SYLLABUS OF INFORMATION SECURITY

I – Semester

COMPUTER SECURITY (IS 501)


Threats - Viruses, worms, Trojan horse, bombs, trap doors, spoofs, email virus, macro viruses, remedies, Intruders, Malicious software, Firewalls, vulnerabilities & threats, Network Denial of service attack.

Communication security- Encryption, classical encryption techniques, data encryptions standards, advance encryption techniques

Network Security- Kerberos, X.509, some network security projects- SDNS, DISNet, Project MAX, Secure NFS


Server security- security for network server, web servers, mobile technologies (java and java script etc)

Intrusion detection techniques – techniques to provide privacy in Internet Application and protecting digital contents (music, video, software) from unintended use, authentication.

System and Application Security- mail security (PGP etc) file System security, program and security, memory security, Sandboxing.

Security threads protection intruders- Viruses-trusted system.

Secure programming languages- concepts structured multiprogramming, shared classes, cooperating sequential processes, structure of te multiprogramming system RC-4000 software.

Books:
Cryptography

1. Introduction to cryptography, cryptosystems, communication channel used in cryptographic system, various types of ciphers, cryptanalysis of various cipher techniques types of attacks.

2. Various types of securities, joint and conditional probability, Baye’s theorem, independent random variables, perfect secrecy, average length encoding, entropy and huffman’s code, entropy, use of probability theory in key equivocation, entropy and redundancy in natural language, product cryptosystems.

3. Encryption and decryption using round functions, SPN, linear and differential cryptanalysis, DES, AES, various modes of operation.

4. Comparison of symmetric and public-key cryptographic systems, Euclidean and extended Euclidean algorithm, Chinese remainder theorem, RSA cryptosystems and its implementation, factoring algorithms, attacks on RSA, Rabin cryptosystems, semantic security of RSA.

5. Use of groups in discrete logarithm definition, ElGamal public-key cryptosystems, finite fields, elliptical curves, security of ElGamal cryptosystems.

6. Hash function and data integrity, security of hashing function, various types of problems like collision etc., iterated hash function, SHA, MAC, unconditionally secure MAC.

Introduction to signature scheme, security requirement for signature scheme, digital signature etc., provably secure signature schemes, undeniable signatures.

ADVANCED SOFTWARE ENGINEERING – (IS503)

This is a Research –oriented , seminar type course which will focus on the state of-the-art in various areas of Software Engineering –
Software Project Management, Metrics and measurement, Software configuration management, Software risk management, Requirements engineering ,
Software quality assurance, software reliability models.
Object oriented design, object oriented programming( with C++), Formal specifications, Formal verification of programs,
Jackson method for design, CASE tools and technology, Clean room method for software development, Information system design, Real-time software specification and design.
Role of architecture in software engineering: Enterprise architectures, Zachman’s Framework, Architectural styles, Design Patterns,
Architecture Description Languages, Product-Line architectures, Component Based Development.

• Books and References.

Ghazzi
Frank Buschmann, Regine Meunier, Hans Rohnert, PeterSommerland, Miachel Stal, Doughlas Schmidt Pattern Oriented Software Architecture, Volumes 1 & 2
Len Bass,Paul Clements, Rick Katzman, Ken Bass Software Architecture in
Practice.

George T. Heineman, William T. Councill. Component Based Software Engineering


Cyber Crime and Information Warfare (IS504)

Introduction of Cyber Crime, Categorizing cyber crime, perception of cyber criminals: hackers, insurgents and extremist groups,

Privacy, surveillance and protection, hiding crimes in cyberspace, encryption, anonymity and markets, privacy and security at risk in the global information society

Information Warfare- concept, information as an intelligence weapon, attacks and retaliation, attack and defense.

An I-War risk analysis model, implication of I-WAR for information managers,

Perceptual Intelligence and I-WAR

Handling Cyber Terrorism and information warfare, Web defacements and semantic attacks, DNS attacks

Cyber Law

Industrial espionage and cyber terrorism.

Book:


2) Information Warfare: Corporate attack and defense in digital world, William Hutchinson, Mathew Warren, Elsevier

Elective 1

Computer Vision & Image Processing (IS511)

Computer Vision- introduction of computer vision, computer imaging system, Image Formation
and sensing CVIP tools Software, Image representation

Digital Image Fundamentals


Image Enhancement in the Spatial Domain.


Image Enhancement in the Frequency Domain

Introduction to the Fourier Transform and the Frequency Domain, Smoothing Frequency-Domain Filters, Sharpening Frequency Domain Filters, Homomorphic Filtering.

Image Restoration.


Color Image Processing.


Image Compression.

Image Compression Models, Elements of Information Theory, Error-Free Compression,
Lossy Compression, Image Compression Standards.

Wavelets and Multiresolution Processing.


Detection of Discontinuities, Edge Linking and Boundary Detection, Thresholding, Region-Based Segmentation, Segmentation by Morphological Watersheds, The Use of Motion in Segmentation.

Object Recognition.

Patterns and Pattern Classes. Recognition Based on Decision-Theoretic Methods. Structural Methods.

Elective1- Information Theory and Coding (IS512)

Uncertainty, Information and Entropy Information Measures Characteristics on information measure, Shannon's concept of information, Shannon's measure of information, Model for source coding theorem communication system: Source coding ad line / channel coding, channel mutual information capacity (Bandwidth).

Channel coding, Theorem for discrete memory less channel, Information Capacity theorem: Error detecting & error correcting codes, types of codes: Block codes, Tree codes, Hamming and Lee Metrics, Description of linear block codes by matrices, Description of linear tree codes by matrices. Parity check codes, and Parity check polynomials.

Compression:

Loss less and lossy, Huffman codes, Binary image compression schemes, Run length encoding, CCIIT group 31-D compression, CCITT group 3 2D compression, CCITI group 4 2D compression.
Video Image Compression:


Keys: Single key (secret key) cryptography, two-key (public-key) cryptography. Single key cryptography

Ciphers: Block cipher codes, Stream ciphers, Requirement for secrecy, The Data Encryption Standard

Public Key Cryptography: Diffie-Hellman public key distribution, The Rivest-ShamirAdelman (R-S-A) system for public key cryptography.

Digital signature.

**NEURAL NETWORKS (IS513)**

**(ELECTIVE I)**

Contact Hours - Lectures - 3 Tutorial - 1


Adaptive multi-layer networks, prediction networks, radial basis functions, polynomial networks and regularization.

Difference between supervised and unsupervised learning, counter-propagation networks, adaptive resonance theory, neocognitron.

Hopfield networks, Boltzmann’s training, bi-directional associative memory networks.

Various types of optimization methods such as gradient descent, simulated annealing etc.
Applications of neural networks in the areas of clustering and classification problems, pattern recognition, function approximation, forecasting, vector quantization etc.

Books
2. Neural networks and fuzzy systems by Bart Kosko, Prentice Hall of India.

Elective 1: Advance Computer Architecture (IS514)
Overview of modern processor architectures.

Memory Hierarchy

Update vs. invalidation. The bus-based 'snooping' protocol design space. Scalable shared memory using directory-based cache coherency. MESI protocol.

Types of parallel machine

Replicated Architectures: SIMD/MIMD
Shared Memory and Distributed Memory
RISC, CISC Scalar processors, super Scalar and VLIW Computers

Multi-vector Computers

Connectivity Interconnection networks: topology, routing, flow control, deadlock avoidance, static and dynamic interconnection networks.

Virtual channels, wormhole routing and vertical cut-through.

Program and Network Properties

Conditions of parallelism

Program Partitioning and Scheduling

Program flow mechanisms

Principles of Scalable Performance

Performance Metrics and Measures

Parallel processing Applications

Speedup Performance laws

**LABORATORY – 1 (IS-541)**

**EXPERIMENTS RELATED TO COMPUTER SECURITY (IS-11) AND CYBER CRIME (IS – 12)**

**II – SEMESTER**

Security Assessment, Risk Management and Digital Forensics (IS551)

Network security assessment, tools required- free network scanning tools, comercial network scanning tools, protocol development assessment tools, internet host and network enumeration, NIC,DNS, IP network scanning- ICMP probing, TCP Port Scanning

Risk management- Importance, Process overview, asset identification, threat identification and assessment, the risk assessment
Effective and qualitative Risk analysis, value analysis, Facilitated Risk Analysis Process (FRAP)

Introduction of Software Forensics- Digital forensics definition, objectives, advance tools Dcc, JPlag, YAP

Assessing Remote Information Services , SNMP, LDAP, who, Security Assessment:

Case Studies for Implementing the Nsa Iam

Computer crime Investigation and Forensics

Industrial espionage and cyber-terrorism , principles of criminal law, computer forensic investigation, elements of personnel security and investigations, principles of risk and security management, conspiracy in computer crime, and computer fraud investigation.

Accessing remote information services, web services, remote maintenance services FTP database services, windows networking services, E-Mail services , IP VPN services, Unix RPC services,

Security audit

C security policies

Reference

Network security Assessment , Chris Mcnah, publication O’ Reilly

Database Security and Access control (IS552)

Purpose and fundamentals of access control, brief history, comparing RBAC to DAC and MAC

Access control policy,models and mechanisms, DAC policies, access control matrix,MAC policies and models, Biba’s intricity model, Clark-Wilson model, Domain type enforcement model

Core RBAC features- core RBAC , mapping the enterprise view to the system view, Role hierarchies- inheritance schemes, hierarchy structures and inheritance forms
SoD and Constraints in RBAC systems-types of SoD, using SoD in real system,
Temporal Constraints in RBAC, RBAC, MAC AND DAC.

Integrating RBAC with enterprise IT infrastructures: RBAC for WFMSs, RBAC for UNIX and JAVA environments

Case study: Multiline Insurance Company

Smart Card based Information Security

Smart card operating system—fundamentals, design and implantation principles, memory organization, smart card files, file management, atomic operation, smart card data transmission ATR, PPS

Security techniques—user identification, smart card security, quality assurance and testing, smart card life cycle—5 phases, smart card terminals

**TECHNICAL FOUNDATION FOR E-COMMERCE (IS553)**

**(MANAGERIAL COURSE)**

Auctions and trading mechanisms, safe exchange, payment mechanisms and protocols, searching hyperlinked structures, data mining, copyright protection and security, web software infrastructures, personalization and tracking, Integration of catalogs and other trading information

**WIRELESS AND MOBILE COMPUTING (IS554)**

1. Introduction


Modern Wireless Communication Systems

2G/2.5G/3G/4G Wireless Networks and Standards, Wireless in Local loop & LMDS

Cellular Concepts
Frequency spectrum, frequency reuse, channel assignment strategies, handoff strategies, interference and system capacity, fundamentals of antennas, Equivalent circuit for antenna, Antennas as cell site, Mobile antennas, Analog Vs Digital, Spectrum regulation, Licensing methods.

2. Cellular Networks

Mobile Radio Propagation, A basic cellular system, Performance criterion, Operations of Cellular Networks, Concept of frequency reuse Channels, Co channel Interference and it's reduction factor, types of non co channel Interference, Desired C/I from normal case on omni directional antenna systems, Digital Modulation

3 Multi Access Technique & Wireless Standards

TDD, FDD, Rake receiver, CDD, Spread spectrum, (direct and frequency hopping)
FDMA, TDMA, CDMA, Wireless Standards GSM, CDMA, DECT, UMTS & IMT-2000,
WAP Model and architecture, Gateway, Protocol stack, Wireless Application environment

4 Wireless LAN

IEEE 802.11 Concepts, MAC Layer, Spread Spectrum Wireless LAN, Infrared Wireless LANs, Other

Physical Layer Protocol (IEEE 802.11b, IEEE 802.11a), Wireless PAN (Bluetooth), HIPERLAN, Mobile

Network Layer (Mobile IP), Mobile Transport Layer (Mobile TCP), Mobile Data network (GPRS),

5 GSM Systems Overview

Architecture, Location tracking, and call setup. Security, Data Services N/W Signaling,
GSM mobility management, Operations, Administration and maintenance.

GSM bearer Services
SMS architecture-Protocol Hierarchy, DTE-DCE interface, Mobile prepaid phone services.

References
1) Wireless communication, T. S. Rappaport, PHI
3) Mobile Communications, J. Schiller, Pearson Education

Elective 2
Distributed System (IS561)
Communication: Layered protocols, Client server protocols, RPC, group communication.
Coordination, synchronization & consistency: Logical clocks, Physical clocks, mutual exclusion, election algorithms, atomic broadcast, sequential consistency transaction distributed consensus,
Threads: Thread synchronization, implementation issues, threads vs. RPC.
Models of distributed computing: client server and RPC, RPC architecture, exceptions, underlying protocols, IDL, marshalling etc.
Group models and peer to peer: Groups for service replication/ reliability, groups for parallelism / performance, client/ server vs. peer to peer, multicast, atomic broadcast.
Distributed file system: security, Naming/ location transparency, R/W semantics, cache coherence, replication.
Distributed shared memory: DSM architecture, consistency models and relation to caching, release consistency, comparison with message passing and RPC.
Fault tolerant distributed systems: Introduction, dependability, faults vs. errors vs. failure, space time and value redundancy, fault tolerant architecture, failure detection algorithms,
partitioning, FT consensus.

Distributed multimedia system: Introduction, characteristics, resource management stream adaptation.

Security: introduction, security techniques, cryptographic algorithms, authentication and access control.

Case study: CORBA, MACH

**Elective 2**

Game Theory and its Applications (IS562)

Basics of game theory; Different types of games: two party, multiparty games, coalition games on graphs; Nash equilibrium; Walsarian and other equilibria, Analysis of optimal strategies; Applications of game theory (network economics, bandwidth allocations, etc.)


Object Oriented Modeling and Design (IS563)

**ELECTIVE - II**

Object Oriented Concepts and Modeling Techniques

Design Methodology

OMT methodology, Analysis, Overview of system design, Subsystem, concurrency, Common architectural frameworks designing algorithm, Design optimization, Implementation of control, Design of Associations, Object design, Class design, Comparison of design methodology with SASD, JSD and others.

Implementation

Programming style, Reusability, Extensibility, Programming in the large, Translating a design into an Implementation class definition, Object oriented Language features, Survey of object-oriented languages, Object storage and relation with database.

Advanced Topics

Distributed objects, Components development, Introduction to Distributed object system like CORBA, EJB, COM+, DCOM, and other design architectures.

High Performance Computing (IS564)

Elective II

Contact Hours - Lectures - 3, Tutorial - 1

Introduction to high performance computing: cluster, grid, meta-computing, middleware etc., examples of representative applications.

Programming models: shared memory, message passing, peer-to-peer, broker-based.

Introduction to PVM and MPI.

Architecture of cluster-based systems, Issues in cluster design: performance, single-system-
image, fault tolerance, manageability, programmability, load balancing, security, storage..


Shared-memory processing: Architectures (extensions of the memory hierarchy), Programming paradigms, OpenMP

Distributed-memory processing: Architectural issues (networks and interconnects), Programming paradigms, MPI (+MPI2)

Grids: Computational grids, Data grids, Architecture of Grid systems, Grid security infrastructure.

Examples of Grids: Globus etc

Performance issues and measurement: Profiling and development tools, Sustained versus peak performance, Performance libraries and packages

The productivity crisis & future directions: Development overheads, Petaflops programming, New parallel languages: UPC, Titanium, Co-Array FORTRAN

BOOKS:

Laboratory II (IS591)

Experiment related to Security Assessment, Risk Management & Digital Forensics (IS-21), Database Security & Access Control (IS-22), Wireless and Mobile Computing (IS-
III – Semester

Bio metrics and Human Interface (IS601)

Unit I

Overview of Biometrics: Definitions, biometric modalities, course outline,..

Basic applications: access control, e-commerce, forensics...

Design of a Biometric System: Building blocks, Modes of operation,…

Unit II

Fingerprint verification: Minutiae Based Fingerprint Matching, Non-minutiae Based Representations,

Fingerprint Enhancement, and Fingerprint Classification.

Face Recognition:- Introduction, Authentication vs. Identification, Challenges in Face recognition,

Algorithms for face recognitions.

Unit III

Iris Recognition: Introduction, devices for capturing Iris, Iris representation schemes, Iris recognition

algorithms.

Biometrics based on hand geometry, signature, ear, palm, voice and DNA.

Unit IV

Multimodal Biometrics: Limitations of unimodal systems, multibiometric scenarios, levels of fusion,

system design, score fusion techniques, score normalization, user-specific parameters, and soft biometrics.

Unit V
WIRELESS AND MOBILE SECURITY(IS602)

Wired/wireless networks; Effect of mobility on networks, and systems; Impact on IP stack from MAC layer and up; ad-hoc and sensor networks; wireless broadcast, IP broadcast, Satellite broadcast; issues of information capacity; distinction between wired and wireless networks from information theory; Issues of security in wireless; issues of 802.11 protocols; routing in wireless networks, design of secure protocols: key distribution for access control, source authentication of transmissions and nonrepudiation; Power management and selfishness issues, attacks in wireless networks; DOS and DOS attacks, reaction to attacks, information processing for sensor networks

Optical network security

Opto-electronic networks, all optical networks: fibers, amplifiers and wavelength selective switches (WSSs), QoS , security architectures, physical security, Vulnerabilities and attacks, service disruption(SD) , tapping, jamming, reaction to attacks
Elective III Random Algorithms (IS611)

Unit I:
Introduction, A min-cut algorithm, Las Vegas and Monte Carlo, Binary planar partition,
A probabilistic recurrence, Computational models and time complexity.

Unit II:
Markov Chains and Random Walks: A 2-sat example, Markov chains, Random Walks on
graphs, Cover times, Graph connectivity.

Unit III:
Random Data Structure : The fundamental data structure problem, Treaps, skip lists,
Hash tables, Hashing with O(1) time.

Unit IV:
Geometric algorithms and Linear programming:
Randomized incremental construction, Convex Hulls in the plane, Duality, Half space
Intersection, Delaney triangulation, Trapezoidal decomposition, Binary Space partition,
The diameter of point set, Random sampling, Linear programming.

Graph algorithms: All pairs shortest paths, The min cut problem, Minimum Spanning
tree,

Unit V:
Parallel and Distributed Computing: The PRAM Model, Sorting on a PRAM, Maximal
independent sets, Perfect Matching, The choice coordinate problem, Byzantine
Agreement.

Text book:- Randomized Algorithm by Motwani and Raghavan, Cambridge press
Elective III QUANTUM COMPUTING (IS612)

Unit-I


Unit-II

Introduction to Computer Science: Models for computation, Analysis of computational problems, Perspectives on computer science

Quantum Circuits: Quantum algorithms, Summary of Quantum circuit model of computation, Simulation of Quantum systems

Unit-III

The Quantum Fourier Transform and its applications: Phase estimation, order finding and factoring.

Applications of Quantum Fourier Transform

Quantum search algorithms, Quantum search as a quantum simulation, quantum counting, speeding up the solution of NP-complete problems, quantum search of an unstructured database, optimality of the search algorithm, black box algorithm limits

Unit –IV

Quantum computers: physical realization, guiding principles, conditions for quantum computation, harmonic oscillators quantum computer, optical photon quantum computer, optical cavity quantum electrodynamics, Ion traps, Nuclear magnetic resonance.

Quantum noise and quantum operations: classical noise and Markov process, quantum
operation, examples, application, limitations

Unit V

Distance measures for quantum information, quantum error correction, the Shor code,
Theory of quantum error – correction, Constructing quantum code, stabilizer codes,
Fault- tolerance quantum computation.

Embedded System & Electronic Design Automation IS613

Introduction: Embedded systems overview and their characteristics, Design Challenges and
issues in embedded software development, Processor Technology, IC Technology, Design
Technology. Verilog programming

Hardware & electronics fundamentals for software engineers, categories of different processor
microprocessor & microcontroller, study of 8051, PIC microcontroller, AVR microcontroller,
68000 series computers, DSP based controller, etc, assembly language programming for above
controller.

General Purpose processor: Basic Architecture, Operation, Programmer’s view, Development
environment, ASIPs, selecting processors, General Purpose processor design.

Peripherals: Timer, Counters Watchdog timers, UART, PWM, LCD Controller, Keypad
Controller, Stepper motor controller, Analog-to-digital Converters, Real-time clocks.

Memory: Memory write ability, common memory types, Composing memory, memory
hierarchy

and cache, advanced RAM,

Interfacing: Communication Basics, Microprocessor Interfacing: I/O Addressing,
Microprocessor Interfacing: Interrupts, Microprocessor Interfacing: Direct Memory Access,
Arbitration, Multilevel Bus Architectures, Advanced Communication Principles, Serial
Protocols, Parallel Protocols, Wireless Protocols

Examples of Embedded systems: Digital Camera Examples, Embedded database applications, etc


Control Systems: Open-Loop and Closed-Loop Control Systems, General Control Systems and PID Controllers, Software Coding of a PID Controller

IC Technology: Full-Custom (VLSI) IC Technology, Semi-Custom (ASIC) IC Technology, Programmable Logic Device (PLD) IC Technology

Hardware Software Partitioning,


Advance topics in Embedded systems

Text Books:

1) Embedded system Design, Frank Vahid, Tony Givargis, John Wiley & Sons

2) 8051 Microcontroller & Embedded Systems, Rajiv Kapadia, Jaico Books
3) The 8051 Microcontroller & Embedded Systems, Mazidi & Mazida, Pearson education

4) Embedded systems, Rajkamal, TMH

ADVANCE COMPUTER NETWORKS(IS614)

Contact Hours - Lectures - 3, Tutorial - 1

Review of networking concepts: Network models, Addressing, Data rate limits, Bandwidth, throughput, Latency

Multiple Access: Random Access, Aloha, CSMA, CSMA/CD, CSMA/CS, Controlled Access, Reservation, Polling, Token Passing, FDMA, TDMA, CDMA

Standard Ethernet, Fast Ethernet and Gigabit Ethernet, SONET, ATM, QoS in ATM, ATM applications

Residential broadband (High speed access to home): ADSL, Cable modems, Hybrid- Fiber Coax

IPv4, IPv6, IP Security, Virtual Private Networks

Multimedia Networks: Voice/Video over IP, IP Telephony, Voice over ATM, AAL2

Quality of Service in Data Networks, Wavelength division multiplexing (WDM) Optical DWDM Networks, IP over DWDM


Advance Operating system

IS 615


SRT/multimedia scheduling.

Translation schemes. Demand paging/segmentation. Replacement strategies:
OPT, FIFO, LRU (and approximations), NRU, LFU/MFU, MRU. Working set
Storage systems. Basic I/O revisited. Disks I/O. Disk scheduling: FCFS,
SSTF, SCAN, C-SCAN, etc. Logical volumes. RAID. Disk caching; motivation,
Unix buffer cache, NT cache manager. Filing systems: file mapping
algorithms, metadata, and name-space. Directory implementation. Integrity
management. Examples: FAT, FFS/EXT2, NTFS, LFS.
Authentication schemes. Access matrix: ACLs and capabilities. Combined
scheme. Covert channels.
References:
• Bacon, J. & Harris, T. (2003). Operating systems (3rd ed.). Addison-Wesley.
concepts. Addison-Wesley (5th ed.).
Leffler, S. (1989). The design and implementation of the 4.3BSD Unix
operating system. Addison-Wesley.
Press (3rd ed.).
• Singhal, M. & Shivaratri, N. (1994). Advanced concepts in operating systems:
distributed, database, and multiprocessor operating systems. McGraw-Hill.