# Punjab Technical University, Jalandhar
## Study Scheme Batch 2013
### M.Tech (Information Technology & Cyber Warfare)

#### Schedule of Teaching
<table>
<thead>
<tr>
<th>Lecture</th>
<th>Tutorials</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Schedule of Examination
<table>
<thead>
<tr>
<th>Time (Hrs)</th>
<th>Theory Marks</th>
<th>Sessional Marks</th>
<th>Viva Marks</th>
<th>Total Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **All theory Subjects**: 3 Hrs, 100 Marks, 50 Marks, Total 150 Marks
- **Projects**: 50 Marks, 100 Marks
- **Seminar**: 100 Marks, 100 Marks
- **Dissertation**: Satisfactory/Not Satisfactory

#### SEMESTER-I

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>L</th>
<th>T</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITCW-501</td>
<td>Advance Topics in Software Engineering</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-503</td>
<td>Computer Security, Audit Assurance and Risk Management</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-505</td>
<td>Advanced Internet &amp; Web Technology</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>IT-506</td>
<td>Research Methodologies</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-507</td>
<td>Data Warehousing &amp; Data Mining</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-509</td>
<td>Advanced IT and Cyber Warfare Lab-I</td>
<td>-</td>
<td>-</td>
<td>4</td>
</tr>
</tbody>
</table>

#### SEMESTER-II

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>L</th>
<th>T</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITCW-502</td>
<td>Forensics and Cyber Law</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-504</td>
<td>Applied Cryptography</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-506</td>
<td>Ethical Hacking</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-508</td>
<td>Wireless &amp; Mobile Security</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-510</td>
<td>Intrusion Detection &amp; Analysis</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-512</td>
<td>Advanced IT and Cyber Warfare Lab-II</td>
<td>-</td>
<td>-</td>
<td>4</td>
</tr>
</tbody>
</table>

#### SEMESTER-III

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>L</th>
<th>T</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITCW</td>
<td>Elective-I</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW</td>
<td>Elective-II</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-531</td>
<td>Project</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>ITCW-533</td>
<td>Seminar</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
</tbody>
</table>

#### SEMESTER-IV

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITCW-514</td>
<td>Dissertation</td>
</tr>
</tbody>
</table>
ELECTIVE-I, II *

ITCW-513 Biometric Security.
ITCW-515 Security Assessment and Verification.
ITCW-517 Security Threats.
ITCW-519 Steganography and Digital Watermarking.
ITCW-521 Distributed Systems Security.
ITCW-523 Securing Windows & Linux.
ITCW-525 Cyber Incident Handling & Reporting.
ITCW-527 Web Service Security.
ITCW-529 Virtualization and Cloud Security.

* The student will have to opt any two subjects from the above list of electives.
Semester-I
ITCW- 501 ADVANCE TOPICS IN SOFTWARE ENGINEERING

Objective: The course will stress on concepts of modern approaches to software Formal design methods, Reengineering systems, object oriented designs, software quality and modeling structures for secure software designs

Formal Methods: Basic concepts, mathematical preliminaries, Applying mathematical notations for formal specification, formal specification languages, using Z to represent an example software component, the ten commandments of formal methods, formal methods- the road ahead


REFERENCES
Objective: The course will stress on concepts of Security Threats, Cryptography Systems encryption techniques, security policies and auditing assurance for the aim of further security protocols design and improvements.


Risk management and security planning: Risk management Process Overview on 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

REFERENCES
ITCW – 505 ADVANCED INTERNET & WEB TECHNOLOGY

L    T    P
3    1    -

PREREQUISITES: Computer Networks & Data Communication.

OBJECTIVES: After this course students should have general knowledge on how the Internet works and have basic network programming skills. They will be able to understand technical papers in this area. More importantly, they will think like network people.

Introduction: Transmission Control Protocol, User Datagram Protocol, and selected topics on Internet infrastructure and applications such as: Internet Quality of Service (eg Integrated Services Model, Resource Reservation Protocol, Differentiated Services)


Internet Application: Datagram Congestion Control Protocol; Electronic commerce (the Internet Open Trading Protocol); Web services; Mobile IP; Mobile Data (eg the Wireless Application Protocol, Multimedia Messaging Service); Real Time Protocol; Multimedia over Packet Networks (ITU-T Recommendations H.323, H.245);

Application Oriented Services: Hypertext Transfer Protocol (HTTP, HTTPS), Electronic Mail; Domain Name Service, File Transfer, Middleware:-Object Management Architecture, object request brokers (CORBA, OLE/COM), services (trading, naming, event, transaction, security), and interorb protocols. HTML5.0, CSS, JSP


REFERENCES:

Additional References
1 Tanenbaum, "Computer Networks," 4th edition
3 Comer, "Internetworking with TCP/IP, Volume 1," 4th edition
4 Bertsekas and Gallager, "Data Networks," 2nd edition
OBJECTIVES: Provides in depth knowledge about the systematic process of collecting and analyzing Information (data) in order to increase our understanding of the phenomenon with which we are concerned or interested.

Nature and Objectives of research: Methods of research: historical, descriptive and experimental. Study and formulation of research problem. Scope of research and formulation of hypotheses; Feasibility, preparation and presentation of research proposal.

Introduction to statistical analysis: Measures of central tendency and dispersion: mean, median, mode, range, mean deviation and standard deviation.

Regression and correlation analysis: Probability and probability distributions; Binomial, Poisson, Geometric, Negative binomial, Uniform, Exponential, Normal and Log-normal distribution. Basic ideas of testing of hypotheses; Tests of significance based on normal, T and Chi-square distributions. Analysis of variance technique.

Design of experiments: Basic principles, study of completely randomized and randomized block designs. Edition and tabulation of results, presentation of results using figures, tables and text, quoting of references and preparing bibliography. Use of common softwares like SPSS, Mini Tab and/or Mat Lab. For statistical analysis.

REFERENCES:

Additional References
OBJECTIVES: The course focuses on developing strategies to enhance end-user access to a variety of data along with gaining expertise in developing seamless commercial business applications, specifically concentrating on customer relationship management systems.

Introduction to data warehouse: Need for data warehousing: Escalating need for strategic information, Failures of past decision-support systems, operational versus decision-support systems, data warehouse building blocks: Defining features, data warehouses and data marts, overview of the components, and metadata in the data warehouse. Defining the business requirements: Dimensional analysis, information packages: a new concept, requirements gathering methods, KDD.

Principles of dimensional modeling: Objectives, From requirements to data design, the STAR schema, STAR Schema Keys, Advantages of the STAR Schema, Dimensional Modeling: Updates to the Dimension tables, miscellaneous dimensions, the snowflake schema, aggregate fact tables, and families of STARS.

OLAP in the Data Warehouse: Demand for Online analytical processing, need for multidimensional analysis, fast access and powerful calculations, limitations of other analysis methods, OLAP is the answer, OLAP: definitions and rules, OLAP characteristics, major features and functions, general features, dimensional analysis, what are hyper cubes? Drill-down and roll-up, slice-and-dice or rotation, OLAP models, overview of variations, the MOLAP model, the ROLAP model, ROLAP versus MOLAP, OLAP implementation considerations

Data Mining Basics: What is Data Mining, Data Mining Defined, The knowledge discovery process, OLAP versus data mining, data mining and the data warehouse.

Data Mining Techniques: Cluster Analysis & detection (Partitioning Method, Hierarchical Method, Density Based & Grid Based) classification & prediction (decision trees, memory-based reasoning, link analysis, Linear & Non Linear Regression, neural networks, genetic algorithms), Mining data Stream, Mining Time Series Data, Spatial Data Mining.

Data Mining Application: Data Mining Applications, Benefits of data mining, applications in retail industry, applications in telecommunications industry, applications in banking and finance, data mining for biological data analysis, scientific application, intrusion detection.

Recommended Books:

Reference Books:
2. Kamber and Han, “Data Mining Concepts and Techniques”, Hartcourt India P. Ltd.,
3. A Guide to Data Warehousing - Hocht
4. Data Warehousing in Real World - Anahory
5. Data Mining - Addisiaans (Addison Wesley)
Laboratory Work

To impart practical experiments relevant to the courses offered in scheme with orientation towards IT & Cyber Warfare
Semester-II

Emergence of information based society, economic, administration, social, dependence of use of information, accession, threats, civil society and global society

Fundamentals: Overview of computer forensics and Investigative Techniques, Computer forensic tools, activities of forensic investigations and testing methodology,


Role of Computers and Internet in Cyber crime penetration and prevention : Computer as witness, evidence, act, defining evidence, computer forensics, computer storage, media of electric record for use of course of law

Cyber Security: The concept of cyber security, meaning, scope and the frame work, basic structure, development, and management, Rules, Regulations, Act, Legislation, Meaning, Scope, Difference between Rules

Need for a Cyber Act: The Indian Context, Need for a Cyber Act, Information Technology Act, its Scope and further Development, Information Technology Act ( Amendment), coverage of Cyber Security and Cyber Crime Indian cyber Laws vs. cyber laws of U.S.A, similarities, scope and coverage, Effectiveness

Recommended Books:
UNIT I

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

UNIT IV

UNIT V

REFERENCES
UNIT I
Casing the Establishment, What is footprinting, Internet Footprinting, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services, Case study, Network Security Monitoring

UNIT II

UNIT III

UNIT IV

UNIT V

REFERENCES:
UNIT I

UNIT II

UNIT III

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
Global Mobile Satellite Systems; case studies of the IRIDIUM and GLOBALSTAR systems. Wireless Enterprise Networks: Introduction to Virtual Networks, Blue tooth technology, Blue tooth Protocols. Server, side programming in Java, Pervasive web application architecture, Device independent example application

UNIT VI
Apple iPhone: iPhone Development environment, Security testing, Application format, permissions and user control, Local data storage, Networking, Push notifications.

Windows Mobile Security: Introduction to Windows Mobile platform, Kernel Architecture, Development and security testing, Permissions and user control, Local data storage, Networking


REFERENCES
Introduction and an Overview of Intrusion Detection systems: Introduction to networking basic concepts, Introduction about intrusion detection systems, Purpose and Scope of intrusion detection systems, Need of intrusion detection systems, applications of intrusion detection systems, Firewalls and intrusion detection systems, Challenges to Intrusion Detection Systems, Sample IDS Deployment examples.

Intrusion Detection Systems and Associated Methodologies: Uses of Intrusion detection technologies, Key Functions of Intrusion detection systems, Common Detection Methodologies, Signature Based Detection, Anomaly Based Detection, stateful protocol analysis, Types of Intrusion detection technologies

Intrusion detection Technologies and components: Components and Architecture, Typical Components Network Architectures, Security capabilities, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities Prevention Capabilities and its implementation, Deploying IDS.


Using and Integrating Multiple Intrusion Detection Systems Technologies: The Need for Multiple IDS technologies, Integrating Different IDS Technologies, Direct IDS Integration Indirect IDS Integration, Other Technologies with IDS Capabilities, Network Forensic Analysis Anti, Malware Technologies, Honeypots


Recommended Book
ITCW-512  Advanced IT and Cyber Warfare Lab-II

Laboratory Work

To impart practical experiments relevant to the courses offered in scheme with orientation towards Security & Cyber Warfare
Semester-III - Electives
MOLECULAR BIOLOGY AND BIOLOGICAL CHEMISTRY:
The genetic material, Gene structure and information content, Protein structure and function, The nature of chemical bonds, Molecular biology tools, Genomic information content.

DATA SEARCHES AND PAIRWISE ALIGNMENTS: Dot plots, Simple alignments, Scoring, Gaps, Scoring matrices, The Needleman and Wunsch algorithm, Local and global alignments, Database searches, Multiple sequence alignments.

SUBSTITUTION PATTERNS: Patterns of substitutions within genes, Estimating substitution numbers, Variations in substitution rates between genes, Molecular clocks, Evolution in organelles.

DISTANCE-BASED METHODS OF PHYLOGENETICS: History of molecular phylogenetics, Advantages to molecular phylogenies, Phylogenetic trees, Distance matrix methods, Maximum likelihood approaches, Multiple sequence alignments.

CHARACTER-BASED APPROACHES TO PHYLOGENETICS: Parsimony, Inferred ancestral sequences, Strategies for faster searches, Consensus trees, Tree confidence, Comparison of phylogenetic methods, Molecular phylogenies.


PROTEIN FOLDING: Polypeptide composition, Secondary structure, Tertiary and quaternary structure, Protein folding, Structure prediction.

BIO SECURITY: Biosafety, genetic modification, Biological risk management, Biosecurity and Biosafety Associations, World Health Organization and its roles, biosafety and biosecurity activities, Role of government during times of public health crisis, Global Governance and biosecurity, Biotechnology as it relates to biosecurity.

REFERENCES
2. Computational approaches in Cheminformatics and Bioinformatics edited by Dr. Rajarshi Guha and Dr. Andreas Bender, Wiley Publishing., 2010.
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, biometric matching methods, Accuracy in biometric systems.

UNIT II

UNIT III
Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description—classification, keyboard and 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: Physiological, Behavioral and multifactor biometrics in identification systems.

REFERENCES
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

UNIT III
Business process evaluation: Technology evaluation, Risk analysis, Risk mitigation.

UNIT IV

UNIT V
Information security standards: Information security Legislation, formal security verification, security verification with SSL.

REFERENCES
UNIT I
**Network Threats:** Active/ Passive, Interference, Interception, Impersonation, Spam’s , Ad ware, Spy war, covert channels, Backdoors, Bots – IP, Spoofing, ARP spoofing, Session Hijacking, Sabotage, Internal treats, Environmental threats, Threats to Server security.

UNIT III

UNIT IV
**Security Elements:** Authorization and Authentication, types, policies and techniques, Security certification, Security monitoring and Auditing, Security Requirements Specifications, Security Polices and Procedures, Firewalls, IDS, Log Files, Honey Pots

UNIT V
**Access control:** Trusted Computing and multilevel security, Security models, Trusted Systems, software security issues, Physical and infrastructure security, Human factors, Security awareness, training, Email and Internet use policies.

REFERENCES
UNI T 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.

UNI T 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.

UNI T 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.

UNI T 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

UNI T V

**Fingerprints:** Examples, Classification, Research history, Schemes, Digital copyright and Watermarking, Conflict of copyright laws on the internet.

REFERENCES

5. Digital Watermarking and Steganography (The Morgan Kaufmann Series in Multimedia Information and Systems) Ingemar Cox (Author), Matthew Miller (Author), Jeffrey Bloom (Author), Jessica Fridrich (Author), Ton Kalker (Author), 2011
UNIT – I

UNIT – II
**Host-level Threats and Vulnerabilities:** Transient code Vulnerabilities, Resident Code Eavesdropping, Job Faults. Infrastructure-Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities, Grid Computing Threats and Vulnerabilities, Storage Threats and Vulnerabilities, Overview of Infrastructure Threats and Vulnerabilities.

UNIT - III

UNIT - IV
**Host Level Solutions:** Sandboxing, Virtualization, Resource Management, Proof Carrying, Code, Memory Firewall, Antimalware, Infrastructure, Level Solutions, Network Level Solutions, Grid-Level Solutions, Storage Level Solutions, Application Level Solutions, Application Level Security Solutions.

UNIT - V

**REFERENCES**

Cryptography: Basic Cryptography Concepts, PKI Concepts, Implementing PKI and Certificate Management,


Security Assessments and Audits: Vulnerability Assessments and Testing, Monitoring, Logging and Auditing


Recommended Books:
4. Linux in a Windows World Leverage Linux to make Windows more secure, responsive & affordable, 2009

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


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

Recommended Books
2. The effective incident response team, Julie Lucas, Brian Moeller, Addison-Wesley Professional
5. Incident Response & Computer Forensics, Mandia, Tata McGraw-Hill Education-2010
Introduction to Web Service Technologies
Introduction to web services, Security for Web Services and Security Goals, Need of security and Privacy in web services, applications of web service security, SOA and Web Services Principles, Web Services Architecture, Web Services Technologies and Standards, SOAP, Web Services Description Language (WSDL), Service Discovery, Universal Description, Discovery, Integration (UDDI) Considerations, Web Services Infrastructure

Web Services Threats, Vulnerabilities, and Countermeasures
Threats and Vulnerabilities, Threat Modeling, Vulnerability Categorizations and Catalogs, Threat and Vulnerabilities Metrics

Standards for Web Services Security

Digital Identity Management and Trust Negotiation

Access Control for Web Services

Recommended Books:
2. Web Services Security by Mark O’NEILL 2011
3. Professional Web Services Security Author: David Whitney Date: December 2010, Revised edition Publisher: Wrox Press
5. Improving Web Services Security Author(s) J.D. Meier, Carlos Farre, Jason Taylor, Prashant Bansode, Steve Gregersen, Madhu Sundararajan, Rob Boucher Publisher: Microsoft corporation (February, 2009)


Virtualization: concept and properties of virtualization, CPU virtualization, memory virtualization, I/O virtualization, Forms of CPU virtualization

Virtualization scenarios: server consolidation, software development, debugging, fault tolerance, and security. Planning, Designing, Migrating and Deploying Virtual Infrastructure using Microsoft hyper-V, Citrix XenServer, QEMU and VMWare.

Cloud security: Cloud Security challenge, Principal Characteristics of Cloud Computing security, Data center security Recommendations, Encryption and key management in the cloud, identity and access management, trust models for cloud, Cloud forensics, traditional security, business continuity and disaster recovery

Data security tools and techniques for the cloud: Understanding the cloud architecture, Governance and enterprise risk management, design of customized cloud security measures, application security, targets of cyber crime

Trustworthy cloud infrastructures, Secure computations, Cloud related regulatory and compliance issues, Virtual Machines and Security Issues

Recommended Books:
4. Cloud Computing Bible, Barrie Sosinsky, By Wiley Publisher 2011