MTCF-101 Operating Systems and Security

UNIT I

Evolution of operating systems, basic operating system functions, understanding how operating systems work, the kernel, resource managers, device drivers, the role of application software, the role of BIOS, mainframe systems, desktop systems, multiprocessor systems, distributed systems, clustered systems, network operating system, handheld system, operating system services, operating system structure, system calls, system programs, operating system design & implementation, types of operating systems

UNIT II

Process Concept, process scheduling, operations on processes, cooperating processes, inter-process communication, multithreading models, CPU scheduling algorithms, critical section problem, semaphores, classical problems of synchronization, critical regions, monitors, atomic transactions, deadlock characterization, methods for deadlock handling, Swapping, paging, segmentation, demand paging, page replacement, thrashing, file concept, access methods, directory structure, file sharing, file system implementation, disk storage basics, block allocation, partitions, formatting, Windows file system, Unix file system, disk scheduling.

UNIT III

Introduction to security in operating system, requirements for operating system security, secure operating systems, the security problem, protection mechanisms, domain of protection, user oriented access control, data oriented access control, access matrix, implementation of access matrix, access rights, language based protection, user authentication, threat model, program threats, system threats, malicious software, intruders, security vulnerabilities, security violations, securing systems and facilities, implementing security defenses, file sharing, file system security, Trojan horse defense,

UNIT IV

Multics security, UNIX security, windows security, verifiable security goals, security kernels, secure capability systems, secure virtual machine systems

UNIT V

Trusted operating system, trust vs. security, trust model, trusted computing base, security policy, models of security, trusted operating system design, security features of trusted operating system, assurance in trusted operating systems.

Refrerences:

1.Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, “Operating System Concepts”, Sixth Edition, John Wiley & Sons (ASIA) Pvt. Ltd, 2003.
2. William Stallings, “Operating System”, Prentice Hall of India, 4th Edition, 2003.
3.Pramod Chandra P. Bhatt , “An Introduction to Operating Systems, Concepts and Practice”, PHI, 2003.
4. Trent Jaeger, “Operating system Security”, Morgan and Claypool publishers, 2008

MTCF-102 Database Security and Privacy

UNIT: 1

DBMS Concepts Introduction, Data models, Entities and attributes, Relationships, E-R diagram. Relational Data models: Domains, Tupples, Attributes, Keys, Relational database, Schemas, Integrity constraints. Relational algebra and relational calculus, Normalization, Normal forms.HASH-BASED INDEXING: Static hashing; Extendible hashing, Linear hashing, comparisons, Query Processing and Optimization. Distributed databases: client/server database Fragmentation, Replication, Location & Fragment transparency, Distributed Query Processing and Optimization.

UNIT :2

Database Protection: Integrity, Constraints in Query-by-Example, Security, Security in query-by-Example, Security in Statistical Databases. Concurrent Operations on the Database: Basic Concepts, A simple Transaction Model, Model with Read- and Write-Locks, Read-only, Write-only Model, Concurrency for Hierarchically Structured Items, Protection against Crashes, Optimistic Concurrency Control.

UNIT :3

Security Principle, E-mail Security, database Recovery Criteria, Database Security, Security Management System Architecture, , develop continuity and Recovery Plans, Physical And Environmental Security, Security plan for implementation, Goals of data base security, Access control, Statistical database security

UNIT :4

Security Perimeter, Relationship Between a Security Policy and a Security Model, State Machine Models, Confidentiality and Integrity models, Bell-LaPadula Model, Biba Model, Bell-LaPadula versus Biba, Clark-Wilson Model, Information Flow Model, Noninterference Model, Brewer and Nash Model, Graham-Denning and Harrison-Ruzzo-Ullman Models, access matix models.

UNIT :5

Security Management, Data/ information, protecting Password file, Access Control Structure, Software Security, Element of Information Security, Steps for Better Security, Malicious Software, System Security Assurance Concepts, Importance of Information System,

References:

1. R. Elmasri, S. Navathe, Fundamentals of Database System, Pearson Education.
2. C.J. Date, An Introduction to Data base Systems, Volume I, Pearson Education.
3. Databse Systems, SK Singh, Pearson Education.
4. H. F. Korth and A. Silberschatz. Database Concept, TMH .
5.Godbole, ”Information system security”, Wiley.
6.Cole.Krutz & Conley “ Network security” Wiley.

MTCF-103 Cyber Law and Emerging Jurisprudence

UNIT: 1

Introduction:Defining Cyber Space, Cyber Law and IT Act 2000, Jurisdiction in Cyber Space, Contracts, Electronic Contracts, Cyber Contracts and Indian Legal Position.

UNIT: 2

Faith in Cyber World: Digital Signature and Electronic Signature, Electronic Governance, Internet Governance.

UNIT: 3

Cyber Crimes: Introduction to Cyber Crimes, Law Relating to Cyber Crimes, Procedural Law & Other Laws Relating to Cyber Crime, Evidence Act.

UNIT: 4

International Laws and Cyber Crimes: Cyber Crime in International Perspective.

UNIT: 5

Case Laws: Study of Landmark Cases relating to Cyber Crime

(1) Hacking.	(2) Obscenity & Pornography.	(3) Cyber Stalking
(4) Cyber Terrorism.	(5) Identity Theft.	(6) Cyber Fraud.

References:

1) The Indian Cyber law with Cyber glossary, Suresh T. Vishwanathan, New Delhi, Bhart Law House, 2000.
2) Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives, Nina Godbole, Sunit Belapure, Wiley India
3) Law of Cyber Crimes and Information Technology Law, S.V. JogaRao, 2007.
4) Cyber Law, Cyber Crime Internet and E-Commerce, Vimlendu Tayal.
5) Information Technology Law and Practice, Vakul Sharma.

MTCF-104 E-Commerce Security

UNIT: 1

Introduction to E-commerce: Operating System Services, Advantages and Disadvantages of E – Commerce, Developer Services, Data Services, Application Services, Store Services, Client Services, Types of E Commerce Solutions- Direct Marketing and Selling, Supply Chain Integration, Corporate Procurement.

UNIT: 2

Business Models for E-Commerce: E-Business models based on Relationship of Transaction Parties, Brokerage Model, Aggregator Model, Info-mediary model, Community Model, Value chain model, Manufacturer model, Advertising Model, Subscription model, E- Marketing – Identifying Web Presence Goals, BowsingBehaviour Model, Building Customer Relationship Based on One – to – One Marketing, E – branding, Elements of Branding, Spiral Branding.

UNIT:3

Electronic Data Interchange: Evolution, uses, Benefits, Working of EDI,EDIStandards(includes variable length EDI standards),Cost Benefit Analysis of EDI, ElectronicTrading Networks, EDI Components, File Types ,EDI Services,EDI Software, Business Approach of EDI, EDIFACT(Overview, Structure, EDIFACTSoftware),Business Future of EDI,EDI Administration.EDI Security, Digital signatures, Digital Certificates, Cryptography export restrictions, Secure Sockets Layer(SSL), Secure Electronic Transactions (SET),Smart Cards and its applications, WAP, WAP Architecture, WAP Programming Model.

UNIT: 4

Electronic Payment Security: Electronic Payment Systems – Electronic Commerce, Offline Versus Online, Debit Versus Credit, Macro versus Micro, Payment Instrument, Electronic Wallet, Smart Cards, Electronic Payment Security. Payment Security Services – Payment Transaction Security, Digital Money Security, Electronic Check Security, Availability and Reliability, Electronic Payment Framework.

UNIT: 5

Security on the Web&Mobile : Network and Website Security Risks, HTTP Cache Security Issues, HTTP Client Authentication, Web Transaction Security, Web Server Security, Web Client Security, Mobile Agent Security – mobile Agents, Security Issues, Protecting Platforms from Hostile Agents, Smart Card Security, Firewall Concept, Firewall Components, Benefits of an Internet Firewall, Enterprise-Wide Security Framework, Secure Physical Infrastructure.

References:

1) E-Commerce: Fundamentals and Applications, Henry Chan, Wiley India
2) E-Commerce An Indian Perspective, P.T.Joseph, S.J., PHI.
3) Electronic Commerce: Greenstein, Merylin, Tata Mc.Graw Hill.
4) E-Commerce Business.Technology. Society, Kenneth C. Laudon, Carol Guerico Traver, Pearson Education.

MTCF-105 Cryptography and Network Security

UNIT: 1

An overview of computer security ,Goals of information security, confidentiality, integrity, Availability, Security policies: Types of access control, Basic cryptography, OSI security architecture , Classical encryption techniques, Cipher principles, Data encryption standard, Block cipher design principles and modes of operation, Evaluation criteria for AES, AES cipher, Triple DES, Placement of encryption function, Traffic confidentiality.

UNIT: 2

Authentication: Authentication basics, Passwords, Key management , Diffie Hellman key exchange , Elliptic curve architecture and cryptography , Introduction to number theory , Confidentiality using symmetric encryption , Public key cryptography and RSA.

UNIT: 3

Security Attacks, Trojan Horses, Security Services, Security Mechanisms, and a Model for Network Security ,Non Cryptographic Protocol Vulnerabilities DoS, DDoS, Session Hijacking and Spoofing, Software Vulnerabilities,Phishing, Buffer Overflow, Format String Attacks, SQL Injection, Basics of Cryptography Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Other Cipher Properties Confusion, Diffusion, Block and Stream Ciphers.

UNIT: 4

SQL injection and cross-site scripting, symmetric encryption, SSL and TLS, PKI and Certificate Systems, Passwords and Secure Cookies, IPsec, Ingress filtering, and Firewalls, Digital signatures, Digital Signature Schemes, Authentication Protocols, Digital Signature Standards, files and devices, Program security,

UNIT: 5

Intrusion Detection ,Firewalls and proxy, Image Security-Biometrics, Web Security: Web Security Considerations, Secure Sockets Layer and Transport Layer Security, Electronic Payment Combining security Associations, Internet Key Exchange, Virus and worms.

References:

1) Introduction to computer security by Matt Bishap Sathyanarayana S.Venkatramanayya.
2) Cryptography and network security by Atual Kahate, TMH
3)Cryptography and network security: Principles and Practice: Fourth or Fifth Edition By William Stalling, Printice Hall.
4) Network security Essentials: Application and Standards by William Stallings, Prentice Hall.
5) Cryptography and Security: Padmanabhan, Wiley India