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

Schedule of Teaching			**Schedule of Examination**				
Lecture	Tutorials	Total	Time (Hrs)	Theory Marks	Sessional Marks	Viva	Total
All theory Subjects		3	100	50			150
Projects				50	50		100
Seminar				100			100
Dissertation			Satisfactory/Not Satisfactory				

SEMESTER-I		**L**	**T**	**P**
ITCW-501	Advance Topics in Software Engineering	3	1	-
ITCW-503	Computer Security, Audit Assurance and Risk Management	3	1	-
ITCW-505	Advanced Internet & Web Technology	3	1	-
IT-506	Research Methodologies	3	1	-
ITCW-507	Data Warehousing & Data Mining	3	1	-
ITCW-509	Advanced IT and Cyber Warfare Lab-I	-	-	4
SEMESTER-II				
ITCW-502	Forensics and Cyber Law	3	1	-
ITCW-504	Applied Cryptography	3	1	-
ITCW-506	Ethical Hacking	3	1	-
ITCW-508	Wireless & Mobile Security	3	1	-
ITCW-510	Intrusion Detection & Analysis	3	1	-
ITCW-512	Advanced IT and Cyber Warfare Lab-II	-	-	4
SEMESTER-III				
ITCW	Elective-I	3	1	-
ITCW	Elective-II	3	1	-
ITCW-531	Project			
ITCW-533	Seminar			
SEMESTER-IV				
ITCW-514	Dissertation			

ELECTIVE-I, II *

ITCW-511 Bioinformatics and BioSecurity.
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-527Web 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

L	T	P
3	1	-

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

Object Oriented Design : Goodness of design, structured analysis and design, Detailed Structure Analysis, Object oriented Concepts and Principles, Object oriented Analysis and Design, Abstractions, Compositions and Aggregations, Object oriented Testing, Object oriented Measurements and Metrics, classifications-class size, class inheritance, class internals, class externals. UML Designs and Concepts.

Software Implementation & Quality: Development Environment Facilities: User interface design, Coding standards and guidelines. Code walkthrough and reviews, Software Testing-Unit Testing framework, Regression Testing, Silk Test, Test Automation, Reliability, Testability, ISO 9000 SEI CMM, PSP, and Six Sigma

Rapid Software Development: Agile Methods, Extreme Programming, pair programming, Rapid Application Development, Software Prototyping.

Software Reuse & Reengineering: Reuse Methodologies, Reuse Repository, Design Patterns, Generator based Reuse Component Based software Development Process, Domain engineering, Classifying and Retrieving components. Business Process Reengineering, Reverse Engineering & Forward Engineering, Code Restructuring and Data Restructuring.

Secure Software Engineering: Using UML for Security, UML 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

REFERENCES

1. Ian Sommeriele, “Software Engineering”, Addison Wesley.
2. C.Easteal and G.Davis, Software Engineering Analysis and Design, Tata McGraw Hill.
3. Pressman, Software Engineering –A Practitioner’s Approach.
4. Richard Fairley ,Software Engineeering Concepts ,Tata Mcgraw Hill.
5. Pankaj Jalote , An Integrated Approach to Software engineering, Narosa Publication.

ITCW – 503 COMPUTER SECURITY, AUDIT ASSURANCE AND RISK MANAGEMENT

L	T	P
3	1	-

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.

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.

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.

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.

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.

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

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.

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)

Routing Technology: Introduction to the basic Router User Interface, CDP, ARP, Creating a Host Table, Static Routes, RIP, Troubleshooting RIP, IGRP, PPP with CHAP Authentication, Connectivity Tests with Trace route, ISDN, IPX, Introduction to the Switch, Frame Relay Hub and Spoke Topology, Frame Relay Full Mesh Topology, Standard Access List, Telnet, VLAN, VTP, and OSPF Routes.

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

Security protocols: IPsec overview , IP security architecture , IPsec-Internet Key Exchanging(IKE) , IKE phases, 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.

REFERENCES:

1, K. Prasad, "Principles of Digital Communication Systems and Computer Networks," eBook
2, W.Richard Stevens, "TCP/IP Illustrated, Volume 1: The Protocols," Addison-Wesley, 1994
3, Larry L. Peterson and Bruce S. Davie, "Computer Networks A Systems Approach", 3rd edition, Morgan Kaufmann, 2003.

Additional References

1 Tanenbaum, "Computer Networks," 4th edition
2 Kurose and Ross, "Computer Networks: A Top-Down Approach Featuring the Internet," 2nd edition
3 Comer, "Internetworking with TCP/IP, Volume 1," 4th edition
4 Bertsekas and Gallager, "Data Networks," 2nd edition

IT -506 RESEARCH METHODOLOGIES

L	T	P
3	1	-

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:

1. Borth, Wayne C, et.Al., The Craft of Research: Chicago Guides to Writing Edition and Publishing.
2.Johnson, R.A., Probability and Statistics, PHI, New Delhi.
3. Meyer, P.L., Introduction to Probability & Statistical, Applications: Oxford, IBH.

Additional References

1. Hogg, R.V. & Craig, A.T., Introduction to Mathematical Statistics, MacMillan.
2. Goon, A.M., Gupta, M.K. & Dasgupta, Fundamentals of Statistics, Vol.I: World Press.
3. Gupta, S.C. & Kapoor, V.K., Fundamentals of Mathematical Statistics, Sultan Chand & Sons.

ITCW-507 DATA WAREHOUSING AND DATA MINING

L	T	P
3	1	-

OBJECTIVES: The course focus 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 (Partioning Method, Hierarchical Method, Density Base & 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:

1. Paul Raj Poonia, “Fundamentals of Data Warehousing”, John Wiley & Sons, 2003.
2. Sam Anahony, “Data Warehousing in the real world: A practical guide for building decision support systems”, John Wiley, 2004

Reference Books:

1. W. H. Inmon, “Building the operational data store”, 2nd Ed., John Wiley, 1999.
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 - Addsiaans (Addison Wesley)

ITCW -509 ADVANCED IT AND CYBER WARFARE LAB

L	T	P
-	-	4

Laboratory Work

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

Semester-II

ITCW-502 FORENSICS AND CYBER LAW

L	T	P
3	1	-

Introduction to Forensics and Cyber Crime: Fundamentals of computer, Internet Technology, E,Governance & E, Business,Crime, Introduction, crime, criminology, origin, source, recent trends.

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,

Types and Categories of Cyber Crime Categories of cyber crime: Personal, Business, Financial, Office Security, Cyber Crime, Complete transparency, hacking/cracking, denial of service, IP piracy, phrasing, hetaerism etc. Cyber attack, cyber attackers

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:

1. Cyber crime**:** Bernadette H. Schell and Clemens Martin, ABC,CLIO, Inc.
2. Scene of the Cybercrime**:** Computer Forensics Handbook by Debra Littlejohn Shinder.,Syngress Shinder Books by Michael cross , Second Edition. 2008
3. Computer Forensics: Cybercriminals, Laws, and Evidence by Marie-Helen Maras Edition 2012, Jones and Bartlett Learning, LLC.
4. Cybercrime and the Law: Challenges, Issues, and Outcomes by Susan W. Brenner , UPNE 2012

ITCW- 504 APPLIED CRYPTOGRAPHY

L	T	P
3	1	-

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, hamir's Three Pass Protocol, IBM Secret, Key Management Protocol, MITRENET, Kerberos, IBM Common Cryptographic Architecture.

REFERENCES

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" John Wiley & Sons, Inc, 2nd Edition, 2006.
2. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2008
3. Atul Kahate, "Cryptography and Network Security", Tata McGrew Hill, 2009.
4. William Stallings, "Cryptography and Network Security", 5th Edition, Pearson Education, 2011.

ITCW-506 ETHICAL HACKING

L	T	P
3	1	-

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

Securing permission, Securing file and folder permission. Using the encrypting file system, Securing registry permissions. Securing service, Managing service permission. Default services in windows 2000 and windows XP. Unix, The Quest for Root. Remote Access vs. Local access. Remote access. Local access. After hacking root.

UNIT III

Dial, up, PBX, Voicemail, and VPN hacking, Preparing to dial up. War, Dialing. Brude, Force Scripting PBX hacking. Voice mail hacking. VPN hacking. Network Devices, Discovery, Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability.
Detecting Layer 2 Media.

UNIT IV

Wireless Hacking, Wireless Footprinting. Wireless Scanning and Enumeration. Gaining Access. Tools that exploiting WEP Weakness. Denial of Services Attacks. Firewalls, Firewalls landscape, Firewall Identification, Scanning Through firewalls, packet Filtering, Application Proxy Vulnerabilities . Denial of Service Attacks, Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. Unix and Windows DoS

UNIT V

Remote Control Insecurities, Discovering Remote Control Software. Connection. Weakness. VNC. Microsoft Terminal Server and Citrix ICA .Advanced Techniques Session Hijacking. Back Doors. Trojans. Cryptography . Subverting the systems Environment. Social Engineering. Web Hacking. Web server hacking web application hacking. Hacking the internet User, Malicious Mobile code, SSL fraud, E,mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.

REFERENCES:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.
2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010.

ITCW-508 WIRELESS & MOBILE SECURITY

L	T	P
3	1	-

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-repudiation 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

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

Android Security: Android Securable IPC Mechanism, Android Security Model, Intents, Activities, Services, Android Security tools.

REFERENCES

1. Russel Dean Vines, "Wireless Security Essentials: Defending Mobile from Data Piracy", John Wiley & Sons, 3rd Edition, 2008.
2. Cyrus, Peikari and Seth Fogie, "Maximum Wireless Security", SAMS Publishing 2010.
3. Yi,Bing Lin and Imrich Chlamtac, "Wireless and Mobile Networks Architectures",John Wiley & Sons, 2008.
4. Raj Pandya, "Mobile and Personal Communication systems and services", Prentice Hall of India, 2008.
5. Tara M. Swaminathan and Charles R. Eldon, "Wireless Security and Privacy, Best Practices and Design Techniques", Addison Wesley, 2002.
6. Mobile Application Security, Himanshu Dwivedi, Chris Clark, David Thiel, Tata McGraw Hill Edition, 2010

ITCW-510 INTRUSION DETECTION & ANALYSIS

L	T	P
3	1	-

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.

Network Based Intrusion Detection Systems: Networking Overview, Application Layer, Transport Layer, Network Layer, Hardware Layer, Components and Architecture, Typical Components, Network Architectures and Sensor Locations, Security Capabilities, Information Gathering Capabilities, Logging Capabilities

Wireless Network based Intrusion Detection Systems: Wireless Networking Overview, WLAN Standards, WLAN Components, Threats against WLANs Components and Architecture, Typical Components, Network Architectures, Security Capabilities, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities, Handling Alerts

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

Host Based IDS and Network Behaviour analysis: Components and Architecture, Typical Components and Network Architectures, Host Architectures, Security Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities, Components and Architecture of network behaviour in presence of IDS, Components in presence of IDS, Network Architectures and Sensor Locations, Security Capabilities in presence of IDS, Information Gathering Capabilities, Logging Capabilities, Detection Capabilities, Prevention Capabilities.

Recommended Book

1. Tim Crothers, Implementing Intrusion Detection Systems: A Hands On Guide for Securing the Network, John Wiley and Sons, ISBN: 978-0-7645-4949-6, reprint edition 2010
2. Christopher Kruegel, Fedrick Valeur, Intrusion Detection and Correlation: Challenges and Solutions, Springer, 2011
3. Intrusion Detection Systems (Advances in Information Security)Roberto Di Pietro and Luigi V. Mancini , Springer , 2008
4. Improved Real-Time Discretize Network Intrusion Detection System Heba F Eid, Ahmad Taher Azar, and Aboul Ella Hassanien ,Springer Vol. 201, 2013

ITCW-512 Advanced IT and Cyber Warfare Lab-II

L	T	P
–	–	4

Laboratory Work

To impart practical experiments relevant to the courses offered in scheme with orientation towards Security & Cyber Warfare

Semester-III -Electives

ITCW-511 Bioinformatics and BioSecurity

L	T	P
3	1	-

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.

GENOMICS AND GENE RECOGNITION: Prokaryotic genomes, Prokaryotic gene structure., Prokaryotic gene density, Eukaryotic genomes, Eukaryotic gene structure, Open reading frames, Gene expression, Transposition, Repetitive elements, Eukaryotic gene density.

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

1. Bioinformatics Computing (International Edition): Dan Krane, Michael Raymer,Bryan Bergeron, 2012
2. Computational approaches in Cheminformatics and Bioinformatics edited by Dr. Rajarshi Guha and Dr. Andreas Bender, Wiley Publishing., 2010.
3. Biosecurity Law and Policy: Biosecurity, Biosafety and Biodefense Law, by Victoria Sutton (Author) Vargas Publishing (January 26, 2014), ISBN-10: 0983802491 , ISBN-13: 978-0983802495,

ITCW -513 BIOMETRIC SECURITY

L	T	P
3	1	-

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

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 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

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, “Biometrics -Identity verification in a network”, Wiley Eastern, 2012.
2. John Chirillo and Scott Blaul,” Implementing Biometric Security”, Wiley Eastern Publications, 2012.
3. John Berger,” Biometrics for Network Security”, Prentice Hall, 2010.

ITCW -515 SECURITY ASSESSMENT AND VERIFICATION

L	T	P
3	1	-

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.

REFERENCES

1. Sudhanshu Kairab, "A practical guide to security assessments", CRC press, 2010.
2. Douglas J.Landoll, "A Security risk assessment Handbook", Auerbach publications, 2012.
3. Network Security Assessment: From Vulnerability to Patch By Steve Manzuik Ken Pfeil Andrew Gol 2009
4. Operational Semantics and Verification of Security Protocols Cremers, Cas, Mauw, Sjouke, Springer,2012.

ITCW -517 SECURITY THREATS

L	T	P
3	1	-

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

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

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

1. Joseph M Kizza, "Computer Network Security", Springer Verlag, 2012
2. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2009.
3. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", PHI, 2008.
4. Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2010.
5. Insider Threats in Cyber Security : Series: Advances in Information Security, Vol. 49 Probst, C.W.; Hunker, J.; Bishop, M.; Gollmann, D. (Eds.)2012

ITCW -519 STEGANOGRAPHY AND DIGITAL WATERMARKING

L	T	P
3	1	-

UNIT I

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

UNIT II

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

UNIT III

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

UNIT IV

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

UNIT V

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

REFERENCES

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, "Information hiding techniques for Steganography and Digital Watermarking", ARTECH House Publishers, January 2011.
2. Jessica Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications", Cambridge university press, 2010.
3. Steganography, Abbas Cheddad, Vdm Verlag and Dr. Muller, "Digital Image" Aktienge sells chaft & Co. Kg, Dec 2009.
4. Ingemar Cox, Matthew Miller,Jeffrey Bloom,Jessica Fridrich and Ton Kalker, "Digital Watermarking And Steganography", Morgan Kaufmann Publishers, Nov 2011.
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

ITCW -521 DISTRIBUTED SYSTEMS SECURITY

L	T	P
3	1	-

UNIT – I

Introduction: 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.

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

Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities Injection Vulnerabilities , Cross-Site Scripting (XSS) , Improper Session Management , Improper Error Handling ,Improper Use of Cryptography , Insecure Configuration Issues, Denial of Service, Canonical Representation Flaws , Overflow Issues. Service-Level Threats and Vulnerabilities: SOA and Role of Standards , Service Level Security Requirements , Service Level Threats and Vulnerabilities , Service Level Attacks , Services Threat Profile.

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

Service Level Solutions: Services Security Policy , SOA Security Standards Stack – Standards in Dept , Deployment Architectures for SOA Security , Managing Service Level Threats, Compliance in Financial Services **,** SOX Compliance , SOX Security Solutions , Multilevel Policy, Driven Solution Architecture , Case Study: Grid **,** The Financial Application **,** Security Requirements Analysis. Future Directions, Cloud Computing Security **,** Security Appliances **,** Usercentric Identity Management **,** Identity Based Encryption (IBE) **,** Virtualization in Host Security.

REFERENCES

1. Abhijit Belapurakar, Anirban Chakrabarti and et al., “Distributed Systems Security: Issues. Processes and solutions”, Wiley, Ltd., Publication, 2011.
2. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, “Distributed Systems Security: Issues, Processes and Solutions”, Wiley publications, 2011.
3. Rachid Guerraoui and Franck Petit, “Stabilization, Safety, and Security of Distributed Systems”, Springer, 2010.

ITCW -523 SECURING WINDOWS & LINUX

L	T	P
3	1	-

Introduction to General Security Concepts: Principles of Information Security, Information Security Standards, Regulations, and Compliance, Authentication, Authorization, and Accounting (AAA).

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

Network Security: General Network Concepts and Vulnerabilities, Network Services and Network Devices, Internet Security and Vulnerabilities, Network Security Tools and Devices

Application Security: HTTP Security, Electronic Mail, Samba Security.

System Security: General System Security Threats, Hardware and Peripheral Devices, OS and Application Security, Virtualization, System-Based Security Applications, Understanding Linux Security, System Monitoring and Auditing.

Organizational and Operational Security: Physical Security Concepts and Vulnerabilities, Policies and Procedures, Risk Analysis, Business Continuity and Disaster Recovery, Network layer firewalls, transport layer firewalls, application layer firewalls

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

Remote Access and Authentication: Virtual Private Networking, Strong User authentication.

Recommended Books:

1. Security for Microsoft Windows System Administrators, Introduction to key Information Security concepts, Derrick Rountree, Elsevier,2010
2. Linux Security, Ramón J. Hontañón, 2011 ,Sybex, ISBN: 0-7821-2741-X
3. Linux Security Cookbook, Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes, O'Reilly, June 2009 ISBN: 0-596-00391-9
4. Linux in a Windows World Leverage Linux to make Windows more secure, responsive & affordable,2009

ITCW -525 CYBER INCIDENT HANDLING & REPORTING

L	T	P
3	1	-

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

Recommended Books

1. An introduction to computer security: the NIST handbook, Barbara Guttman, Edward Roback, NIST Special Publication 2012
2. The effective incident response team, Julie Lucas, Brian Moeller, Addison-Wesley Professional
3. Principles of incident response and disaster recovery, Michael E. Whitman, Herbert J. Mattord, Thomson Course Technology, 2011
4. Incident response: a strategic guide to handling system and network security Breaches, E. Eugene Schultz, Russell Shumway, New Rider Publishing-2012
5. Incident Response & Computer Forensics, Mandia, Tata McGraw-Hill Education-2010

ITCW -527 WEB SERVICE SECURITY

L	T	P
3	1	-

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
The Concept of Standard Web Services Security, Standards Framework, An Overview of Current Standards, XML Data Security, Security Assertions Markup Language (SAML), SOAP Message Security, Key and Trust Management standards, Standards for Policy Specification, Access Control Policy Standards, Implementations of Web Services Security Standards

Digital Identity Management and Trust Negotiation
Overview of Digital Identity Management, Overview of Existing Proposals Liberty Alliance, WS-Federation, Comparison of Liberty Alliance and WS-Framework, Other Digital Identity Management Initiatives, Discussion on Security of Identity Management Systems, Business Processes.

Access Control for Web Services
Approaches to Enforce Access Control for Web Services, WS-AC: An Adaptive Access Control Model for Stateless, Web Services, The WS-AC Model, WS-AC Identity Attribute Negotiation, WS-AC ,Parameter Negotiation.

Recommended Books:

1. Elisa Bertino, Lorenzo D. Martino, Federica Paci, Anna C. Squicciarini, Security for Web Services and Service Oriented Architectures, Springer Science (2009).
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
4. Security for Web Services and Service-Oriented Architectures Bertino, E., Martino, L., Paci, F. Squicciarini, A. 2010, XII, 218p.
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)

ITCW -529 VIRTUALIZATION AND CLOUD SECURITY

L	T	P
3	1	-

Introduction: Basics of the emerging cloud computing paradigm, Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Virtualization Technology and Cloud Computing

Cloud Computing: Cloud Service Models, cloud-computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing,

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:

1. Jim Smith, Ravi Nair, and Virtual Machines: Versatile Platforms for Systems and Processes, Morgan Kaufmann, 2011.
2. Cloud Computing: Implementation, Management, and Security, JohnRittinghouse and James F.Ransome, CRC Press Taylor and Francis Group,2010
3. Virtualization Security : Protecting Virtualized Environment : By Dave Shackleford Published By Wiley 2013
4. Cloud Computing Bible , Barrie Sosinsky, By Wiley Publisher 2011