Punjab Technical University, Jalandhar
Study Scheme Batch 2012

M.TECH (INFORMATION SECURITY)

Schedule of Teaching

Lecture	Tutorials	Practical
All theory Subjects		
All Labs		
Projects		
Seminar		
Dissertation		

Schedule of Examination

	Time (Hrs)	Theory Marks	Sessional Marks	Viva	Total
All theory Subjects	03	100	50		150
All Labs		50	50		100
Projects		50	50		100
Seminar			100		100
Dissertation	Satisfactory/Not Satisfactory				

Semester 1

Subject Code	Title of Course	L	T	P	Credit
SS 501	Advance Data Structures	4	0	--	4
IS 503	Secure Coding	4	0	--	4
IS 505	Ethical Hacking	4	0	--	4
IS 507	Information Theory and Coding	4	0	--	4
IS 509	Cryptography	4	0	--	4
SS 511	Advanced Data Structures Lab	--	--	4	2
SS 513	Secure Coding Lab	--	--	4	2

Semester 2

Subject Code	Title of Course	L	T	P	Credit
IS 502	Network Security	4	0	--	4
IS 504	Penetration testing and auditing	4	0	--	4
IT 506	Research Methodologies	4	0	--	4
IS AAA	Elective –I	4	0	--	4
IS BBB	Elective-II	4	0		4
IS 508	Network Security Lab	--	--	4	2

Semester-III

Subject Code	Title of Course	L	T	P	Credit
IS CCC	Elective-III	4	0	--	4
IS DDD	Elective-IV	4	0	--	4
IS 521	Major project	--	--	4	4
IS 523	Seminar	4	--	--	4

Semester-IV

Subject Code	Name of Subject	L	T	P
IS 500	Dissertation	-	-	-

Elective-I (IS) AAA

IS 512 Secure Information Storage and Retrieval

IS 514 IT Security Policies and Procedures.

IS 516 Mobile Application Development and Security

Elective-II (IS) BBB

IS 515 Virtualization and Cloud Security

IS517 Cyber incident Handling and Reporting

IS 519 Database Security and Governance

Elective-III (IS) CCC

IS 525 Forensics and cyber laws

IS 527 Reverse Engineering Malware

IS 529 Intrusion Detection Analysis

Elective-IV (IS) DDD

IE 513 Organization Theories and Behaviour

SS 522 Total Quality Management

SS 524 Product Design and Management

SS 526 Enterprise Resource Planning

SS528 IT Strategy and Management

SS-501 Advance Data Structures

L T P

4 0 –

Objective: This course helps students, step by step to develop algorithms and to solve real world problems. Implementing various data structures and understanding various searching & sorting techniques, to arrange data in a particular manner. These manner or set of rules is defined in the advanced data structure so that the data used in computer systems can properly used at necessary time.

Review of Elementary Data Structures: Arrays, linked lists, stacks, queues, binary trees, hashing, graphs, sorting & searching techniques.

Sparse Matrices: Properties of sparse matrices, Linked list representation of sparse matrices.

Threaded Trees: Properties of threaded trees, insertion, deletion and traversal.

AVL Trees: Properties of AVL trees, rotations, insertion and deletion.

Red-Black Trees: Properties of red-black trees, rotations, insertion and deletion.

B-Trees: Definition of B-trees, basic operations on B-trees, deleting a key from a B-tree.

Heaps: Properties of Min-max heaps, building a heap, basic operations on heaps, application of min-max heaps.

Binomial heaps: Binomial tress and binomial heaps, operations on binomial.

Fibonacci heaps: Structure of Fibonacci heaps, merge able heap operations, decreasing a key and deleting a node, bounding a maximum degree.

Data Structures for Disjoint Sets: Disjoint set operations, linked list representation of disjoint sets, disjoint set forests.

Graph Algorithms: Topological sort, minimum Spanning tree, single-source shortest paths, all-pairs shortest paths, bi-connected components, strongly connected components, cycles, articulation points, bridges.

String Matching: String-matching algorithm, Rabin-Karp algorithm, String matching with automata, Knuth-Morris-Pratt algorithm, Boyer-Moore algorithm.

NP-completeness: Complexity classes P and NP, examples of reductions.

Suggested Readings/ Books:

1. Peter Brass, "Advanced Data Structures" Cambridge University Press, 2008.
2. Kurt Mehlhorn, Peter Sanders "Algorithms and Data Structures", Springer Berlin Heidelberg, 2008.
3. A.A.Puntambekar, "Advanced Data Structures And Algorithms", Technical Publications, 2008
4. Darren Redfern, Colin Campbell, **"**Advanced Data Structures" Springer New York, 1998.
5. Frank Dehne, John Iacono, Jörg-Rüdiger Sack," Algorithms and Data Structures" 12th International Symposium, WADS 2011, NY, USA, 2011.

IS 503- SECURE CODING

L T P

4 0 –

Objective: Students shall understand vulnerabilities in coding, identify, and remediate them.

Need & Significance: The need for secure systems, Proactive Security development process: security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, SD3 (Secure by design, default and deployment), Security principles, Threat modelling.

Security: Security techniques, authentication, authorization, Buffer Overrun, Access control, least privilege, Input issues: database, web-specific, internationalization.

Socket Security, Securing RPC, ActiveX and DCOM, Protection against DoS attacks.

Testing: Security testing, security code review, secure software installation, writing security documentation.

References:

1. Howard Michael and LeBlanc David, "Writing Secure Code", Microsoft Press.
2. Haridas Nithin, "Software Engineering - Security as a Process in the SDLC".
3. Burns Steven, "Threat Modeling: A Process to Ensure Application Security".
4. Gupta Sandeep , " A Proactive Approach to Information Security".
5. Deckard Jason, "Defeating Overflow Attacks".

IS 505 -Ethical Hacking

L T P

4 0 –

Objective: This course will help students in getting the insight of some techniques and skills as an ethical hacker to help prospective clients understand how to stay secure. In this course, they will learn what it takes to become an ethical hacker and the methods real attackers use to penetrate networks and computer systems.

Introduction: Introduction of Ethical Hacking concept, Networking & Basics, Foot Printing, Google Hacking, Scanning, Windows Hacking, Linux Hacking, Trojans & Backdoors, Virus & Worms, Proxy & Packet Filtering, Denial of Service, Sniffer, Social Engineering.

Securities & Vulnerabilities: Introduction to Computer Systems and Networks , information systems and networks (including wireless networks) and their role in industry business and society, System and Network Vulnerability and Threats to Security , various types of attack and the various types of attackers in the context of the vulnerabilities associated with computer and information systems and networks Physical Security, Steganography, Cryptography, Wireless Hacking, Firewall & Honeypots, IDS & IPS, Vulnerability, Penetration Testing, Session Hijacking, Hacking Web Servers, SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobiles Phone Hacking.

Hacking Tools: An introduction to basic ethical hacking tools and usage of these tools in a professional environment in a form of project.

Legal & Ethical Issues: An introduction to the particular legal, professional and ethical issues likely to face the domain of ethical hacking. ethical responsibilities, professional integrity and making appropriate use of the tools and techniques associated with ethical hacking.

Reference Books:

1. Simpson Michael, Backman Kent ,Corley James, " Hands-On Ethical Hacking and Network Defence"
2. DeFino Steven, Kaufman Barry, Valenteen Nick, "Official Certified Ethical Hacker Review Guide"
3. Stuart McClure, Joel Scambray and Goerge Kurtz, "Hacking Exposed Network Security Secrets & Solutions", Tata Mcgrawhill Publishers, 2010.
4. Bensmith, and Brian Komer, "Microsoft Windows Security Resource Kit", Prentice Hall of India, 2010.
5. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (Syngress Basics Series) [Paperback].
6. Hands-On Ethical Hacking and Network Defence Print Replica Kindle Edition.

IS 507- Information Theory and Coding

L T P
4 0 -

Objective: This course covers information theory and coding within the context of modern digital communications applications. This course will help students in quantify the notion of information in a mathematically and intuitively sound way. This course will help in explaining how this quantitative measure of information may be used in order to build efficient solutions to multitudinous engineering problems

Introduction: 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. Information, channel capacity, the concept of amount of information, entropy, Information rate, Conditional and joint entropies.

Discrete channels – Symmetric channels, Binary Symmetric Channel, Binary Erasure Channel, Cascaded channels, repetition of symbols, Binary un-symmetric channel, Shannon theorem. Continuous channels – Capacity of band limited Gaussian channels, Shannon-Hartley theorem, Trade-off between band width and signal to noise ratio, Capacity of a channel with infinite band width, Optimum modulation system.

Source coding : Noise less coding, Shannon's first fundamental theorem, Discrete memory less channel, Mutual information, Sources with finite memory, Markov sources, Shannon's second fundamental theorem on coding, Huffman coding, Lempel – Ziv algorithm, Shannon-Fano algorithm.

Channel coding: Codes for error detection and correction – Parity check coding, Linear block codes, Error detecting and correcting capabilities, Generator and Parity check matrices, Standard array and Syndrome decoding, Hamming codes, Encoding and decoding of systematic and unsystematic codes. Cyclic codes – Generator polynomial, Generator and Parity check matrices, Encoding of cyclic codes, Syndrome computation and error detection, Decoding of cyclic codes, BCH codes, RS codes, Burst error correction., Repetition codes, Linear block codes, binary cyclic codes, BCH codes, Reed-Soleman codes, Golay codes.

Convolution Coding: 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.

References:

1. Gover T. M., Thomos J. M., "Elements of Information Theory", Wiley, 1991
2. Ranjan Bose, "Information theory, coding and cryptography", Tata McGraw Hill, 2002.
3. Viterbi, "Information theory and coding", McGraw Hill, 1982.
4. Proakis J. G., "Digital Communications", Mc Graw Hill.
5. Shoup Victor, "A Computational Introduction to Number Theory and Algebra", Cambridge University Press,
6. Koblitz Neal, "A Course in Number Theory and Cryptography", 2nd Edition, Springer, 2002.
7. Simon Haykin, Communication Systems, John Wiley & Sons. Pvt. Ltd.
8. Taub & Schilling, Principles of Communication Systems, Tata McGraw-Hill
9. Shu Lin & Daniel J. Costello Jr, Error Control Coding Fundamentals and Applications. Prentice Hall Inc.

IS 509 -Cryptography

L T P

4 0 –

Objective: This course is intended as an introduction to Cryptography. This course examines basic cryptography principles such as encryption, hashes, message authentication codes, digital signatures, digital certificates and network defense. Students will become familiar with cryptographic techniques for secure (confidential) communication of two parties over an insecure (public) channel.

UNIT I

Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols – Advanced Protocols - Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity -Blind Signatures - Identity-Based Public-Key Cryptography - Oblivious Transfer - Oblivious Signatures – Esoteric Protocols

UNIT II

Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block Chaining Mode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode - Synchronous Stream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving - Block Ciphers versus Stream Ciphers - Choosing an Algorithm - Public- Key Cryptography versus Symmetric Cryptography - Encrypting Communications Channels - Encrypting Data for Storage - Hardware Encryption versus Software Encryption - Compression, Encoding, and Encryption - Detecting Encryption – Hiding and Destroying Information.

UNIT III

Information Theory - Complexity Theory - Number Theory - Factoring - Prime Number Generation - Discrete Logarithms in a Finite Field - Data Encryption Standard (DES) – Lucifer - Madryga - NewDES - GOST – 3 Way – Crab – RC5 - Double Encryption - Triple Encryption - CDMF Key Shortening - Whitening.

UNIT IV

Pseudo-Random-Sequence Generators and Stream Ciphers – RC4 - SEAL - Feedback with Carry Shift Registers - Stream Ciphers Using FCSRs - Nonlinear-Feedback Shift Registers - System-Theoretic Approach to Stream-Cipher Design - Complexity-Theoretic Approach to Stream-Cipher Design - N- Hash - MD4 - MD5 - MD2 - Secure Hash Algorithm (SHA) - One- Way Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms - Message Authentication Codes

UNIT V

RSA - Pohlig-Hellman - McEliece - Elliptic Curve Cryptosystems -Digital Signature Algorithm (DSA) - Gost Digital Signature Algorithm - Discrete Logarithm Signature Schemes – Ongchnorr- Shamir -Cellular Automata - Feige-Fiat-Shamir -Guillou-Quisquater - Diffie-Hellman - Station-to-Station Protocol -Shamir's Three-Pass Protocol - IBM Secret-Key Management Protocol - MITRENET - Kerberos - IBM Common Cryptographic Architecture.

References:

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

SS 511 -ADVANCED DATA STRUCTURES LAB

L	T	P
-	-	4

The Students are required to implement the applications based on SS-501.

IS 513 -SECURE CODING LAB

L	T	P
-	-	4

The Students are required to implement the applications based on IS - 503

IS 502 -Network Security

L T P

4 0 –

Objective: The objectives of this course are to systematically study theories, principles and techniques of computer and network security. Students will learn basic cryptography, fundamentals of computer/network security, risks faced by computers and networks, security mechanisms, operating system security, secure systems design principles, and network security principles. This course is formulated to understand students the common threats and vulnerabilities of networked systems. It will describe network security primitives, and helps students in learning recent advances in Network security.

Network Security Overview: Introduction to Critical Infrastructure Protection, Risk Analysis, Eavesdropping and Wiretapping, Informants and Surveillance, Cyber Crime and Cyber criminals, Privacy and Cyberspace Law Privacy and Information Operations.

IPSec: 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.X.509AuthenticationService, Comparison between IPv4 and IPV6, Mobile IP.

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.

Attack Classifications: Software Flaws, Buffer Overflow, Linearization Attacks, ARP attacks, route table modification, ARP Spoofing, Denial of Service, DDoS

Network Management Systems: Trust Based Systems, Firewall and its Types, Firewall Design Principles.

Security Consideration: Encrypted Tunnels, Authentication header, WEP, key distribution protocols, Digital signatures, and Digital certificates.

Tools: Xradar, Appscanner,N map,Nessus,OpenVas,Hydra,BrutusA2.

References:

1. Douglas Stinson, "Cryptography Theory and Practice", 2nd Edition, Chapman & Hall/CRC.
2. Forouzan B. A., "Cryptography & Network Security", Tata Mc Graw Hill.
3. Stallings W., "Cryptography and Network Security", Pearson Education.

IS 504 -Penetration Testing and Auditing

L T P

4 0 –

Objective: Penetration testing is increasingly used by organizations to assure the security of Information systems and services, so that security weaknesses can be fixed before they are exposed. This course will help students in understanding the process of performing a penetration test to verify that new and existing applications, networks and systems are not vulnerable to a security risk that could allow unauthorized access to resources

Introduction: Introduction to Penetration Testing, Methodologies Penetration Testing Process, Announced /Unannounced Testing. Strategies of Penetration Testing. Guideline for security checking.

Initial Stages and Risk: Need of Penetration Testing and its Approaches, Initial stages of penetration testing, success criteria, Penetration Testing risk, testing by using third parties.

Planning and Scheduling: Purpose of Test plan, IEEE standards, Test plan phases. Defining the scope, staffing and developing project plan.

Pre–Penetration Checklist and Information Gathering: Introduction, obtain permission, prepare rule, security tools, Information gathering steps.

External Penetration Testing and Application: Steps for conducting External Penetration Testing, Application Penetration Testing

Auditing: Principles of Auditing, Auditing Tools and Techniques, Perimeter Intrusion Prevention.

References:

1. EC-Council "Penetration Testing: Procedures and Methodologies" Cengage Learning.
2. Jackson Chris, "Network Security Auditing" Cisco Press.

IS 512 -Secure Information Storage and Retrieval (Elective I)

L T P

4 0 –

Objective: The course addresses the basics of Information Storage technology and retrieval that are commonly used in industry. It will help students in attaining the ability to properly find and utilize data, which is key to success in modern business, research and education.

Complexity of Information Management: Proliferation of Data, Data Center Evolution, Managing Complexity, I/O and the five pillars of technology, Storage Infrastructure,

Evolution of Storage: Storage Systems Architecture**,** Intelligent Disk Subsystems, Physical Disks, Back End, Cache, Front End, Host Environment

Introduction to Networked Storage: Storage Networking Overview, Direct Attached Storage, Storage Area Networks, Case study – Applying SAN concepts, Network Attached Storage, Case study – Applying NAS concepts, IP SAN, CAS, Hybrid Network Storage Based Solutions/ Emerging Technologies, Case study – Applying SAN, NAS, IP SAN concepts

Introduction to Information Availability: Business Continuity Overview, Data Availability, Business Continuity – Local, Case study – Applying local information availability strategies, Business Continuity – Remote, Case study – Applying remote information availability strategies.

Disaster Recovery Managing and Monitoring: Monitoring in the Data Center, Case study – Monitoring exercise, Management in the Data Center.

Secure Information Retrieval Methods & algorithms: *Domain specific search models: Boolean model, vector space model, Probabilistic model, Apachelucene,* Semantic ACP2P, FAFSA-IRS data retrieval tool, Encryption based retrieval methods.

References:

1. Osborne Farley Marc, "Building Storage Networks", Tata McGrawHill, 2001
2. Spalding Robert, "Storage Networks: The Complete Reference", Tata Mcgraw Hill, 2003
3. NIIT, "Introduction to Information Security Risk Management", Prentice-Hall of India, 2000

IS 514 – IT SECURITY POLICIES AND PROCEDURES (Elective I)

L T P
4 0 -

Objective: This course will enable students to identify emerging security risks and implement security policies to support organizational goals. It will help in defining authorities, responsibilities, and accountabilities for Information Resources and Information Systems security.

Introduction: Why to implement information security policies, basic definitions, policy key elements, policy format. Corporate Policies, Organization-wide policies, Legal requirements, laws & regulations: The economic espionage act of 1996.

Managing the Process: Scope of work, time & cost management, planning for quality, managing human resources, creating a communication plan.

Planning & Preparation: Objectives of policies, standards& procedures, preparation activities, core & support teams, development responsibilities, key factors in establishing the development cost, milestones & responsibilities.

Developing Policies: Asset Classification Policy: Information Classification & categories, employee responsibilities, de-classification or re-classification of information, records management policy, information handling standards matrix, information classification methodologies, Authorization for access.

Developing Standards & Procedures: Overview of standards, important procedure requirements, key elements in procedure writing, procedure styles, procedure development review, and observations.

Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals.

Case studies: Corporate Policies**:** Typical Tier1 policies, Typical tier 2 policies, the company information security standards manual.

References:

1. Thomas R Peltier, Justin Peltier and John blackley, "Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996

2. Peltier R. Thomas "Information Security Policies & Procedures- A Practitioners reference" Auervach, 2nd edition.

3. Peltier R. Thomas "Information Security Policies & Procedures- Guidelines for effective Information Security Management" Auervach, 2nd edition.

4. Tipton F. Harold, Krause Micki "Information Security Management Handbook" CRC Press, 5th Edition.

5. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O' Reilly Media, 2006.

6. Merkow Mark, Breithaupt Jim " Information Security Principles & Practices, PHI, 2006

7. Whiteman E. Michael, Mattord J. Herbert "Principles of Information Security" Thomson Course Technology, 3rd Edition.

IS 516 -Mobile Application Development and Security (Elective I)

L T P

4 0 -

Objective: This course will introduce students to application development for mobile devices. Students will learn about the various constraints facing mobile application designers, both with respect to hardware and with respect to user expectation. Students will also learn how to address these constraints with techniques in implementation, software design, and user-interaction design. Additionally, students will also learn about concepts at the core of modern mobile computing

Introduction to Mobile devices and administration: Mobile devices vs. desktop devices, ARM and Intel architectures, Power Management, Screen resolution, Touch interfaces, Application deployment, App Store, Google Play, Windows Store, native applications v/s web applications.

Mobile communications: Basics and medium access control. Bluetooth, 802.11, GSM, GPRS, UMTS, LTE, Mobile networking: Naming and Mobile IP, Mobile ad-hoc networks and sensor networks, Client APIs for mobile Web Bluetooth, WiFi, SMS, Services.

Mobile operating system: Operating system structure, Constraints and Restrictions, Hardware configuration with mobile operating system, Features: Multitasking Scheduling, Memory Allocation, File System Interface, Keypad Interface, I/O Interface, Protection and Security, Multimedia features. **Case Study**: Comparing and Contrasting architectures– Android, iOS and Windows, Underlying OS (Darwin vs. Linux vs. Win 8) ,Kernel structure and native level programming , Runtime (Objective-C vs. Dalvik vs. WinRT) , Approaches to power management, Security.

Mobile application development: Phases of mobile application development, multitasking, databases, Mobile development SDLC: Process of development, Native V/S Cross platform development, and different development environments **Case Study**: Study of cross-platform development tools like Worklight, PhoneGap, Appcelerator, RhoMobile, Widgetpad, Xamarin.

Mobile device security: Mobile malware, Device protections, Bluetooth security, Proximity-based authentication, **Case Study**: iOS "Jailbreaking", Android "rooting" and Windows' "defenestration".

References:

1. Jochen Schiller, Mobile Communications, 2nd ed., Addison-Wesley, 2003
2. John Krumm, Ubiquitous Computing Fundamentals, CRC Press, 2010
3. Alan Cooper, Robert Reimann, and Dave Cronin , About Face 3: The Essentials of Interaction Design, Wiley, 2007
4. Steven Hoober and Eric Berkman , Designing Mobile Interfaces , O'Reilly, 2011
5. Reto Meier , Professional Android 4 Application Development , Wiley, 2012
6. James Steele and Nelson To , The Android Developer's Cookbook: Building Applications with the
7. Android SDK , Addison-Wesley, 2010
8. Yaghmour Karim ,."Building Embedded Linux Systems", O'Reilly Media
9. Kyrnin Jennifer, "Sams Teach Yourself HTML5 Mobile Application Development in 24 Hours", Sams Publishing, 2011.
10. Oehlman Damon, Blanc Sébastien, "Pro Android Web Apps: Develop for Android using HTML5, CSS3 & JavaScript", Apress, 2011.
11. Burd, "Android Application Development All-in-One For Dummies", John Wiley & Sons, 2011.
12. Lee Henry, Chuvyrov Eugene, "Beginning Windows Phone App Development", Apress, 2012.

IS 515 -VIRTULISATION AND CLOUD SECURITY (Elective II)

L	T	P
4	0	-

Objective: This course covers a series of current cloud computing technologies, including technologies for Virtualization, Infrastructure as a Service, Platform as a Service, Software as a Service, and Physical Systems as a Service. Cloud computing adoption and diffusion are threatened by unresolved security issues that affect both the cloud provider and the cloud user. This subject will help in showing how virtualization can increase the security of cloud computing, by protecting both the integrity of guest virtual machines and the cloud infrastructure components.

Introduction: Overview, Roots of Cloud Computing, Layers and Types of Cloud, Desired Features of a Cloud, Benefits and Disadvantages of Cloud Computing, Cloud Infrastructure Management, Infrastructure as a Service Providers, Platform as a Service Providers, Challenges and Risks, Assessing the role of Open Standards, Federation in the Cloud, Presence in the Cloud, Privacy and its Relation to Cloud-Based Information Systems, Security in the Cloud, Common Standards in the Cloud, End-User Access to the Cloud Computing

Cloud Architecture, Services and Applications:
Exploring the Cloud Computing Stack, Connecting to the Cloud, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), SaaS Vs. Paas, Using Paas Application Frameworks, Software as a Service, Identity as a Service, Compliance as a Service

Abstraction and Virtualization:
Introduction to Virtualization Technologies, Load Balancing and Virtualization, Understanding Hyper visors, Understanding Machine Imaging, Porting Applications, Virtual Machines Provisioning and Manageability Virtual Machine Migration Services, Virtual Machine Provisioning and Migration in Action, Provisioning in the Cloud Context, Cloudsim, Apache cloudstack, openNebula

Managing & Securing the Cloud:
Administrating the Clouds, Cloud Management Products, Emerging Cloud Management Standards, Securing the Cloud, Securing Data, Establishing Identity and Presence

Cloud Middleware:
Introduction to Cloud Stack, Open Stack, IBM Smart Cloud, Microsoft Azure, Google cloud services, Amazon webservices

References:

1. Rittinghouse John W. and Ransome James F., "Cloud Computing Implementation, Management and Security", 2010, CRC Press, Taylor & Francis Group, Boca Raton London New York.
2. Mendoza Alfredo, "Utility Computing Technologies, Standards, and Strategies", Artech House INC, 2007.
3. Bunker and Thomson Darren, "Delivering Utility Computing", 2006, John Wiley & Sons Ltd.
4. Reese George, "Cloud Application Architectures", O'reilly Publications, 2009.

IS 517 -Cyber Incident Handling and Reporting (Elective-II)

L T P

4 0 -

Objective: Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. This course will assist students in understanding the need of establishing computer security incident response capabilities and handling incidents efficiently and effectively. This course will provides guideline for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident

Introduction: Concept of Computer security Incident, Types of Incident-denial of service-malicious code, unauthorized access, Inappropriate Usage. Need for incident Response, Policies, Plans and Procedure related to incident Response, Incident reporting organization.

Incident Response Team structure: Introduction to Response Team, Team Models, Staffing Models, Incident Response Personnel, Incident Response Team Services, Incident Response Life cycle- Preparation, Detection and Analysis, Containment Eradication and Recovery, Post - Incident Activity

Incident Detection and Analysis: Profiling, Behaviors, Centralized logging , Event Correlation, Diagnosis matrix , Incident Analysis – Incident Documentation ,incident Prioritization, Incident Response SLA Matrix , Incident Notification.

Handling denial of Service Incident: DoS attacks, Concept of DDoS , Types of DDoS- Reflector Attacks, Amplifier Attacks and Floods, Prevention of DDoS- Incident Handling Preparation, Containment Strategy, Handling Unauthorized Access Incidents, Malicious Code Incidents.

Handling Multiple Components Incidents: Preparation, Detection and Analysis, Containment Eradication and Recovery

References:

1. Barbara Guttman, Roback Edward, " An introduction to computer security: the NIST handbook" , NIST Special Publication 800-12
2. Lucas Julie, Moeller Brian, " The effective incident response team" , Addison-Wesley Professional
3. Whitman Michael E., Mattord Herbert J. , " Principles of incident response and disaster recovery" , Thomson Course Technology, 2007
4. Breaches, Eugene Schultz E., Shumway Russell, " Incident response: a strategic guide to handling system and network security" , New Rider Publishing-2002
5. Mandia , "Incident Response & Computer Forensics", Tata McGraw-Hill Education-2006

IS 519 - DATABASE SECURITY AND GOVERNANCE (Elective II)

L T P

4 0 -

Objective: With the advancement of technology and ability to handle big data bases effectively and securely, this course has become the need of the hour. The student will able to learn various techniques of securing as well as recovering data.

UNIT I

Overview of Database Security and governance Difference between logging and monitoring, Three guiding principles to improve data security and compliance Understanding holistic database security, 8 steps to successfully securing enterprise data sources, Secure Enterprise Data and Ensure Compliance, Auditing Categories and what to audit, Ten Database Activities Enterprises Need to Monitor

UNIT II

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 III

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 IV

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

UNIT – V

Distributed Systems: Distributed Systems Security. Security in Engineering: Secure Development Lifecycle Processes - A Typical Security Engineering Process – Security Engineering Guidelines and Resources. Common Security Issues and Technologies: Security Issues, Common Security Techniques.

References:

1. Lewis Philip M., Bernstein Arthur and Kifer Michael, "Databases and Transaction Processing: An Application-Oriented Approach", Addison-Wesley, 2002.
2. Elmasri R. and Navathe S.B., "Fundamentals of Database Systems", 3rd Edition, Addison Wesley, 2004.
3. Silberschatz Abraham, Korth Henry. F. and Sudharsan S., "Database System Concepts", 4th Edition, Tata McGraw Hill, 2004.
4. Ramakrishnan Raghu and Gehrke Johannes, "Database Management Systems", 3rd Edition, TMH, 2003.
5. Ben Ron, "Implementing Database Security and Auditing"
6. Ben Ron, "How to Secure and Audit Oracle 10g and 11g"
7. Ben Ron, "Definitive 454-page text for security, risk management & database pros"

IS 508 -Network Security Lab

L	T	P
-	-	4

The Students are required to implement the applications based on IS – 502
To use Xradar & AppScan tools.

IS 525 -FORENSICS AND CYBER LAWS (Elective-III)

L T P

4 0 -

Objectives: The advancement of internet in diversifies fields not only proves its effectiveness but also brings various crimes and other ill-effects associated with it. So, this course will make students aware about these and also give an in-depth knowledge of various laws and acts available in India and globally to tackle it.

Computer and Cyber Forensic Basics- Introduction to Computers, Computer History, Software, Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Basic Computer Terminology, Internet, Networking, Computer Storage, Cell Phone / Mobile Forensics, Computer Ethics and Application Programs, Cyber Forensic Basics- Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology.

Data and Evidence Recovery- Introduction to Deleted File Recovery, Formatted Partition Recovery, Data Recovery Tools, Data Recovery Procedures and Ethics, Preserve and safely handle original media, Document a "Chain of Custody", Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Recover Swap Files/Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Tool Kit (FTK) etc, Use computer forensics software tools to cross validate findings in computer evidence related cases.

Cyber Crimes and Cyber Laws- Introduction to IT laws & Cyber Crimes – Internet, Hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits, and Cyber
Security etc.

Cyber Forensics Investigation- Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking.

Cyber Security- Introduction to Cyber Security, Implementing Hardware Based Security, Software Based Firewalls, Security Standards, Assessing Threat Levels, Forming an Incident Response Team, Reporting Cyber crime, Operating System Attacks, Application Attacks, Reverse Engineering & Cracking Techniques and Financial Frauds.

References:

1. Russell Debby and Gangemi G.T, "Computer Security Basics (Paperback)", 2ndEdition, O' Reilly Media, 2006.
2. Peltier Thomas R., "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3. Knapp Kenneth J., "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
4. Peltier Thomas R, Peltier Justin and blackley John, "Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996
5. Rosenoer Jonathan, "Cyber law: the Law of the Internet", Springer-Verlag, 1997.

IS 527 -Reverse Engineering Malware (Elective-III)

L T P

4 0 -

Objectives: The objective of this course is to familiarize students with the practice of reverse engineering suspicious files by utilizing static and dynamic tactics, techniques, and procedures in order to gain an understanding as to what impact the suspicious file may have on a particular computer system when executed.

Introduction to Malware: Analysis and Trends, Malware taxonomy and characteristics

Understanding Malware Threats: Malware Indicators, Malware Classifications, Examining ClamAV signatures, creating custom ClamAV databases.

Fundamentals of Malware Analysis (MA): Reverse Engineering Malware (REM) Methodology, Introduction to key MA tools and techniques, Behavioural Analysis vs. Code Analysis

Resources for Reverse-Engineering Malware (REM) :Initial Infection Vectors and Malware Discovery, Sandboxing Executables and Gathering Information From Runtime Analysis, The Portable Executable (PE32) File Format, Identifying Executable Metadata, Executable Packers and Compression, and Obfuscation, Techniques

Utilizing Software Debuggers to Examine Malware, Analyzing Malicious Microsoft Office and Adobe PDF Documents, Analyzing Malicious Browser---based Exploits, Automating the Reverse Engineering Process

References:

1. Ligh Michael, Adair Steven, Hartstein Blake, and RichardMatthew, "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code", First Edition (2010), Wiley Publications
2. Skoudis Ed and Zeltser Lenny, "Malware: Fighting Malicious Code" (2003). Prentice Hall Publications
3. Malin Cameron H., Casey Eoghan, and James M. Aquilina, "Malware Forensics: Investigating and Analyzing Malicious Code" (2008), Syngress Publications.
4. Eilam Eldad, "Reversing: Secrets of Reverse Engineering" (2005), Wiley

IS 529 -Intrusion Detection Analysis (Elective-III)

L T P

4 0 -

Objectives: Intrusion detection systems are an important component of defensive measures protecting computer systems and networks from abuse. This course will led students in analyzing the importance of it and also gives an insight of its architecture and implementation.

Introduction: IDS concepts and definitions, intrusions and their Phenomenology, detection method, analysis schemes.

Architecture: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Architecture, IDS and IPS internals

Implementation and deployment: Internet security system's Real Secure, Cisco secure IDS, Snort, NFR security

Firewalls: Firewall Planning and Design, Developing a Security Policy, Firewall Configuration Strategies, Packet Filtering, Working with Proxy Servers and Application-Level Firewalls, Authenticating Users, Encryption and Firewalls.

Security and IDS management: Data Correlation, Incident response, Policy and Procedures, Laws standards and organizations, security business issues, future of Intrusion Detection and Prevention

Advanced topics: Catching intruders in the act by recognizing the characteristics of various kinds of attacks in real time, both manually and with the use of filters and other automated systems such as snort; techniques for identifying security weaknesses and minimizing false security alarms.

References:

1. Endorf Carl, Schultz Eugene, and Mellander Jim, "Intrusion Detection & Prevention", Tata McGrawHill, 2006
2. Kruegel Christopher, Valeur Fredrik, Vigna Giovanni, "Intrusion Detection and Correlation: Challenges and Solutions", Springer 2005, Volume 14
3. Bace Gurley Rebecca, "Intrusion Detection", New Riders
4. Trost. Ryan, "Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century", Addison-Wesley 2010.

IE 513- ORGANIZATION THEORY AND BEHAVIOUR

L T P

4 0 -

Objective: Understanding the meaning of Organizational behavior, fundamental concepts connected with Organizational behavior, basic approaches of Organizational behavior, framing the study of Organizational behavior, goals of organizational behavior, knowing the importance of Organizational behavior for the managers.

Concept of organization and management: Development of management thought; different theories of management. Japanese management. Planning and planning process. Decision making. MBO, Decentralization, Span of management, Delegation. Line staff and functional relationship. Beurocratic organization.

Role of behavioral sciences in organization: Individual behaviour, different theories of motivation. Interpersonal and group behaviour, transactional analysis and group dynamics. Importance of human relations. Controlling and directing human behaviour in organization. Leadership, theories of leadership and leadership styles, managerial grid, organizational conflicts, and organizational effectiveness. Communication significance, process and variables.

Concept of personal management and industrial relations: role and scope. Planning personnel functions – Human resource development, functions and operations of personnel department, employee's selection, recruitment and training. Job description and analysis, career planning, transfers and promotions. Compensation planning, wages and salary administration. Concept of workers participation in management.

Reference Books:

1. Newstorm, J.W & Keith, Davis Organization Behaviour Tata McGraw Hill 1995
2. Ahuja, K.K Organization Behaviour Kalyani Publisher 1990
3. Luthans, F. Organization Behaviour Tata McGraw Hill 1995
4. Prasad, L.M Organization Behaviour Sultan Chand & Sons 1996
5. Tripthi, P.C Personnel Mgt. & Behaviour Sultan Chand & Sons 1994
6. Flippo, E.B Personnel Management McGraw Hill 1984
7. Prasad, Ladies & Bannerjee Management of Human Resources Sterling Pub 1994

SS- 522 Total Quality Management

L T P

4 0 -

Objective: This course is designed to give students fundamentals of Total Quality, Management with emphasis on contemporary quality planning, control and management approaches, implementations and criticisms.

Introduction: Quality – Basic concepts, dimensions, economics of quality, quality Gurus, TQM: Definition, evolution, journey from inspection to TQM, comparison at different stages, dimensions of TQM,TQM viewpoints, reasons for adopting TQM.

Introspection to TQM environment: Sphere of TQM, components of TQM, TQM – Managing Total Quality, Factors affecting TQM environment, Classification and interaction among factors, Researchers' viewpoint, TQM as a system, steps in TQM implementation, Roadblocks in TQM implementation, Reasons for TQM Failure.

Role of soft options in TQM: Hard vs. Soft factors, Role and expectation of employer, employee, customer and supplier from organization and vice versa. Human factors in TQM, Role of top management commitment, work culture, motivation, coordination, attitude, innovation.

Quality initiatives in organizations: Role of tools and techniques in TQM, Classification of tools and techniques – Problem identification, Data analysis, Graphical, Creativity, Companywide. Brief description of Quality awards – MBNQA, Deming award, European quality award, Australian Quality award.

TQM Effectiveness: Impact of TQM, Need and difficulty in measuring TQM effect, Parameters governing effect of TQM and the attributes thereof.

Suggested Readings/ Books:

1. Besterfield, "Total Quality Management", Pearson Education India, 2011.
2. Logothetis, "Managing For Total Quality: From Deming To Taguchi And SPC", PHI, 2002.
3. Armand Vallin Feigenbaum, "Total quality control", McGraw-Hill, 2007.
4. John S. Oakland, Peter Morris, "TQM: A Pictorial Guide for Managers", Butterworth-HeinemannLimited, 1997.

SS-524 Product Design and Management

L T P

4 0 -

Objective: At the completion of this course, the student should be able to examine the design and performance of supply networks and processes in different business contexts. Students develop capabilities in logistics, digital coordination for supply chain integration, inventory management; risk pooling, procurement, product and process design, and international supply chain management.

Introduction: Characteristics of successful product development, Design and development of products, duration and cost of product development, the challenges of product development.

Development Processes and Organizations: A generic development process, concept development: the front-end process, adopting the generic product development process, the AMF development process, product development organizations, the AMF organization.

Product Planning: The product planning process, identify opportunities. Evaluate and prioritize projects, allocate resources and plan timing, complete pre project planning, reflect all the results and the process.

Identifying Customer Needs: Gather raw data from customers, interpret raw data in terms of customer needs, organize the needs into a hierarchy, establish the relative importance of the needs and reflect on the results and the process.

Product Specifications: What are specifications, when are specifications established, establishing target specifications, setting the final specifications.

Concept Generation: The activity of concept generation clarify the problem, search externally, search internally, explore systematically, reflect on the results and the process.

Concept Selection: Overview of methodology, concept screening, and concept scoring,

Concept Testing: Define the purpose of concept test, choose a survey population, choose a survey format, communicate the concept, measure customer response, interpret the result, reflect on the results and the process.

Product Architecture: What is product architecture, implications of the architecture, establishing the architecture, variety and supply chain considerations, platform planning, related system level design issues.

Industrial Design: Assessing the need for industrial design, the impact of industrial design, industrial design process, managing the industrial design process, assessing the quality of industrial design.

Design for Manufacturing: Definition, estimation of manufacturing cost, reducing the cost of components, assembly, supporting production, impact of DFM on other factors.

Prototyping: Prototyping basics, principles of prototyping, technologies, planning for prototypes.

Product Development Economics: Elements of economic analysis, base case financial mode,. Sensitive analysis, project trade-offs, influence of qualitative factors on project success, qualitative analysis.

Managing Projects: Understanding and representing task, baseline project planning, accelerating projects, project execution, postmortem project evaluation.

Suggested Readings/ Books:

1. A C Chitale, R C Gupta, "Product Design and Manufacturing", PHI Learning Pvt. Ltd., 2007.
2. Ulrich, Steven D. Eppinger, "Product Design and Development", Tata McGraw-Hill Education, 2003.
3. Butterworth Heinmann, "New Product Development", Oxford UCI, 1997.
4. Geoffery Boothroyd, Peter Dewhurst and Winston Knight, "Product Design for Manufacture and Assembly", CRC Press, 2010.

SS-526 Enterprise Resource Planning

L T P

4 0 -

Objective: The ERP will develop and implement curricula in the students that bring ERP concepts and business disciplines hands-on exposure to how enterprise-wide information systems support the planning and management of business processes. It also provides the study about the connection between all the business disciplines in the real world and how ERP systems support the planning and management of business processes.

Introduction to ERP: An Overview, Enterprise – An Overview, Benefits of ERP, ERP and Related Technologies, Business Process Reengineering (BPR), Data Warehousing, Data Mining, OLAP, SCM.

ERP Implementation: Lifecycle, Implementation Methodology, Hidden Costs, Organizing the Implementation, Vendors, Consultants and Users, Contracts with Vendors, Consultants and Employees, Project Management and Monitoring.

Business modules: ERP Package, Finance, Manufacturing, Human Resources, Plant Maintenance, Materials Management, Quality Management, Sales and Distribution.

ERP Market: SAP AG, Peoplesoft, Baan, JD Edwards, Oracle, QAD, SSA.

Present and Future: Turbo Charge the ERP System, EIA, ERP and e-Commerce, ERP and Internet, Future Directions.

Suggested Readings/ Books:

1. Joseph A Brady, Ellen F Monk, Bret Wagner, "Concepts in Enterprise Resource Planning", Thompson Course Technology, USA, 2001.
2. Vinod Kumar Garg and Venkitakrishnan N K, "Enterprise Resource Planning – Concepts and Practice", PHI, New Delhi, 2003
3. Alexis Leon, "ERP Demystified", Tata McGraw Hill, New Delhi, 2000.
4. Ravi Shankar, S. Jaiswal, "Enterprise Resource Planning", Galgotia, 1999.

SS-528 IT Strategy and Management

L T P

4 0 -

Objectives: This course gives an in-depth study of the information technology as a strategic resource, the need for a strategic approach for its management, and the necessity of its alignment with business strategy. It explains how to prepare an effective plan for the implementation of information strategy.

Business Strategy: Introduction, Business Strategy: Principles, Challenges & opportunities, IT Strategy: Application Strategy, Technological & IT Management Strategy, Stages of IT Strategy development & Implementation, Business & IT alignment: Challenges, 3D framework, Tools.

Strategic IT Planning: Definition, motivations, SITP process , Difficulties in developing & executing SITP, SITP Approaches, Resource Planning: People plans, Financial plans, Administrative plans, technology plan, Implementation consideration of SITP.

Enterprise IT Architecture & IT Applications Strategy: Introduction, why EITA? Advantages of defining EITA, Contents of a typical EITA, IT Applications Strategy: Introduction, In-House & subcontracting, COTS package selection lifecycle, COTS implementation strategy.

Technology & Program Management strategy: Introduction, Technology management strategy framework, motivations, constituents of technology management strategy, prevalent technology reference architecture framework & standards, Strategic view of project, program & portfolio management, program management versus project management, PMO: Benefits, Qualities, types & management of PMO, Success factors of PMO.

IT Service Management Strategy: Introduction, Information Technology Infrastructure Library: overview, service support processes, service delivery, service lifecycle, stages of Implementation.

IT Sourcing Strategy & planning IT investment: Outsourcing, Need of Outsourcing, Associated Risks & their minimization, Strategic & Generic Sourcing, variant of Outsourcing, Success with outsourcing, IT Business value framework, critical factors for IT Benefits, measuring benefits from IT.

Strategy for IT Challenges & Cyber Crime Prevention: IT strategy Implementation, Barriers of change, managing change, driving the change to steering Committee, acquire & Enhance new skill set, case studies, computer ethics, e-ethics code, IPR, copyright laws in India, overviews of cyber crimes, challenges in enacting laws in cyber space, Information Technology act 2000, WIN- WIN model.

Reference Books:

1) Dubey Shankar Sanjiba "IT Strategy & Management" PHI 2011, 2nd Edition.

2) Brown V. Carol, W. Daniel, Martin E. Wainright "Managing Information Technology" PHI 7th Edition.

3) Hanschke Inge "Strategic IT Management" Springer 2010

4) Eng K. Chew, Petter Gottschalk "Information Technology Strategy and Management: Best Practices, IGI Global Snippet, 2009