computational complexities, Computational Approaches and methods for combinatorial optimization, Design of digital hardware and HDLs, Introduction to logic circuits, Implementation technologies, Verilog Programming concepts, Gate level modelling , Data flow modelling , Behavioural modelling, Combinational circuit design, Flip-flops, registers, counters and processor, Sequential circuits design, Tasks and functions, Timing and Delays ,Data Structure in VLSI design , Layout, placement and partition, floor planning,

routing, Logic Synthesis, Model Optimization, Verification and Testing , Simple Microprocessor Design .

References:

1. Algorithm for VLSI Design automation, Sabih H. Gerez
2. Fundamental of Digital Logic with Verilog Design Brown & Vranesic,
3. Digital VLSI Design with Verilog, John Williams.

IS557 DIGITAL IMAGE PROCESSING

Introduction to Image Processing Systems, Digital Image Fundamentals:- Image model, Relationship between Pixels, Imaging geometry, Camera model. Image Sensing and Acquisition. Sampling and quantization. Image Enhancement and in spatial Domain: Point processing, Neighbourhood Processing, High pass filtering , High boost filtering, zooming. Image Enhancement based on Histogram medelling. Image Enhacement in frequency domain: 1D& 2D Fourier transform, Low pass frequency domain filter, High pass frequency domain filters, Homomorphics filtering. Image Segmentation:- Detection of discontinuation by point detection, line detection, edge detection. Edge linking and boundary detection:- Local analysis, global by graph, theoretic techniques. Thresh-holding. Morphology, Representation and description. Discrete image transform. Image Compression. Wavelet transformation.

References:

1. Digital Image Processing Gonzalez & Wood
2. Digital Image Processing A.K.Jain
3. Image Processing Dhananjay K.Techkedath

IS558 TECHNICAL FOUNDATION FOR E-COMMERCE

Introduction: Electronic commerce, technology and prospects, forces behind e-commerce, advantages and disadvantages, architectural framework, e-commerce strategy, e-commerce emerging issues and implementation issues, e-commerce law, government policies and agenda.

E-Commerce Infrastructure: Internet and Intranet based e-commerce- Issues, problems and prospects, Network Infrastructure, Network Access Equipments, Broadband telecommunication (ATM, ISDN, FRAME RELAY). Mobile Commerce: Introduction, Wireless Application Protocol, WAP technology, Mobile information device, mobile computing applications, security issues in m-commerce. Electronic Payment System: Overview, electronic payment mechanisms and protocols, SET protocol, payment gateway, certificate, digital tokens, smart card, credit card, magnetic strip card, electronic money, electronic contracts, micro-payments, e-checks, e-cash Credit/Debit card based EPS, e-commerce payments security, online banking. electronic data interchange and its applications. Internet Advertising. Models of Internet advertising, sponsoring contents, corporate website, weaknesses in Internet advertising, web auctions and trading mechanism. Securing Business on Network. Security policies, procedures and practices, site security, firewalls, securing web service, transaction security, cryptology, cryptological algorithms, public key algorithms, authentication protocols, digital Signatures, virtual private

network, security protocols for web commerce. Advanced Topics. Electronic commerce optimization algorithms, decision support systems for e-commerce, data mining for e-commerce, intelligent techniques for e-commerce.

References:

1. E- Commerce Strategies, Technology and ap lications (David) Tata McGrawHill.
2. E-Business Organizational and technical foundation (Michael P) Wiley Publication
3. John Benamati ,William S.Davis, E-Commerce Basics Technology Foundations and E-Business Applications, Prentice Hall

IS 559 CLOUD COMPUTING

Definition of Cloud computing (NIST), Cloud computing models, Secure data outsourcing, Secure computation outsourcing, Query on encrypted data; Proof of data possession / retrievability, Virtual machine security, Trusted computing technology and clouds, Cloud-centric regulatory compliance issues and mechanisms, Business and security risk models, Applications of secure cloud computing.

Reference:

1. Anothony T Velte, Toby J Velte, Robert Elsenpeter, Cloud Computing: A Practical Approach, MGH, 2010.
2. Gautam Shroff, Enterprise Cloud Computing, Cambridge, 2010.
3. Ronald Krutz and Russell Dean Vines, Cloud Security, 1st Edition, Wiley, 2010.

IS 560 STATISTICAL METHODS

Introduction to Statistics, Meaning of Statistics as a Science, Importance of Statistics. Scope of Statistics, Introduction to Data Analysis, Population and Sample, Types of characteristics , Types of data, Notion of a statistical population, Methods of sampling, Presentation of Data, Data Visualization, Measures of Central Tendency, Measures of Dispersion, Moments, Skewness and Kurtosis, Theoy testing ,Optimization, Hypothesis Testing, Bayesian Statistics,7 Subjective Probabilities, Heuristic analysis, Histograms:, Regression, Correlation, Error, Relational Databases, Cleaning Data:

References:

1. Goon Gupta and Das Gupta : Fundamentals of Statistics, Vol. 1, The World Press Pvt. Ltd., Kolkata.
2. Dawn Griffiths: Modern Head First Statistics, O Reilly Pubilcation
3. Snedecor and Cochran : Statistical Methods, Oxford and IBH Publishers
4. Mukhopadhyay, P. : Mathematical Statistics (1996), New Central Book Agency, Calcutta, Introduction to Mathematical Statistics, Ed. 4 (1989), MacMillan Publishing Co. New York.
5. Gupta and Kapoor : Fundamentals of Mathematical Statistics, Sultan Chand and Sons, New Delhi.
6. Neil Weiss : Introductory Statistics : Pearson Publishers.

7. Gupta and Kapoor : Fundamentals of Applied Statistics, Sultan Chand and Sons, New Delhi.
8. Amir D. Aczel and Jayael Soundarpandiyan, Complete Business Statistic: McGraw Hill Education (6th Edition).
9. B. L. Agarwal : Programmed Statistics, New Age International Publishers,New Delhi.
10. D. C. Montgomory : Introduction to Statistical Quality Control, Wiley, Eastern Publishers.
11. K. V. S. Sarma : Statistics Made Simple : Do it yourself on PC. Prentice, Hall of India Pvt. Ltd., New Delhi.

NETWORK AND CYBER SECURITY LABORATORY (LAB-I):

Cryptography- Secret-Key Encryption, Public-Key Encryption, One-time padding, MAC(Message Authentication Code), Digital Signatures, Diffie-Hellman Key Exchange.
Intrusion Detection System: Network enumeration through port scanning, SYN flooding
Threats and Vulnerabilities- Cross Site Scripting (XSS) & Buffer Overflow Attack, Code Injection Attacks: SQL Injection, PHP Injection, Command Injection
DNS Vulnerability Analysis- DNS Spoofing, DNS Cache Poisoning, DNS Pharming, DNS Cache Analysis, WHOIS Query to Research Domains
OS Attack – OS Finger printing, Banner Grabbing through telnet, Analysis of Hibernate and hosts file Email- E-mail Spoofing, E-mail Bombing, Header Analysis of E-mail
Malware Analysis- Malware Classification: Polymorphic and Metamorphic Malware, Virus, Rabbit, Trojans, Back Door, Spyware
Understand the Tools and Techniques – IEXPRESS 2.0, CAY KARAT, Damm Web Application Vulnerabilities (DWAV), WebGoat, ProRat Trojan, Key Logger, Steganographer etc.

DATABASE SECURITY AND DIGITAL FORENSICS (LAB-II):

Database Vulnerabilities: Excessive Privileges Attack, Privilege Abuse, Unauthorized Privilege, Blind SQL, Understand the Weak Authentication, Exposure of Data Backup
Evidence Handling - Registry, Slack Space, windows log file
Analyzing Data from Networked Systems :- Log Files: Access Log, Security Log, Firewall Log, Server log,E-mail Investigations,Cell Phone and Mobile Device Forensics Tools & Techniques: SNORT, Wireshark, TCP Dump, Nexus, RegEdit, Process Monitor

Experimental Objectives

1. Analyze Trojan wrapping by combining the genuine application with a vulnerable program using IEXPRESS 2.0 tool
2. Analyze working and functionalities to remote accessing system through Prorat Trojan
3. Perform surveillance through Packet sniffer tool like Wireshark & TCP Dump
4. Customized packet generation through CAT KARAT Packet builder
5. How Key logger and Spyware breaks user privacy
6. Perform anonymity through e-mail spoofing and bombing using PHP. Subsequently detect these attacks through analyzing the e-mail header.
7. Run online scanners like VirusTotal, Jotti, and NoVirusThanks
8. Find vulnerabilities of target system through Nessus vulnerability Scanner
9. Network enumeration through port scanning using spoofed IP address
10. Case study of SNORT IDS in windows and UNIX environment
11. Analyze SYN flooding attacks through Low orbit ION Cannon tool
12. Detect the Operating System running on target machine through OS Finger printing technique.
13. Perform banner grabbing using telnet
14. What is Hibernate File? Shows the steps to read the contents of the Hibernate File.
15. Develop secure coding practices to handle Code Injection Vulnerabilities such as SQL Injection, PHP Injection and Command Injection
16. Study Programming vulnerability such as buffer overflow, Cross Site Scripting (XSS) and its countermeasures
17. Understand security issues through exploiting vulnerabilities in the Damm Web Application Vulnerabilities (DWAV) or WebGoat tools