Punjab Technical University
Syllabus for M.Tech (e-SECURITY) Batch 2010 onwards

SEMESTER-I

	L	T	P
CS-501 Advance Software Engineering	3	1	-
CS-503 Network Security	3	1	-
CS-505 Advanced Computer Architecture	3	1	-
CS-507 Advanced Database Management System	3	1	-
CS-509 Advanced Programming Language	3	1	-
CS-511 Advanced Software Engineering Lab	-	-	4
CS-513 Advanced Database Management System Lab	-	-	4

SEMESTER-II

	L	T	P
CS-502 Digital image Processing	3	1	-
CS-504 Distributed Systems	3	1	-
CS-506 Compiler Design	3	1	-
CS- Elective-I	3	1	-
CS- Elective-II	3	1	–

SEMESTER-III

CS- Elective-III	3	1	-
CS- Elective-IV	3	1	-
CS-523 Project			
CS-525 Seminar			

SEMESTER-IV

CS-500 Dissertation

LIST OF ELECTIVES

ELECTIVE-I

527- Mathematical Models for Internet
528- Financial Mathematics
529- Digital Defense

ELECTIVE-II

530- Cryptography
531- Public Key Infrastructure and Trust Management
532- Biometric Security

ELECTIVE-III

533-Game theory and its applications
534-Intrusion Detection
535- Security Engineering

ELECTIVE-IV

536-Information Security Risk Management537-Cyber laws and rights in today's digital age 538-Computer Security Audit and Assurance 539-Decision Support Systems and Methods

CS-501 Advance Software Engineering

L T P 3 1 -

Introduction: Life cycle models, Requirement Analysis and specification, Formal requirements specification.

Fundamental issues in software design: Goodness of design, cohesions, coupling. Function-oriented design: structured analysis and design. Overview of object –oriented concepts.

Unified Modeling Language (UML). Unified design process. User interface design. Coding standards and guidelines. Code walkthrough and reviews.

Unit testing. Black box and white box testing. Integration and system testing. Software quality and reliability.

SEI CMM and ISO 9001. PSP and Six Sigma. Clean room technique.

Software maintenance issues and techniques. Software reuse. Client-Server software development.

Reference:

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.

CS-503 Network Security

L T P 3 1 -

Introduction :

Overview of computer networks, seven-layer architecture, TCP/IP suite of protocols, etc.

MAC protocols for high-speed LANS,MANS and wireless LANs. (For Example, FDDI,DQDB,HIPPI,Gigabit Ethernet, Wireless Ethernet, etc.)

Fast access technologies(For Example, ADSL, Cable Modem, etc.

Ipv6: Basic Protocol, extensions and options, support for QoS, security ,etc., neighbour discovery, autoconfiguration, routing. Changes to other protocols. Application Programming Interface for IPV6.

Mobility in networks. Mobile IP, Security related issues.

IP Multicasting, Multicast routing protocols, address assignments, session discovery, etc.

TCP extension for high-speed networks, transaction-oriented applications. Other new options in TCP.

Network security at various layers. Secure-HTTP,SSL,ESP, Authentication header, key distribution protocols,. Digital signatures, digital certificates.

References:

W.R.Stevens. TCP/IP Illustrated, Volume 1: The Protocols, Addison Wesley, 1994.

R.Wright.TCP/IP Illustrated, Volume 2: The Implementation, Addison Wesley , 1995.

W.R Stevens. TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP and the unix domain protocols, Addison Wesley, 1996.

CS- 505 Advance Computer Architecture

L T P 3 - -

1.Computational model
2.The concept of Computer Architecture
3.Introduction to Parallel Processing
4.Introduction to ILP Processors
5.Pipelined Processors
6.VLIW Architecture
7.Super Scalar Processors
8.Processing of Control transfer instruction
9.Code Scheduling for ILP-processors
10.Introduction to Data Parallel Architecture, SIMD Architecture, MIMD Architecture
11.Vector Architecture.
12.Multi threaded Architecture
13.Distributed Memory MIMD Architecture
14.Shared memory MIMD Architecture.

Reference:

1.Dezso Sima , Terence Fountani, Peter Kacsuie , “Advanced Computer Architectures : A Design Space Approach, 1/e , Pearson Eduction.
2.Computer Architecture by Stone

CS-507 Advance Database Management Systems

L T P 3 1 -

Introduction of DBMS ,Types of DBMS and their advantages and disadvantages

Introduction of RDBMS, Types of relational query language, Normalization, Query optimization

Database protection in RDBMS –Integrity, Concurrency control, Recovery

Distributed Databases :- concepts, structure, trade-offs

Methods of data distribution –fragmentation, replication, design & advance concepts of DDBMS

Introduction to object oriented databases ,Deductive databases

Data warehousing Concepts: Architecture, Dataflows, Tools & Technologies, Data Marts Data Mining & Online Analytical Processing

Spatial & Multimedia databases

Mobile Computing & Mobile Databases Textbooks:-

1)Elmasri, Navathe, ”Fundamentals of Database Systems”, Pearson Education.

2)Henry F. Korth, A Silberschatz, ”Database Concepts”, Tata Mc Graw Hill.

3)Thomas Conolly, Carolyn Begg,” Database Systems”, Pearson Education.

4)Alexis Lcon, Mathews Leon, ”Database Management Systems”.

5)C.J.Date ,”An Introduction to DBMS”, Narosa Publishing House.

CS_509 ADVANCED PROGRAMMING LANGUAGES L T P
3 1 -

Introduction: Brief history of Programming Language, Characteristics of programming language.

Programming Language Processors: The structure and operation of a computer, Hardware and firmware computers, Translator and simulator computers, Syntax, semantics and virtual computers, hierarchies of computers, binding and binding time

Elementary Data Types: Data object, variable and constants, data types, specification of elementary data types, declarations, type checking and type conversion, assignment and initialization, numeric data types, enumerations, Boolean, characters

Structured Data Types: Structured data object and data types, specification of data structure types, implementation of data structure types, declarations and type checking for data structures, vector and arrays, record, character strings, variable sized data structures, pointers andprogrammer-constructed data objects, sets, file and input/output

Subprogram And Programmer-Defined Data Types: Evolution of the data type concept, Abstraction, encapsulation, and information hiding, subprogram, type definitions, abstract data types

Sequence Control: Implicit and explicit sequence control, sequence control within expression, sequence control between statements, subprogram sequence control, recursive subprogram, exceptions and exception handlers, Co-routines, scheduled subprograms, tasks and concurrent execution, data structures and sequence control.

Data Control: names and referencing environments, static and dynamic scope, block structure, local data and local referencing environments, shared data, task and shared data.

Storage Management: Major Runtime elements requiring storage, programmer and system controlled storage management, storage management phases, static storage management, stack based storage management, heap storage management

Syntax And Translation: General syntactic criteria, syntactic elements of language, stages in translation, formal definition of syntax.

Operating And Programming Environment: Batch processing environment, interactive environments, embedded system environments, programming environments

Theoretical Models: Problem in syntax and translation, problem in semant

References:

Programming Languages, design and implementation second edition by Terrence W. Pratt Prentice Hall of India pvt.ltd. New Delhi

CS-511 & CS-513 Project Lab (DBMS & Software Engineering)

L T P - - 4

The Students are required to implement the applications based on

1.Fuzzy databases
2.Expert databases
3.Object-oriented Databases
4.Distributed databases
5.Library management system
6.Crop management system
7.On-line sharing of computer systems
8.Highway systems
9.Hospital management system
10.Hotel management system
11.University management system
12.Inventory control
13.Railway management system
14.Any other similar database system

CS-502 Digital Image Processing

L T P 3 1 -

Fundamentals: Introduction, Origin, Areas of Image Processing, steps in Digital Image Processing, Components of Image Processing System, Image Sensing , Sampling and Quantisation, Neighbouring of Pixels

Image Enhancement and Restoration: Enhancement: Spatial Filtering, Introduction to Fourier Transformation, Restoration: A model of the Image Degradation/ Restoration Process.**Color Image Processing:** Color fundamentals, models, transformation and segmentation. Noise in color images.

Wavelets: Wavelet functions, Wavelet transformations in one and two dimensions, fast wavelet transform.

Image Compression: Image compression models, Error free compression, Lossy compression.**Image segmentation:** Line detection, edge detection, Edge linking and boundry detection, region based segmentation.

Representation and Description: Representation, Boundry and Regional Descriptors, Relational Descriptors.

Object Recognition: Pattern and pattern classes, recognition based on Decision Theoretic Methods, Structural Methods.

References:

Digital Image Processing by Rafael C. Gonzalez, Richard E. Woods

CS-504 DISTRUBUTED SYSTEMS L T P

3 1 -

1.Characeterization of Distributed Systems: Introduction, system models –Architectural and fundamental models

2.Interprocess communication: API for internet protocol, Marshalling. Client server communication, group communication case study: unix

3.Distributed objects and remote invocation: communication between Distributed objects, RPC, events and notification case study: Java RMI

4.Operating System Support: Operating System layer. Protection , processes ands threads, operating system architecture

5.Distributed File System: File service architecture, network file system, Sun network file system, Andrew file system Case Study: unix

6.Name services: Name services and domain name system . directory and discovery services Case Study: Global Name service

7.Transaction and concurrency control: transactions, nested transactions, Locks, optimistic concurrency control, time stamp ordering, Comparison of methods for concurrency control

8.Distributed transaction: Flat and nested distributed transactions. Atomic Commit protocol, Distributed dead locks

9.Distributed Multimedia systems; characteristics of multimedia, multimedia data. Quality of service management, resorce management, stream adaptation.

Case study; Tiger video file server.

10.Distributed shared memory: design and implementation issues, sequential consistency and Ivy and Release Consistencyan Munin

Case Study of distributed systems: CORBA Books :

1.G. Coulouis, et al. Distributed Systems: Concepts and design, Pearson Education Asia,2004

2.A.S. Tanenbaum, Modern operating Systems, Prentience Hall

3.www.cdk3.net/refs

4.www.ietf.org/rfc

CS-506 Compiler Design

L T P 3 1 -

Course Contents:

Compiler structure: analysis-synthesis model of compilation, various phases of a compiler, tool based approach to compiler construction.

Lexical analysis: interface with input, parser and symbol table, token, lexeme and patterns. Difficulties in lexical analysis. Error reporting. Implementation. Regular definition, Transition diagrams, LEX.

Syntax analysis: CFGs, ambiguity, associativity, precedence, top down parsing, recursive descent parsing, transformation on the grammars, predictive parsing, bottom up parsing, operator precedence grammars, LR parsers (SLR, LALR, LR), YACC.

Syntax directed definitions: inherited and synthesized attributes, dependency graph, evaluation order, bottom up and top down evaluation of attributes, L- and S-attributed definitions.

Type checking: type system, type expressions, structural and name equivalence of types, type conversion, overloaded functions and operators, polymorphic functions.

Run time system: storage organization, activation tree, activation record, parameter passing, symbol table, dynamic storage allocation.

Intermediate code generation: intermediate representations, translation of declarations, assignments, control flow, boolean expressions and procedure calls. Implementation issues. Code generation and instruction selection: issues, basic blocks and flow graphs, register allocation, code generation, dag representation of programs, code generation from dags, peep hole optimization, code generator generators, specifications of machine.

Books and References:

A.V. Aho, R. Sethi, and J. D. Ullman. *Compilers: Principles, Techniques and Tools* , Addison-Wesley, 1988.

C.Fischer and R. LeBlanc. *Crafting a Compiler* , Benjamin Cummings, 1991.

C.Fischer and R. LeBlanc. *Crafting a Compiler in C* , Benjamin Cummings.

A.C. Holub. *Compiler Design in C* , Prentice-Hall Inc., 1993.

Appel. *Modern Compiler Implementation in C: Basic Design* , Cambridge Press. Appel. *Modern Compiler Implementation in Java: Basic Design* , Cambridge Press.

Fraser and Hanson. *A Retargetable C Compiler: Design and Implementation* , Addison-Wesley.

Electives

CS -527 Mathematical Models for Internet

L T P 3 1 -

1)MATHEMATICAL BACKGROUND

a)Introduction to Probability and Distributions

b)Graph Theory and Graphical Models

c)Singular Value Decompositions and Markov Chains

d)Classification, Clustering

e)Information Theory and Power Law Distributions

2)MATHEMATICAL MODELS FOR INTERNET

a)Design and control of communication networks that respond to randomly fluctuating demands and failures

b)Stability and Fairness of rate control algorithms

c)Simulation of such networks

3)BASIC WWW TECHNOLOGIES

a)Web Documents and Resource Identifiers

b)Protocols

c)Search Engines

4)WEB GRAPHS

a)Internet and Web Graphs

b)Generative Models

c)Applications

5)TEXT ANALYSIS

a)Indexing

b)Lexical Processing

c)Content Based Ranking

d)Latent Semantic Indexing

e)Clustering and Extraction

6)LINK ANALYSIS AND ADVANCED CRAWLING TECHNIQUES

a)Page Ranking

b)Stability and Link Analysis

c)Types of Crawling

d)Web Dynamic

TEXT BOOKS:

1)Modeling Internet and Web by P. Baldi, P. Frasconi and P. Smyth, John Wiley and Sons

2)The Mathematics of Internet Congestion Control by Rayadurgam Srikant

CS-528 Financial Mathematics

L T P 3 1 -

Fundamentals of Mathematical Finance

Stochastic models of financial markets. Forward and futures contracts. European options and equivalent martingale measures. Hedging strategies and management of risk. Term structure models and interest rate derivatives. Optimal stopping and American options.

Computation and Simulation in Finance

Monte Carlo, finite difference, tree, and transform methods for the numerical solution of partial differential equations in finance. Emphasis is on derivative security pricing. Prerequisite: 238 or equivalent.

Statistical Methods in Finance

Regression analysis and applications to investment models. Principal components and multivariate analysis. Likelihood inference and Bayesian methods. Financial time series. Estimation and modeling of volatilities. Statistical methods for portfolio management.

Financial Modeling Methodology and Applications

Substantive and empirical modeling approaches. Statistical trading strategies and their evaluation. Nonparametric regression. Advanced time series modeling and forecasting. Options and interest rate markets. Credit markets and default risk modeling.

Algorithmic Trading and Quantitative Strategies

An introduction to financial trading strategies based on methods of statistical arbitrage that can be automated. Methodologies related to high frequency data and stylized facts on asset returns; models of order book dynamics and order placement, dynamic trade planning with feedback; momentum strategies, pairs trading. Emphasis on developing and implementing models that reflect the market and behavioral patterns.

Statistical Models and Methods for Risk Management and Surveillance

Banking and bank regulation. Market risk and credit risk, asset and liability management. Logistic regression, generalized linear models and generalized mixed models. Censored data and survival analysis, loan prepayment and default as competing risks. Back testing, stress testing and Monte Carlo methods. Risk surveillance, early warning and adaptive risk control methodologies.

Data Mining as Modern Applied Statistics

Two-part sequence. New techniques for predictive and descriptive learning using ideas that bridge gaps among statistics, computer science, and artificial intelligence. Emphasis is on statistical aspects of their application and integration with more standard statistical methodology. Predictive learning refers to estimating models from data with the goal of predicting future outcomes, in particular, regression and classification models. Descriptive learning is used to discover general patterns and relationships in data without a predictive goal, viewed from a statistical perspective as computer automated exploratory analysis of large complex data sets.

Monte Carlo

Random numbers and vectors: inversion, acceptance-rejection, copulas. Variance reduction: antithetics, stratification, control variates, importance sampling. MCMC: Markov chains, detailed balance, Metropolis-Hastings, random walk Metropolis,independence sampler, Gibbs sampling, slice sampler, hybrids of Gibbs and Metropolis, tempering. Sequential Monte Carlo. Quasi-Monte Carlo. Randomized quasi-Monte

Carlo. Examples, problems and motivation from Bayesian statistics,machine learning, computational finance and graphics.

Credit Risk: Modeling and Management
Credit risk modeling, valuation, and hedging emphasizing underlying economic, probabilistic, and statistical concepts. Point processes and their compensators. Structural, incomplete information and reduced form approaches. Single name products: corporate bonds, equity, equity options, credit and equity default swaps, forwards and swaptions. Multiname modeling: index and tranche swaps and options, collateralized debt obligations. Implementation, calibration and testing of models.

References

Martin Baxter and Andrew Rennie, Financial Calculus: An Introduction to Derivative Pricing, Cambridge University Press, 1996

Jamil Baz and George Chacko, Financial Derivatives: Pricing, Applications, and Mathematics, Cambridge University Press, 2004

Thomas Björk, Arbitrage Theory in Continuous Time, 2nd ed., Oxford University Press, 2004 Z. Brzeźniak and T. Zastawniak, Basic Stochastic Processes, Springer, 1998

Sasha Cyganowski, Peter Kloeden and Jerzy Ombach, From Elementary Probability to Stochastic ,Differential Equations with MAPLE, Springer, 2001

Alison Etheridge,A Course in Financial Calculus, Cambridge University Press, 2002 Hélyette Geman, Commodities and Commodity Derivatives, John Wiley & Sons, 2005

Desmond Highham, An Introduction to Financial Option Valuation: Mathematics, Stochastics and Computation, Cambridge University Press, 2004

John C. Hull,Options, Futures, and Other Derivatives, 5th ed., Prentice Hall, 2002 Peter James, Option Theory, John Wiley & Sons, 2003

Mark Joshi, The Concepts and Practice of Mathematical Finance, Cambridge University Press, 2003

Paul Wilmott, Sam Howison and Jeff Dewynne,The Mathematics of Financial Derivatives: A Student Introduction, Cambridge University Press, 1995

CS -529 Digital Defense

L T P 3 1 -

Viruses, worms, malicious codes, Trojan Horses etc.: History, Threats, Components, models of propagation and their epidemic spread, defense against worms viruses and malicious codes

DOS attacks, DDoS: Introduction, History, Effects, Evolution, Semantic Levels of ddos, IP Spoofing, ddos defense approaches.

Design of Testbeds for simulation of attacks against critical infrastructures: Attack vectors, Attack simulation their analysis and modeling.

Architectures for Internet: Design Principles, Architectural Constraints, Principles of avoiding failures.

Information Security and Data Management: Information Security, Information Management Technologies, Issues, Discretionary and Mandatory policies for information security, secure distributed and heterogeneous database systems

Introduction to secure data warehousing and data mining for security applications

Books:-

1)Malware: Fighting Malicious Code, Ed Skoudis; Lenny Zeltser, Prentice Hall, November 07, 2003

2) Internet Denial of Service: Attack and Defense Mechanisms ,Jelena Mirkovic, Sven Dietrich, David Dittrich, Peter Reiher , Prentice Hall.

3)Attack Simulation and Thread Modeling by Olu Akindeinde, February 2008.

4)Internet Architecture and Innovations, Barbara van Schewick,july 2010, MIT press

5)Scalable Internet Architecture, Thoe Schlossnagle,2007

6)Database and Applications Security: Integrating Information Security and data management by Bhavani Thuraisingham, Auerbach Publications.

CS-530 Cryptography

L T P 3 1 -

Unit 1:

Introduction :Cryptography, Encryption Schemes, Pseudorandom Generators, Digital Signatures, Fault-Tolerant Protocols and Zero-Knowledge Proofs, Introduction to Steganography, Probability Theory.

Unit 2:

One-Way Functions: Strong One-Way Functions, Weak One-Way Functions, Candidates forOne-Way Functions, Non-Uniformly One-Way Functions. Weak One-Way Functions Imply Strong Ones

Unit 3:

Pseudorandom Generators: Computational Approaches to Randomness, A Rigorous Approach to Pseudorandom Generators, Definitions of Pseudorandom Generators, The Applicability of Pseudorandom Generators, Pseudo randomness and unpredictability.

Unit 4:

Zero-Knowledge/ Interactive Proof Systems: Perfect and Computational Zero-Knowledge,Zero-Knowledge w.r.t. Auxiliary Inputs, Sequential Composition of Zero-Knowledge Proofs, Proofs of Knowledge, Applications, Proofs of Identity , Strong Proofs of Knowledge,Computationally-Sound Proofs, Non-Interactive Zero-Knowledge Proofs.

Unit 5:

Encryption Schemes: Private-Key versus Public-Key Schemes, The Syntax of Encryption Schemes, Security, Indistinguishability of Encryptions, Equivalence of the Security, Constructions of Secure Encryption Schemes, Beyond eavesdropping security,Key-dependent passive attacks, Chosen plaintext and ciphertext attack.

Unit 6:

Digital Signatures and Message Authentication: The two types of schemes, The unified treatment, Attacks and security, Length-restricted signature scheme, Constructing collision-freehashing functions, Constructions of Message Authentication Schemes, Constructions of Signature Schemes.

Unit 7:

General Cryptographic Protocols: The Definitional Approach and Some Models, Some Known Results, The Two-Party Case, The semi-honest model, The malicious model, Privately Computing (2-Party) Functionalities: The 1-out-of-k OT protocol , Privately computing amultiplication-gate, The circuit evaluation protocol.

References:

- Oded Goldreich: Foundation of Cryptography, volume2 basic applications
- Jonathan Katz and Yehuda Lindell: Introduction to Modern Cryptography Principles and Protocols

CS -531 Public Key Infrastructure and Trust Management

L T P 3 1 -

1.Describe PKI and the major components of a PKI: What Is PKI, Components of PKI, Digital signatures, Digital Certificates., Key Management.

2.Design a certification authority (CA) hierarchy to meet business requirements: Certifying Authority, Different trust Model Hierarchical /Mesh/Bridge,Certification,authorities/Parameters/Certificate chain,Certificate management, Registration & Initialization,Certification,Expiration and Revocations – CRL (Certification Revocation List)

3. Certificate services: Install Certificate Services to create a CA hierarchy, Perform certificate management tasks, CA management tasks, and plan for disaster recovery of Certificate Services., Create and publish a certificate template, and replace an existing certificate template, Enroll a certificate manually, auto-enroll a certificate, and enroll a smart card certificate, Configure trust between organizations by configuring and implementing qualified subordination.

4.Directory services such as X.500 and LDAP: X.500 for publication of PKC &CRL,X.509 version 3 certificates,Certificate Validation methods ,Time Stamps,Certificate Lifecycle Management,Cross certification,PKI Architecture and its working.

5.Impact on E-commerce and E business.

References:

1)An INTRODUCTION to CRYPTOGRAPHY, Second Edition ,Author: RICHARD A. MOLLIN
2)Introduction to Cryptography: Principles and Applications, Second Edition, Author: Hans Delfs, Helmut Knebl
3)Internet Security Cryptographic Principles, Algorithms and Protocols, Author: Man Young Rhee

CS -532 Biometric Security

L T P 3 1 -

UNIT – I

Biometrics technology evolution, verification and identification, introduction to Biometrics, Fingerprint Recognition, Face Recognition, Iris Recognition, Hand Geometry Recognition, Gait Recognition, Voice Biometrics, On-Line Signature Verification, Face Recognition, comparison of various biometrics, biometric system errors, biometric deformations.

UNIT – II

False match rate, false non-match rate, biometric applications, biometric sensor interoperability, user psychology in biometric enrollment, Multi-biometrics and multimodal biometrics, Multi-spectral Face Recognition.

UNIT – III

Attacks against Biometric Systems, Biometric Cryptography, Fusion in biometrics, Liveness detection in biometrics, Fingerprint identification technology, scope of fingerprint biometric systems, how to improve the privacy and security of fingerprint biometric system. SFING (synthetic fingerprint generator).

UNIT – IV

Soft-biometric, Incorporating Ancillary Information in biometric Systems. Biometric System Security, Spoof Detection Schemes, Biometrics in Government Sector, Biometrics in the Commercial Sector, Biometric Standards, Biometrics Databases.

Text Books:

1.Davide Maltoni, Dario Maio, Anil K.Jain, and Salil Prabhakar, Handbook of Fingerprint Recognition, Springer.

2.Arun A. Ross, Karthik Nandakumar, and Anil K.Jain, Handbook of Multibiometrics (International Series on Biometrics), Springer.

Reference Books:

1.Anil K. Jain, Biometric Technology for Human Identification II (Proceedings of SPIE).

2.Anil K.Jain, Patrick Flynn, Arun A. Ross, Handbook of Biometrics, ISBN: 978-0-387-71040-

3.John Chirillo and, Scott Blaul, Implementing Biometric Security (Wiley Red Books).

4.Julian Ashbourn, Practical Biometrics: From Aspiration to Implementation, Springer Professional Computing.

CS -533 Game theory and its applications

L T P 3 1 -

Basics of Game theory

Introduction to Game theory, Different types of games: two party, multi party games, coalition games. Applications of Game Theory in the context of Computer Science, in particular, decision making in multi-agent systems.

Introduction to Non-cooperative Game Theory: Games in Normal Form

Definition and Examples of Games in Normal Form, in particular the TCP user's game, Analyzing games: from optimality to equilibrium, Pareto optimality, Defining best response and Nash equilibrium, Finding Nash equilibrium Nash's theorem: proving the existence of Nash equilibrium,

Strategies in normal-form games, Maxmin and minmax strategies, Minimax regret, Removal of dominated strategies, Rationalizability, Correlated equilibrium, Trembling-hand perfect equilibrium

and ϱ-Nash equilibrium.

Computing Solution Concepts of Normal-Form Games

Computing Nash equilibrium of two-player, zero-sum games, Computing Nash equilibrium of two-player, general-sum games: An LCP formulation and the Lemke–Howson algorithm, Computing Nash equilibrium of n-player, general-sum games, Computing maxmin and minmax strategies for two-player, general-sum games, Identifying dominated strategies and Computing correlated equilibrium of n-player normal-form games.

Games with Sequential Actions: Reasoning and Computing with the Extensive Form

Perfect-information extensive-form game: Definition, Strategies and equilibrium, Sub game-perfect equilibrium, Computing equilibrium: backward induction; Imperfect-informationextensive-form games: Definition, Strategies and equilibrium, computing equilibrium: the sequence form and Sequential equilibrium.

Richer Representations: Beyond the Normal and Extensive Forms

Repeated games: Finitely repeated games, infinitely repeated games, Bounded rationality: repeated games played by automata; Stochastic games: Definition, Strategies and equilibrium, Computing equilibrium; Bayesian games: Definition, Strategies and equilibrium, Computing equilibrium and Ex post equilibrium; Congestion games: Definition, Computing equilibrium, Potential games , Non-atomic congestion games and Selfish routing and the price of anarchy; Computationally motivated compact representations: The expected utility problem, Graphical games, Action-graph games and Multi-agent influence diagrams.

Learning and Teaching

The interaction between learning and teaching, Rational learning, Reinforcement learning, Targeted learning, Evolutionary learning and other large-population models.

Mechanism Design

Introduction, Mechanism design with unrestricted preferences, Mechanism design in the quasi-linear setting Groves mechanisms, VCG mechanism, AGV mechanism, Tractable Groves mechanisms, Computational applications of mechanism design: Task scheduling, Bandwidth allocation in computer networks, Multicast cost sharing and Two-sided matching; Constrained mechanism design.

Introduction to Coalitional Game Theory

Definition of Coalitional games with transferable utility, Classes of coalitional games, Analyzing coalitional games, Compact representations of coalitional games: Weighted majority games and weighted voting games, Weighted graph games, Capturing synergies: a representation for super additive games, A decomposition approach: multi-issue representation, A logical approach: marginal contribution nets; Alternative coalitional game models.

BOOKS

1.Martin J. Osborne, "An Introduction to Game Theory", Oxford University Press Inc, USA.

2.Ken Binmore, "Fun and Games: A Text on Game Theory", A.I.T.B.S Publishers.

3.Martin J. Osborne and Ariel Rubinstein, "A Course in Game Theory", MIT Press.

4.Fudenberg, Drew, and Jean Tirole, "Game Theory", Cambridge, MA:MIT Press.

5.Rasmusen, Eric, "Games and Information: An Introduction to Game Theory", Wiley-Blackwell.

6.Shoham, Yoav; Leyton-Brown, Kevin, "Multiagent Systems: Algorithmic, Game- Theoretic, and Logical Foundations", New York: Cambridge University Press.

CS -534 Intrusion Detection

L T P 3 1 -

Introduction to data and methodologies of computer intrusion detection.: Intrusion detection principles, Approaches to intrusion detection, Models Architecture Organization Intrusion response.

Statistical and machine approaches to detection of attacks on computers :SAS System, STATA, bivariate analysis and linear regression modeling.,Host Monitoring. Network Monitoring.

Techniques for studying the Internet: TCP dump filters, Common attacks: network based attacks; probes, DOS., Techniques for visualizing network data. Activity Profiling.

Host Monitoring: Common attacks: host based attacks; buffer overflow and race conditions, malicious code.Computer Immunology, User profiling

Computer virus and worms: How viruses replicate, How viruses scanners work, Virus phylogenies, Computer worms, Covert channels, Back doors, Detecting Trojans

Statistical pattern recognition for detection of attacks: Designing a Statistical Pattern Recognition System.,Multi-Class Pattern Classification, One-Class Pattern Classification, Multiple Classifier Systems

References

1.Computer Intrusion detection and network monitoring: A Statistical Viewpoint. By David J. Marchette, Springer-Verlag, New York, 2001.
2.Network Intrusion Detection System by Lambert M Surhone, Miriam T Timpledon, Susan F Marseken, VDM Verlag Dr. Mueller AG & Co. Kg, 2010.
3.Network Intrusion Detection by Stephen Northcutt Judy, PEARSON EDUCATION LIMITED
4.Intrusion Detection and Prevention by Endorf, Tata McGraw Hill, Edition 1.

CS -535 Security Engineering

L T P 3 1 -

Security Engineering: Introduction, Framework and definition

Usability and Psychology: Attacks Based on Psychology: Pretexting; Passwords; and System Issues

Access Control: Operating System Access Controls; Hardware Protection

Distributed Systems: Introduction; Concurrency; Fault Tolerance and Failure Recovery; Naming and Types of Name

Multilevel Security: Introduction; The Bell-LaPadula Security Policy Model; Historical Examples of MLS Systems; Future MLS Systems; Broader Implications of MLS

Multilateral Security: Introduction; Compartmentation, the ChineseWall and the BMA Model; Inference Control; Residual Problem

Physical Protection: Introduction; Threats and Barriers; Alarms

Monitoring and Metering: Introduction; Prepayment Meters; Taxi Meters, Tachographs and Truck Speed Limiters; Postage Meters

Telecom System Security: Introduction; Phone Phreaking; Mobile Phones; Security Economics of Telecomms

Managing the Development of Secure Systems: Introduction; Managing a Security Project; Methodology; Security Requirements Engineering; Risk Management; Managing the Team

Reference:

1.Ross Anderson, "*Security Engineering: A Guide to Building Dependable Distributed Systems*" 1st Edition, Wiley 2001.

2.Ross Anderson, "*Security Engineering: A Guide to Building Dependable Distributed Systems*" 2nd Edition, Wiley 2008.

3.Julia H. Allen; Sean Barnum; Robert J. Ellison; Gary McGraw; Nancy R. Mead, "*Software Security Engineering: A Guide for Project Managers*" Addison-WesleyProfessional 2008.

*4.*George Coulouris Jean Dollimore Tim Kindberg, "*DISTRIBUTED SYSTEMS: Concepts and Design" Fourth Edition* Addison-Wesley, 2005.

CS – 536 Information Security Risk Management

L T P 3 1 -

RISK MANAGEMENT:

Definition of Risk, Risk Management, Importance Of Risk Management, Integration Of Risk Management Into SDLC

RISK ASSESMENT:

Risk Assessment Methodologies, System Characterization, Threat identification, Vulnerability identification, Control analysis, Likelihood determination, Impact analysis , Risk determination, Control recommendations .

RISK MITIGATION:

Risk Mitigation Options, Risk Mitigation Strategy, Approach for Control Implementation, Control Categories, Cost-Benefit Analysis, Residual Risk

RISK ANALYSIS:

Effective Risk Analysis, Qualitative risk Analysis, Value Analysis, Facilitated Risk Analysis Process, Case Studies of Risk Analysis.

VULNERABILITY IN INFORMATION SYSTEM:

Vulnerability Management, Types of network Vulnerability, Procedure of Vulnerability, Managing Vulnerability, Known Software Vulnerability, Vulnerability Assessment Process. Vulnerability of Critical Infrastructure. Vulnerability Scanning Tools.

THREATS AND ATTACKS:

Principles of Security, Understanding the Attackers, Reducing the Risk of attack, Tools used for the attack, Respond to an Attack.

POST ASSESSMENT ACTIVITIES:

IT Security Architecture and framework, Defining the structure and Hierarchy, Sample IT Security Architecture and Framework, Hierarchical IT Security Architecture and Framework, Security incident Response team.

References:

1.Risk management guide for Information technology systems, Special Publication National institute of Standard and technology, Gaithersburg, MD

2.Thomas R. Peltier, Information Security Risk Analysis, Auerbach Publications; illustrated edition (January 23, 2001).

3.Michael Gregg and **David Kim, Inside Network Security Assessment: Guarding Your IT Infrastructure, Sams (November 28, 2005)**

9.Douglas J. Landoll and Douglas J. Landoll, The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, Auerbach Publications; 1st edition (December 12, 2005)

CS -537 Cyber laws and rights in today's digital age

L T P 3 1 -

1)Introduction to Cyber Crime and IT ACT,2000: Crimes of the millennium, Section 80,Arrest without warrant, Checks and Balances against Arbitrary Arrests, Arrest for about to commit offence, Concept of cyber crime, Hacking, Web Vandals, Cyber fraud and cheating, E-mail Abuse, Virus, Cyber Pornography

2) Jurisdictional Issues and Disputes : Civil Law of Jurisdiction in India, Cause of Action, Jurisdiction and IT Act, Foreign judgements in India, Place of Cause of Action in contractual and IPR disputes, Exclusion clauses and their abuse, Misuse of the law of jurisdiction

3) Copyright Protection in Cyber World : Concept of Domain name, Squatters, legislative moves against squatting, meta tagging, Meaning of copyright, Copyright ownership and assignment, Licence, Term and respect for foreign works, Infringement remedies and Offences, Protection of content on the internet, Downloading for viewing content, Liability of ISPs for Copyright violations, Napster, Software piracy.

4) Digital Signatures, Certifying Authorities and E- Governance : Digital signatures, digital signature certificate, certifying authorities and their liability, E- Governance in India

5) Protection of Cyber Consumers in India : Consumer Protection Act, Goods and Services, Consumer Complaint, Defect in Goods and deficiency in Services, Restrictive and unfair trade practices, Reliefs under CPA, Consumer foras, jurisdiction and implications

6) IT Acts of USA and UK should be discussed.

Recommended Books :

1.Vivek Sood, “Cyber Law Simplified” , Tata McGraw – Hill, 2001
2.Vakul Sharma, “ Handbook of Cyber Laws” , Macmillan, 2002
3.Greenstein & Feinman, “ Electronic Commerce-Security, Risk Mgt and Control”, TMH (2000)
4.Yatindra Singh, “ Cyber Laws ”, Universal publications, Third edition

CS -538 Computer Security Audit and Assurance

L T P 3 1 -

Security Policy frameworks: Practices and Procedures, Policy authority and practices, Policy elements, Information security policy framework, Organizational security policies & procedures, Asset classification and control policies & procedures, Personnel security policies & procedures, Physical and environmental security policies & procedures, Communications and operations management policies & procedures, business practice disclosures. [35%]

PKIs: Public Key Infrastructure, Various PKIs, Core PKI services, Issues of revocation, Anonymity and Privacy issues. [20%]

Key Management:Key generation, key distribution, key storage, key backup and recovery, key management schemes , Threats to key management and protection against those threats, key management Principles and Issues

Certificate Management Life Cycle: Certificate types, Certificate Classes, Certificate Profile, Certificate Application, Certificate Issuance, Listing of certificates, Distributing certificates, Publishing certificates, Storing certificates, Retrieving certificates, Certificate Acceptance, Certificate Suspension and Revocation.

[15%]

XML Security: XML security standards, XML security applications, XML frameworks for security policy specification, Various case studies like X-GTRBAC: An XML-Based Policy Specification Framework and Architecture for Enterprise-Wide Access Control.

[15%]

References

1.Understanding PKI: Concepts, Standards, and Deployment Considerations, 2nd Edition, By Carlisle Adams, Steve Lloyd, Published by Addison-Wesley Professional.

2.Security policies and procedures *principles and practices* By Sari Stern Greene Published by Pearson Prentice Hall in Upper Saddle River, N.J .

3.Web Services Security by Mark O'Neill published by McGraw- Hill

4.Digital Certificates: Applied Internet Security [Paperback] By Jalal Feghhi, Peter Williams.

CS -539 Decision Support Systems and Methods

L T P 3 1 -

UNIT- I
Decision Support Systems and Business Intelligence, Computerized Decision Support – Decision Making, Systems, Modeling, and Support, Decision Support Systems Concepts, Methodologies, and Technologies, Modeling and Analysis.

UNIT II
Business Intelligence, Special Introductory Section: The Essentials of Business Intelligence, Business Analytics and Data Visualization.

UNIT III
Advanced Querying & Information Retrieval, data analysis and OLAP, Data mining, data-warehousing, Information retrieval systems, Data, Text, and Web Mining, Neural Networks for Data Mining.

UNIT IV
Business Performance Management, Collaborative Computing-Supported Technologies and Group Support Systems, Knowledge Management, Intelligent Systems- Artificial Intelligence and Expert Systems.

UNIT V
Advanced Intelligent Systems, Intelligent Systems over the Internet, Implementing Decision Support Systems- Systems Development and Acquisition, Integration, Impacts, and the Future of Management Support Systems.

BOOKS

1.Decision Support and Business Intelligence Systems (8th Edition) by Efraim Turban, Jay E
2.Decision Support and Business Intelligence Systems ; Aronson, Ting-Peng Liang, and Ramesh Sharda, PHI, 2006.

REFERENCES:

1.Decision Support Systems For Sustainable Development : A Resource Book of Methods and Applications; Gregory E. Kersten, Zbigniew Mikolajuk, Anthony Gar-On Yeh; Kiuwer Academic Publishers
2.Developing Web-Enabled Decision Support Systems; Abhijit A. Pol, Ravindra K. Ahuja