M.TECH IN COMPUTER SCIENCE AND ENGINEERING (INFORMATION SECURITY)

CURRICULUM AND SYLLABUS

(Effect from the Academic Year 2007 – 08)

PONDICHERRY UNIVERSITY

PUDUCHERRY – 605014.

M.TECH IN COMPUTER SCIENCE AND ENGINEERING (INFORMATION SECURITY)

COURSE CURRICULUM AND SCHEME OF EXAMINATION

(Minimum Credit Requirement for the completion of the Programme: 72)

M.Tech. in Computer Science and Engineering (Information Security): Candidates for admission to the first semester of four semester M.Tech. Course in Computer Science and Engineering with specialization in Information Security should have passed B.E./B.Tech. in Computer Science and Engineering / Information Technology / Electronics & Communication Engineering / Electrical & Electronics Engineering / Electronics & Instrumentation Engineering / Instrumentation and Control Engineering (or) an examination of any University or Authority accepted by the Pondicherry University as equivalent thereto, with at least 55% marks in the degree examination or equivalent CGPA

SEMESTER – I

Sl. No.	Code	Subject	Hours / Week			Credits	Evaluation (marks)		
			L	T	P		Internal	External	Total
1.	CS 911	Mathematical Foundations of Information Security	3	1	0	4	40	60	100
2.	CS 912	Data Structures	3	1	0	4	40	60	100
3.	CS 913	Internals of Operating Systems	3	1	0	4	40	60	100
4.		Elective – I	3	0	0	3	40	60	100
5.		Elective – II	3	0	0	3	40	60	100
6.	CS 917	Laboratory – I	1	0	3	2	50	50	100
						20	250	350	600

SEMESTER – II

Sl. No.	Code	Subject	Hours / Week			Credits	Evaluation (marks)		
			L	T	P		Internal	External	Total
1.	CS914	Network Security	3	1	0	4	40	60	100
2.	CS 915	Cyber Law and Security Policies	3	1	0	4	40	60	100
3.	CS 916	Information Theory and Coding	3	0	0	3	40	60	100
4.		Elective – III	3	0	0	3	40	60	100
5.		Elective –IV	3	0	0	3	40	60	100
6.		Elective – V	3	0	0	3	40	60	100
7.	CS 918	Laboratory - II	0	0	3	2	50	50	100
						23	290	410	700

SEMESTER – III

Sl. No.	Code	Subject	Hours / Week			Credits	Evaluation (marks)		
			L	T	P		Internal	External	Total
1.		Elective – VI	3	0	0	3	40	60	100
2.		Elective – VII	3	0	0	3	40	60	100
3.	CS 971	Directed Study	0	0	6	3	100	---	100
4.	CS 919	Dissertation Project (Phase I)	0	0	24	8	200	100	400
						17	430	270	700

SEMESTER – IV

Sl. No.	Code	Subject	Hours / Week			Credits	Evaluation (marks)		
			L	T	P		Internal	External	Total
1.	CS 920	Dissertation Project (Phase II)	0	0	36	12	250	150	400
						12	250	150	400

LIST OF ELECTIVE SUBJECTS:

CS941	Advanced Databases
CS942	Agent Technology
CS943	Biometric Security
CS944	Computer Security, Audit Assurance and Risk Management
CS945	Cryptography
CS946	Data and Knowledge Security
CS947	Dependable Distributed Systems
CS948	Embedded Systems
CS949	Fundamentals of Financial Management
CS950	Information Security Policies in Industries
CS951	Mobile Wireless Security
CS952	Security Assessment and Verification
CS953	Secure Software Engineering
CS954	Secured Network Protocols
CS955	Security Threats
CS956	Steganography and Digital Watermarking
CS957	Trust Management in E-Commerce
CS958	Trusted Internet

CS912 DATA STRUCTURES

UNIT I

Problem solving techniques – Space and Time complexity of algorithms-2 Growth of Functions, Asymptotic notation, Standard notations and common functions, Summations

Summation formulas and properties, Bounding summations, Recurrences-substitution method- iteration method- The master method

Sorting – heap sort-quick sort-randomized quick sort- bucket sort-merge sort-radix sort-lower bound on sorting-performance of sorting algorithms-applications of sorting Search –binary and Fibonacci search-applications

UNIT II

Linear data structures-array of structures-stack-queue-priority queues, pointers and linked allocation

Linked list –singly, doubly, circular -polynomial addition-sparse matrices-equivalence relations-garbage collection and compaction

UNIT III

Non linear data structures – Trees- Binary Search Tree, terminology-representation –insertion-deletion-querying

Graphs –terminology-representation-traversals-spanning trees-shortest path-topological sort

UNIT IV

Red black trees, AVL trees , B –trees –building –operations-analysis

UNIT V

Hashing - Basic Ideas- Hash Function- Linear Probing-Quadratic Probing-Separate Chaining Hashing- Hash Tables versus Binary Search Trees- Hashing Application

Reference Books

1. Jean Paul Tremblay and Paul G.Sorenson,"An introduction to data structures with applications" 2nd edition, Tata McGraw hill,2001

2. Thomas H. Cormen (Author), Stein Clifford (Author), Charles E. Leiserson (Author), Robert L. Rivest (Author) "Introduction to Algorithms (Paperback)"

3. Mark Allen Allen Weiss, Florida International University,"Data Structures and Problem Solving Using Java: International Edition, 3/E ", Florida International University,Publisher: Addison-Wesley, Copyright: 2006

4. . S.Saxena, "Splay Trees",Handbook of Data Structure and Application, Chapman & Hall/CRC 2004.

5. Ellis Horowitz and sartaj sahni"Fundamentals of Data Structures",Galgotia Booksource,1995

6. Robert Kruse "C.L.Tondo and Bruce Leung,"Data Structures and Program design in C ",second edition, Pearson Education Asia,2001

CS952 SECURITY ASSESSMENT AND VERIFICATION

Unit I

Evolution of information security, information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

Unit II

Security assessment planning – Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan.
Initial information gathering – Initial preparation, analysis of gathered information.

Unit III
Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

Unit IV
Security Risk assessment project management, Security risk assessment approaches and methods.

Unit V
Information security standards, information security Legislation, formal security verification, security verification with SSL.
Text Book:

1. Sudhanshu Kairab, " A practical guide to security assessments", CRC press, 2005.
2. Douglas J.Landoll, "A Security risk assessment Handbook", Auerbach publications, 2006.

CS952 SECURITY ASSESSMENT AND VERIFICATION

Unit I

Evolution of information security, information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

Unit II

Security assessment planning – Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan.
Initial information gathering – Initial preparation, analysis of gathered information.

Unit III
Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

Unit IV
Security Risk assessment project management, Security risk assessment approaches and methods.

Unit V
Information security standards, information security Legislation, formal security verification, security verification with SSL.
Text Book:

1. Sudhanshu Kairab, " A practical guide to security assessments", CRC press, 2005.
2. Douglas J.Landoll, "A Security risk assessment Handbook", Auerbach publications, 2006.

CS911-MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY

UNIT I

Some topics in elementary number theory: O and Ω notations – time estimates for doing arithmetic – divisibility and the Euclidean algorithm – Congruences – some applications to factoring – finite fields – quadratic residues and reciprocity.

UNIT II

Simple cryptosystems: enciphering matrices – encryption schemes – symmetric and asymmetric cryptosystems – cryptanalysis – Block ciphers – multiple encryption – the use of block ciphers – stream ciphers – the Affine cipher – Vigenere, Hill, and permutation cipher – secure cryptosystem.

UNIT III

Public Key Cryptosystems: The idea of public key cryptography – RSA – discrete log – knapsack – zero-knowledge protocols and oblivious transfer.

UNIT IV

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

UNIT V

Number Theory and Algebraic Geometry: Elliptic curves – basic facts – elliptic curve cryptosystems – elliptic curve primality test – elliptic curve factorization.

REFERENCE BOOKS

1. Neal Koblitz, *A Course in Number Theory and Cryptography*, 2nd Edn., Springer, 2002.
2. Johannes A. Buchman, *Introduction to Cryptography*, 2nd Edn., Springer, 2004.

CS916 - INFORMATION THEORY AND CODING

UNIT I

Source Coding: Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function.

UNIT II

Channel capacity and coding: channel models, channel capacity, channel coding, information capacity theorem, random selection of codes. Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDS codes.

UNIT III

Cyclic codes: polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes, golay codes, CRC codes, circuit implementation of cyclic codes. BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes.

UNIT IV

Convolutional codes: tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding.

UNIT V

Trellis Coded Modulation: concept of coded modulation, mapping by set partitioning, ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels.

REFERENCE BOOKS :

1. Ranjan Bose, "Information theory, coding and cryptography", Tata McGraw Hill, 2002.
2. Viterbi, "Information theory and coding", McGraw Hill, 1982.
3. John G. Proakis, "Digital Communications", 2nd Edition, McGraw Hill, 1989.

CS913 - INTERNALS OF OPERATING SYSTEMS

UNIT I

Introduction to Kernel: Architecture of the UNIX operating system, System concepts, Data structures. Buffer Cache: Buffer header, Structure of Buffer pool, Reading and writing disk blocks. **Files**: INODES, Structure of a regular file, Directories, Super block, Inode assignment.

UNIT II

System calls: OPEN, Read, Close, Write, Create, CHMOD, CHOWN, Pipes, Mounting and Unmounting. **Process:** Layout the system memory, Context, Process control, process creation, signals, Process scheduling, time, clock.

UNIT III

Inter-Process Communications: Process tracing, System V IPC, Shared Memory, Semaphores. **Network Communications**: Socket programming: Sockets, descriptors, Connections, Socket elements, Stream and Datagram Sockets.

UNIT IV

Windows Operating system : versions, Concepts and tools, Windows internals, System Architecture, Requirements and design goals, Operating system model, Architecture overview, Key system components. **System mechanisms**: Trap dispatching, object manager, Synchronization, System worker threads, Windows global flags, Local procedural calls, Kernel event tracing.

UNIT V

Windows Management Mechanisms: The registry, Registry usage, Registry data types, Local structure, Trouble shooting Registry problems, Registry Internals, Services, Applications, Accounts, Service control Manager, Windows Management Instrumentation, Processes, Threads, and Jobs: Process Internals, Flow of create process, Thread Internals, Examining Thread creation, Thread Scheduling, Job Objects.

REFERENCE BOOKS:

1. Maurice J. Bach, The Design of the Unix Operating System, Prentice Hall of India, 1991.
2. Mark E. Russinovich, David A. Solomon, Microsoft® Windows® Internals, Fourth Edition, Microsoft Press, 2004.
3. William Stallings, Operating Systems: Internals and Design Principles, V Edition, Prentice Hall, 2005.

CS914 - NETWORK SECURITY

UNIT I

Introduction to Security in Networks – Characteristics of Networks – Intrusion – Kinds of security breaches – Plan of attack - Points of vulnerability – Methods of defence – Control measures – Effectiveness of controls

UNIT II

Basic encryption and decryption – Encryption techniques – Characteristics of good encryption systems – Secret key cryptography – Data Encryption Standard – International Data Encryption Algorithm – Advanced Encryption Standard – Hash and MAC algorithms

UNIT III

Public Key encryptions – Introduction to number theory - RSA algorithm – Diffie-Hellman – Digital Signature standard – Elliptic Curve cryptography - Digital signatures and authentication – Trusted intermediaries – Security handshake pitfalls

UNIT IV

Secure sockets – IPsec overview – IP security architecture – IPsec-Internet Key Exchanging(IKE) – IKE phases – encoding – Internet security – Threats to privacy – Packet sniffing – Spoofing - Web security requirements – Real Time communication security – Security standards – Kerberos

UNIT V

Security protocols – Transport layer protocols – SSL – Electronic mail security – PEM and S/MIME security protocol – Pretty Good Privacy – Firewalls design principles – Trusted systems – Electronic payment protocols

REFERENCE BOOKS:

1. William Stallings, Cryptography and Network Security: Principles and Standards, Prentice Hall India, 3rd Edition, 2003
2. Charlie Kaufman, Radia Perlman and Mike Speciner, Network Security: Private Communication in a public world, Prentice Hall India, 2nd Edition, 2002
3. Charles P. Pleeger, Security in Computing, Person Education Asia
4. William Stallings, Network Security Essentials: Applications and standards, Person Education Asia, 2000

CS946 - DATA AND KNOWLEDGE SECURITY

UNIT I

Data Security: Database systems- architectures- storage structures- storage issues in in Database Management Systems- Security of data at various levels of Database Management Systems

UNIT II

Distributed Databases: Distributed Data Processing- Distributed Database system- Distributed Database Management System Architecture: Architectural models for Distributed Database Management System – Global directory issues – Distributed database design – distributed design issues – fragmentation – Allocation

UNIT III

Semantic Data Control: View Management – Data centralized Authorization control – Distributed Authorization control – centralized Semantic Integrity Control - Centralized Semantic Integrity Control - Database interoperability - issues related to security in database interoperability

UNIT IV

Knowledge base systems - Knowledge base system design – storage of knowledge – various formats – Levels of security issues in Knowledge base system design – conceptual level – implementation level

UNIT- V

Expert Systems – Design of Expert systems – Knowledge representation techniques in Expert system – structured, semi structured and unstructured data – Knowledge Management and security issues.

REFERENCE BOOKS:

1. Security in Computing, Charles P. Pfleeger and Shari Lawrence Pfleeger, Third Edition, Pearson Education, 2003.
2. Principles of Distributed Database Systems, M.Tamer OZSU and Patrick Valdureiz, Second Edition , Pearson Education, 2001.
3. Artificial Intelligence: A Modern approach, Stuart Russel and Peter Norwig, Third Edition, Pearson Education, 2003.
4. Knowledge Management, Ganesh Natarajan and Sandhya Shekhar, Tata McGrawHill, 2000.

CS953- SECURE SOFTWARE ENGINEERING

UNIT I

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 process- physical 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.

REFERENCE BOOKS:

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

CS915 - CYBER LAW AND SECURITY POLICIES

UNIT I

Security and computing: characteristics of computer intrusion - attacks-security goals-criminals-methods of defense control- cryptography- digital signatures-program security - Protection in operating system - design of trusted operating systems.

UNIT II

Database security- security in networks- network controls-firewalls-Intrusion detection systems-secure Email-Administrating security-organization security polices-legal privacy ethical issues in computer security.

UNIT III

Information security policies and procedures: corporate policies-legal requirements-business requirements- process management-planning and preparation-developing policies-asset classification policy-developing standards.

UNIT IV

Information security: fundamentals-Employee responsibilities-information classification-Information handling-Tools of information security-Information processing-secure program administration

UNIT V

Case studies: Organization security model- Information handling procedures-Developing Information standard manual-Information security manual.

TEXT BOOKS

1. Willis H Ware, Charles P Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", Prentice Hall, 2003

2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004

REFERENCE BOOKS

1 Thomas R Peltier, Justin Peltier, John blackley," Information Security Fundamentals", Second Edition, prentice Hall, 1996

2. Jonathan Rosenoer, "Cyberlaw: the Law of the Internet", Springer-verlag, 1997.

CS944 - COMPUTER SECURITY, AUDIT ASSURANCE AND RISK MANAGEMENT

UNIT-I

Essentials of computer security - Sources of security threats – Intruders, Viruses, Worms and related threats - Threat identification - Threat analysis - Vulnerability identification and Assessment - Components of Computer Security - Physical security – System access control - Goals of Security - Efforts to secure computer networks – Ethical issues in Computer Security- Operational issues, Human issues.

UNIT – II

Cryptography - Public Key Cryptography – Principles of Public Key Cryptosystems – The RSA Algorithm – Key Management – Authentication – Elements, types and methods – Digital Signature – Intrusion Detection System (IDS) – Types and challenges – Intrusion prevention system (IPS) – Firewalls - Design Principles, Scanning, filtering and blocking.

UNIT-III

Vulnerabilities – Sources of vulnerabilities, Vulnerability identification and Assessment, Cyber crime and Hackers, Viruses and content filtering - Security Assessment, Analysis and Assurance – Computer network security protocol and standards - Security Policies – Integrity policies – confidentiality policies - Security models - Access Control Matrix Model, Take-Grant Protection Model.

UNIT – IV

Security Monitoring and Auditing - Assurance and Trust, Need for Assurance, Role of Requirements in Assurance, Audit Assurance in Software Development Phases, Building Secure and Trusted Systems - Designing an Auditing System, Implementation Considerations, Auditing to Detect Violations of a security Policy, Auditing Mechanisms, Audit Browsing.

UNIT-V

Risk management and security planning – Risk management Process Overview- Cost-Benefit Analysis, Risk Analysis, Laws and Customs, Human Issues, Organizational issues - Information system Risk analysis – System approach to risk management, Threat assessment, Assets and safeguards, modes of risk analysis – Effective risk analysis, Qualitative Risk analysis, Value analysis

REFERENCE BOOKS

1. Matt Bishop, "Computer Security: Art and Science", Addison-Wesley Professional, 2003.
2. Joseph M.Kizza, "Computer Network security", Springer, 2005
3. Matt Bishop, "Introduction to Computer Security", Addison-Wesley Professional, 2005.
4. Thomas R.Peltier, "Information Security Risk Analysis", CRC Press, 2001.
5. C.A.Roper, "Risk management for Security professional", Elsevier,1999

CS948 - EMBEDDED SYSTEMS

UNIT I

The 8051 Micro-Controllers: 8051 assembly language programming – instructions – addressing modes – Timer/Counter programming – Serial Communication – Interrupts Programming – Real-World Interfacing

UNIT II

The Microcomputer-based systems: Embedded Computer systems, Architecture of - MC685C05, MC685C08, MC685C11, MC685C12, **Software development:** Quality programming, Modular-layered software development, Device drivers, Object Oriented Interfacing, Threads, Recursion, Debugging, **Interfacing Methods**: Blind cycle counting synchronization, Gadfly or Busy waiting synchronization, Parallel I/O interface Examples.

UNIT III

Interrupt synchronization: General features of interrupts on 6805, 6808, 6811, 6812, Interrupt Vectors and priority, External interrupts, Interrupt Polling, Round Robin Polling, **Threads**: Multithreaded preemptive scheduler, Semaphores, Applications of Semaphores, **Timing Generation and Measurements:** Input-output capture, frequency measurement, conversion between frequency and period

UNIT IV

Serial I/O devices: RS-232C specifications, RS-422 / AppleTalk / RS-423 / RS-485 balanced differential lines, other communication protocols, Serial Communication Interface SCI Applications, **Parallel Port Interfaces**: Input Switches and Keyboards, Output LEDs, LCDs, Transistors used or computer Controlled Relay Keys, DC Motors, Stepper Motors, **Memory Interfacing**: Address decoding, Timing Syntax, Bus-Timings, Memory interface examples, **High-Speed I/O interfacing**: High speed I/O applications, High-Speed interfaces, Examples.

UNIT V

Analog Interfacing: Operational Amplifiers filters, converters, Multiplexer, ADCs, **Data Acquisition Systems:** Transducers, DAS Design, Noise analysys, **Microcomputer-Based Control**: Open-Loop Control systems, Closed Loop Control System, PID Controllers, Simple Networks, Digital Filters.

REFERENCE BOOKS:

1. Muhammad Ali Mazidi & Janice Gillispie Mazidi , "The 8051 Micro-controllers and Embedded Systems", PHI, 2000
2. Jonathan W.Valvano , "The Embedded Microcomputer Systems", Thomson Brooks/Cole, 2000
3. AVR, Barnett, Cox, & O'Cull, "Embedded C Programming and the Atmel", Thomson Brooks/Cole, 2000
4. John B Pitman, "Design with PIC Micro controllers", Pearson Education Asia, 1998
5. David E Simon, "*An embedded software primer*", Pearson Education Asia, 2001

CS945 - CRYPTOGRAPHY

UNIT I

Introduction – Beginning with a simple communication game – Wrestling between safeguard and attack – Encryption symmetric techniques.

UNIT II

Encryption – Asymmetric techniques –Bit security of the basic public key cryptographic functions

UNIT III

Data Integrity Techniques –Authentication framework for public key cryptography.

UNIT IV

Formal and strong security definitions for public-key crypto systems – Provably secure and efficient public-key cryptosystems – Introduction – The optimal asymmetric encryption padding.

UNIT V

The Cramer–Shoup Public-key crypto systems – An overview of provably secure hybrid cryptosystems – Literature notes on practical and provably secure public-key cryptosystems – Strong and provable security for digital signatures.

REFERENCE BOOKS:

1. Wenbo Mao, Modern Cryptography Theory and Practice, Pearson Education, 2004. (UNIT – I: 1-52, 205-243, UNIT-II : 245-296, UNIT – III : 297 – 326, 427 – 456, UNIT – IV : 461 – 523, UNIT – V : 523 – 575)
2. Atvl Kahate, Cryptography and Network Security, Tata McGrew Hill, 2003.
3. William Stallings, Cryptography and Network Security, Third Edition, Pearson Education, 2003.

CS955 - SECURITY THREATS

UNIT I

Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Cyber crimes.

UNIT II

Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms – Virus – Spams – Adware - Spy ware – Trojans – Backdoors – Bots - IP Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats - Threats to Server security.

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 Panning.

UNIT IV

Security Elements: Access Rights - Access control systems - Authorization and Authentication - types, policies and techniques - Security certification - Security monitoring and Auditing - Security Requirements Specifications - Security Polices and Procedures.

UNIT V

Firewalls & Intrusion Detection Systems: Firewalls – Types - Dynamic packet filtering content filtering – Crypto capable Routers, - VPNs - Secure Modems - Intrusion Detection Systems – Types - Intrusion Detection Tools – Penetration testing- Intrusion Analysis - Log file Monitors - Honey pots - Intrusion Prevention Systems - Trusted Systems.

TEXT BOOKS :

1. Joseph M Kizza, "Computer Network Security", Springer, 2005
2. Swiderski, Frank, Syndex, "Threat Modeling", Microsoft Press, 2004.
3. William. R Cheswick, Steven M. Bellowin, Aviel D Rubin, "Firewalls & Internet Security – Repelling the Wily Hacker", 2nd Edition, Addison Wesley Professional, 2003

REFERENCE BOOKS :

1. Thomas Calabrese,Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004

CS957 -TRUST MANAGEMENT IN E-COMMERCE

UNIT I

Introduction to E-Commerce – Network and E-Commerce – Types of E-Commerce – E-Commerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models – E-Commerce Payment systems: Types of payment system – Credit card E-Commerce transactions – B2C E-Commerce Digital payment systems – B2B payment system.

UNIT II

Security and Encryption: E-Commerce Security Environment – Security threats in E-Commerce environment – Policies, Procedures and Laws.

UNIT III

Inter-organizational trust in E-Commerce: Need – Trading partner trust – Perceived benefits and risks of E-Commerce – Technology trust mechanism in E-Commerce – Perspectives of organizational, economic and political theories of inter-organizational trust – Conceptual model of inter-organizational trust in E-Commerce participation.

UNIT IV

Introduction to trusted computing platform: Overview – Usage Scenarios – Key components of trusted platform – Trust mechanisms in a trusted platform

UNIT V

Trusted platforms for organizations and individuals – Trust models and the E-Commerce domain.

REFERENCE BOOKS :

1. Kenneth C. Laudon, Carol Guercio Trave, " E-Commerce Busines. Technology. Society.", Pearson Education, 2005.
2. Pauline Ratnasingam. "Inter-Organazational Trust for Business-to-Business E-Commerce", IRM Press.
3. Siani Pearson, et al, "Trusted Computing Platforms: TCPA Technology in Context", Prentice Hall PTR, 2002.

CS956 - 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.

REFERENCE BOOK:

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

CS950 - INFORMATION SECURITY POLICIES IN INDUSTRIES

UNIT I

Introduction to Information Security Policies – About Policies – why Policies are Important – When policies should be developed – How Policy should be developed - Policy needs – Identify what and from whom it is being protected – Data security consideration – Backups, Archival storage and disposal of data - Intellectual Property rights and Policies – Incident Response and Forensics - Management Responsibilities – Role of Information Security Department - Security Management and Law Enforcement – Security awareness training and support .

UNIT II

Policy Definitions – Standards – Guidelines - Procedures with examples - Policy Key elements - Policy format and Basic Policy Components - Policy content considerations - Program Policy Examples - Business Goal Vs Security Goals - Computer Security Objectives - Mission statement Format – Examples - Key roles in Organization - Business Objectives - Standards – International Standards.

UNIT III

Writing The Security Policies - Computer location and Facility construction - Contingency Planning - Periodic System and Network Configuration Audits - Authentication and Network Security – Addressing and Architecture – Access Control – Login Security – Passwords – User Interface – Telecommuting and Remote Access – Internet Security Policies – Administrative and User Responsibilities – WWW Policies – Application Responsibilities – E-mail Security Policies.

UNIT IV

Establishing Type of Viruses Protection - Rules for handling Third Party Software - User Involvement with Viruses - Legal Issues- Managing Encryption and Encrypted data - Key Generation considerations and Management - Software Development policies - Processes - Testing and Documentation- Revision control and Configuration management - Third Party Development - Intellectual Property Issues

UNIT V

Maintaining the Policies - Writing the AUP - User Login Responsibilities - Organization's responsibilities and Disclosures- Compliance and Enforcement – Testing and Effectiveness of Policies - Publishing and Notification Requirements of the Policies- Monitoring, Controls and Remedies - Administrator Responsibility - Login Considerations - Reporting of security Problems - Policy Review Process - The Review Committee-Sample Corporate Policies – Sample Security Policies

REFERENCE BOOKS :

1. SCOTT BARMAN; Writing Information Security Policies, Sams Publishing, 2002.
2. THOMAS.R.PELTIER; Information Policies , Procedures and Standards, CRC Press, 2004.

CS942 - AGENT TECHNOLOGY

UNIT I

Agent Definition - History - Intelligent Agents- Agent Programming Paradigms - Agent Vs Object - Aglet - Mobile Agents – Agent Frameworks - Agent Reasoning.

UNIT II

Interaction between Agents - Reactive Agents - Cognitive Agents - Interaction protocols - Agent coordination -Agent negotiation - Agent Cooperation - Agent Organization - Self - interested agents in electronic commerce applications.

UNIT III

Agents and Multi-agent Systems- Problem Solving and Knowledge Representation- Reasoning Systems and Learning Systems- Agent Oriented Methodologies and Frameworks- Agent Interoperability- Logics for Multiagent Systems.

Interface Agents - Agent Communication Languages - Agent Knowledge representation - Agent adaptability -Belief Desire Intension - Mobile Agent Applications.

UNIT IV

Situational Calculus - Representation of Planning - Partial order Planning- Practical Planners – Conditional Planning - Replanning Agents.

UNIT V

Agent Security Issues - Mobile Agents Security - Protecting Agents against Malicious Hosts - Untrusted Agent -Black Box Security - Authentication for agents - Security issues for aglets-Agent Technology in Business.

REFERENCE BOOKS :

1. Bradshaw, *Software Agents,* MIT Press, 2000.
2. Russel & Norvig, *Artificial Intelligence: a modern approach*, Prentice Hall, 1994.
3. Richard Murch, Tony Johnson, *Intelligent Software Agents*, Prentice Hall, 2000.
4. Nils.J.Nilsson, *Principles of Artificial Intelligence*, Narosa Publishing House, 1992

CS949 - FUNDAMENTALS OF FINANCIAL MANAGEMENT

UNIT I

Introduction to Financial Management - The Role of Financial Management - The Business, Tax, and Financial Environments - Valuation - The Time Value of Money - The Valuation of Long-Term Securities - Risk and Return

UNIT II

Tools of Financial Analysis and Planning - Financial Statement Analysis - Funds Analysis, Cash-Flow Analysis, and Financial Planning - Working Capital Management - Overview of Working Capital Management - Cash and Marketable Securities Management - Accounts Receivable and Inventory Management - Short-Term Financing

UNIT III

Investment in Capital Assets - Capital Budgeting and Estimating Cash Flows - Capital Budgeting Techniques - Risk and Managerial Options in Capital Budgeting - The Cost of Capital, Capital Structure, and Dividend Policy - Required Returns and the Cost of Capital - Operating and Financial Leverage - Capital Structure Determination - Dividend Policy

UNIT IV

Intermediate and Long-Term Financing - The Capital Market - Long-Term Debt, preferred Stock, and Common Stock - Term Loans and Leases

UNIT V

Special Areas of Financial Management - Convertibles, Exchangeables, and Warrants - Mergers and Other Forms of Corporate Restructuring - International Financial Management

TEXT BOOK :

1. James C. Van Horne and John M. Wachowicz, "Fundamentals of Financial Management", 11th Edition, ISBN: 81-203-2016-6

CS941 - ADVANCED DATABASES

UNIT I

DATABASE MANAGEMENT : Relational Data Model – SQL - Database Design - Entity-Relationship Model – Relational Normalization – Embedded SQL – Dynamic SQL – JDBC – ODBC. Case Studies

UNIT II

ADVANCED DATABASES : Object Databases - Conceptual Object Data Model – XML and Web Data – XML Schema – Distributed Data bases – OLAP and Data Mining – ROLAP and MOLAP. Case Studies

UNIT III

QUERY AND TRANSACTION PROCESSING : Processing Basics – Heuristic Optimization – Cost, Size Estimation - Models of Transactions – Architecture – Transaction Processing in a Centralized and Distributed System – TP Monitor. Case Studies for Real time Systems

UNIT IV

IMPLEMENTING AND ISOLATION : Schedules – Concurrency Control – Objects and Semantic – Locking – Crash, Abort and Media Failure – Recovery – Atomic Termination – Distributed Deadlock – Global Serialization – Replicated Databases – Distributed Transactions in Real World. Case Studies

UNIT V

DATABASE DESIGN ISSUES : Security – Encryption – Digital Signatures – Authorization – Authenticated RPC - Integrity - Consistency - Database Tuning - Optimization and Research Issues. Case Studies

REFERENCE BOOKS:

1. Philip M. Lewis, Arthur Bernstein, Michael Kifer, "Databases and Transaction Processing:An Application-Oriented Approach", Addison-Wesley, 2002
2. R. Elmasri and S.B. Navathe, Fundamentals of Database Systems, 3rd Edition, Addison Wesley, 2004
3. Abraham Silberschatz, Henry. F. Korth, S.Sudharsan, Database System Concepts, 4th Edition., Tata McGraw Hill, 2004
4. Raghu Ramakrishnan & Johannes Gehrke, "Database Management Systems", III Edition,TMH, 2003

CS943 - BIOMETRIC SECURITY

UNIT I:

Biometrics- Introduction- benefits of biometrics over traditional authentication systems-benefits of biometrics in identification systems-selecting a biometric for a system-Applications. Key biometric terms and processes-how biometric matching works-Accuracy in biometric systems

UNIT II:

Physiological Biometric Technologies: Fingerprints- Technical description-characteristics-Competing technologies-strengths – weaknesses-deployment. Facial scan - Technical description-characteristics- weaknesses-deployment. Iris scan - Technical description-characteristics- strengths – weaknesses-deployment. Retina vascular pattern-Technical description-characteristics- strengths – weaknesses-deployment. Hand scan - Technical description-characteristics- strengths – weaknesses-deployment –DNA biometrics

UNIT III :

Behavioral Biometric Technologies: Handprint Biometrics-DNA Biometrics-signature and handwriting technology- Technical description – classification- keyboard /keystroke dynamics -Voice – data acquisition- feature extraction-characteristics- strengths – weaknesses-deployment

UNIT IV :

Multi biometrics: Multi biometrics and multi factor biometrics- two-factor authentication with passwords, tickets and tokens –executive decision- implementation plan

UNIT V:

Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

REFERENCE BOOKS :

1. Samir Nanavathi,Michel Thieme,Raj Nanavathi,"Biometrics -Identity verification in a network", Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul," Implementing Biometric Security", Wiley EasternPublications,2005.
3. John Berger," Biometrics for Network Security", Prentice Hall, 2004.

CS958 -TRUSTED INTERNET

UNIT I

INTERNET : Understanding the Internet, Hardware Requirements to connect to the internet, Software requirements and Internet Service Providers (ISP), Internet Addressing, Internet Protocol : Routing Information Protocol (RIP); User Datagram Protocol (UDP) ; Transmission Control Protocol (TCP), Domain Name Service (DNS), Basic Connectivity : Telnet; FTP, Internet Relay Chat (IRC).

UNIT II

ATTACKS : Access Attacks – Snooping; Eavesdropping; interception, Hacker Techniques – Hacker's motivation; Historical Hacking Techniques; Advance Techniques; Targeted Hacker, Information Security Services – Confidentiality, Integrity; Availability; Accountability.

UNIT III

FIREWALL : Firewall Concepts, Types of Firewalls, Firewall Configuration, Design a Firewall Rule set, Purpose of Firewall, Security role of a Firewall, Advantages and disadvantages of firewall, Firewall Components, Procuring a Firewall, Administrating a firewall, firewall toolkits.

UNIT IV

ENCRYPTION : Basic Concepts, Private Key Encryption, Public Key Encryption, Digital Signature, Trust in the System, Encryption Algorithm – RSA Encryption, Blowfish Encryption.

E-Commerce Security: E-Commerce Services, Importance of Availability, Security Implementation – Client Side; Server side; Application; Database Server.

UNIT V

SECURITY : Security Environment, User Authentication, Attacks form inside the system, Attacks from outside the system, Protection Mechanism, Trusted Systems, Trusted Computing Base, Formal Models of Secure system, Multilevel security, Designing trusted Operating System.

TEXT BOOKS:

1) Marcus Goncalves., "Firewalls - A Complete Guide", Tata McGraw-Hill, 2000
2) Harley Hahn., "The Internet – Complete Reference", Tata McGraw-Hill, 1997
3) Charles P.Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", Pearson Education (Singapore) Pvt Ltd, 3rd Edition.
4) Richard E. Smith, "Internet Cryptography", Pearson Education(Singapore) Pvt Ltd, 2000

REFERENCE BOOKS:

1) Andrew S. Tanenbaum, "Modern Operating Systems", Pearson Education(Singapore) Pvt Ltd, 3rd Edition.
2) William Stallings, "Cryptography and Network Security", Pearson Education(Singapore) Pvt Ltd, 3rd Edition.
3) Ankit Fadia, "Unofficial Guide to Ethical Hacking", Macmillan India Ltd, 2001
4) Fundamentals of Network Security Companion – Cisco Systems, Inc, Pearson Education(Singapore) Pvt Ltd, 2004.

CS951 - MOBILE WIRELESS SECURITY

UNIT I

Wireless Fundamentals : Wireless Hardware- Wireless Network Protocols- Wireless Programming WEP Security. Wireless Cellular Technologies – concepts – Wireless reality – Security essentials – Information classification standards - Wireless Threats : Cracking WEP - Hacking Techniques- Wireless Attacks – Airborne Viruses.

UNIT II

Standards and Policy Solutions – Network Solutions – Software Solutions – Physical Hardware Security- Wireless Security – Securing WLAN – Virtual Private Networks – Intrusion Detection System – Wireless Public Key infrastructure.. Tools – Auditing tools – Pocket PC hacking – wireless hack walkthrough.

UNIT III

Security Principles – Authentication – Access control and Authorization – Non-repudation- privacy and Confidentiality – Integrity and Auditing –Security analysis process. Privacy in Wireless World – Legislation and Policy – Identify targets and roles analysis – Attacks and vulnerabilities – Analyze mitigations and protection.

UNIT IV

WLAN Configuration – IEEE 802.11 – Physical layer – media access frame format – systematic exploitation of 802.11b WLAN – WEP – WEP Decryption script – overview of WEP attack – Implementation - Analyses of WEP attacks.

UNIT V

Mobile Commerce Security and Payment Methods – Reputation and Thrust – Intrusion detection - Vulnerabilities analysis of mobile commerce platform – Secure authentication for mobile users – Mobile Commerce security – Payment methods – Mobile Coalition key evolving Digital Signatures scheme for wireless mobile networks.

TEXT BOOKS

1. Russel Dean Vines,"Wireless Security Essentials: Defending Mobile from Data Piracy", John Wiley & Sons, First Edition – 2002.
2. Cyrus, Peikari, Seth Fogie, "Maximum Wireless Security", SAMS Publishing 2002.
3. Wen Chen hu, Chang Wiu Lee, Weidong kou, "Advances in Security and Payment Methods for Mobile Commerce", Idea Group Inc-2004.

REFERENCES

1. Tara M. Swaminathan, Charles R. Eldon, "Wireless Security and Privacy-Best Practices and Design Techniques", Addison Wesley –2002.
2. Bruce Potter, Bob Fleck, "802.11 Security", O'Reilly Publications,2002.

CS954 - SECURED NETWORK PROTOCOLS

UNIT I

OSI:ISO Layer Protocols:-Application Layer Protocols-TCP/IP, HTTP, SHTTP, LDAP, MIME,-POP& POP3-RMON-SNTP-SNMP. Presentation Layer Protocols-Light Weight Presentation Protocol Session layer protocols –RPC protocols-transport layer protocols-ITOT,RDP,RUDP,TALI,TCP/UDP, compressed TCP. Network layer Protocols – routing protocols-border gateway protocol-exterior gateway protocol-internet protocol IPv4-IPv6- Internet Message Control Protocol- IRDP- Mobile IP – Mobile Support Protocol for IPv4 and IPv6 – Resource Reservation Protocol. Multi-casting Protocol – VGMP – IGMP – MSDP.

UNIT II

Data Link layer Protocol – ARP – InARP – IPCP – IPv6CP – RARP – SLIP .WideArea and Network Protocols- ATM protocols – Broadband Protocols – Point to Point Protocols – Other WAN Protocols- security issues.

UNIT III

Local Area Network and LAN Protocols – ETHERNET Protocols – VLAN protocols – Wireless LAN Protocols – Metropolitan Area Network Protocol – Storage Area Network and SAN Protocols -FDMA, WIFI and WIMAX Protocols- security issues.

UNIT IV

Network Security and Technologies and Protocols – AAA Protocols – Tunneling Protocols – Secured Routing Protocols – GRE- Generic Routing Encapsulation – IPSEC – Security architecture for IP – IPSECAH – Authentication Header – ESP – IKE – ISAKMP and Key management Protocol. IEEE 802.11 - Structure of 802.11 MAC – WEP- Problems with WEP – Attacks and Risk- Station security – Access point Security – Gate way Security – Authentication and Encryption.

UNIT V

IEEE 802.15 and Bluetooth – WPAN Communication Protocols – IEEE 802.16- IEEE 802.16A.WCDMA – Services – WCDMA Products – Networks- device addressing – System Addressing – Radio Signaling Protocol – Multimedia Signaling Protocol.

TEXT BOOKS

1. Jawin, "Networks Protocols Handbook", Jawin Technologies Inc., 2005.
2. Bruce Potter, Bob Fleck, "802.11 Security", O'Reilly Publications,2002..
3. Lawrence Harte, "Introduction to WCDMA" , Althos Publishing, 2004.

REFERENCE BOOKS

1. Lawrence Harte, "Introduction to CDMA- Network services Technologies and Operations" , Althos Publishing, 2004.
2. Lawrence Harte, "Introduction to WIMAX " , Althos Publishing, 2005.

CS947 - DEPENDABLE DISTRIBUTED SYSTEMS

UNIT I

Dependability concepts - Faults and Failures – Redundancy – Reliability – Availability – Safety – Security – Timeliness - Fault-classification - Fault-detection and location - Fault containment - Byzantine failures - Fault injection - Fault-tolerant techniques - Performability metrics.

UNIT II

Fault-tolerance in real-time systems - Space-time tradeoff - Fault-tolerant techniques (N-version programming - Recovery block - Imprecise computation; (m,k)- deadline model) - Adaptive fault-tolerance - Fault detection and location in real-time systems. Security Engineering – Protocols - Hardware protection - Cryptography – Introduction – The Random Oracle model – Symmetric Crypto- primitives – modes of operations – Hash functions – Asymmetric crypto primitives.

UNIT III

Distributed systems - Concurrency - fault tolerance and failure recovery – Naming. Multilevel Security – Security policy model – The Bell Lapadula security policy model – Examples of Multilevel secure system – Broader implementation of multilevel security system. Multilateral security – Introduction – Comparison of Chinese wall and the BMA model – Inference Control – The residual problem.

UNIT IV

Banking and bookkeeping – Introduction – How computers systems works – Wholesale payment system – Automatic teller Machine – Monitoring systems – Introduction – Prepayment meters – Taximeters, Tachographs and trunk speed limits. Nuclear Command and control – Introduction – The kennedy memorandum – unconditionally secure authentication codes – shared control security – tamper resistance and PAL – Treaty verification. Security printing and seals – Introduction – History – Security printing – packaging and seals – systemic vulnerability – evaluation methodology

UNIT V

Bio metrics – Introduction – Handwritten signature – face recognition – fingerprints – Iris codes – Voice recognition. Emission Security – Introduction – Technical Surveillance and countermeasures – Passive Attacks – Active Attacks. Electronic and Information warfare – Introduction – Basics – Communication system – Surveillance and target acquisition – IFF system – Directed Energy Weapon – Information Warefare. Telecom Security – Introduction – Phone Breaking – Mobile phones – Network attack and defense - Protecting E-commerce systems- E – policy – Management issues – systems evaluation and assurance.

REFERENCE BOOKS

1. Ross J Anderson and Ross Anderson, Security Engineering: A guide to building dependable distributed systems, Wiley, 2001.
2. David Powell, A generic fault-Tolerant architecture for Real-Time Dependable Systems, Springer, 2001.
3. Dependable computing systems: Paradigm, Performance issues and Applications, Hassan B Diab and Albert Y. Zomaya, Wiley series on Parallel and Distributed Computing, 2000.