M.Tech

In

Computer Science and Engineering

With

Specialization in

Cyber Forensics and Information Security

Scheme and Syllabus

COLLEGE OF ENGINEERING KALLOOPPARA

Kadamankulam P.O,Kallooppara,Pathanamthitta(Dist),Kerala-689603

Email:*engpta@gmail.com* **Web:***http://www.cek.ac.in*

SCHEME

Semester I

Course Code	Name of Course	Core/ Elective	Credits	Lec.	Lab	Marks		Total Marks
						Intl	Extl	
CSCF3101	Engineering Mathematics and Statistics for Forensic Science	C	4	3	3	50	50	100
CSCF3102	Computer Algorithms	C	4	3	3	50	50	100
CSCF3103	Cyber Forensics Basics	C	4	3	3	50	50	100
	Elective 1	E	3	3	0	50	50	100
	Elective 2	E	3	3	0	50	50	100
	Total for Semester I		**18**	**15**	**9**	**250**	**250**	**500**

Semester II

Course Code	Name of Course	Core/ Elective	Credits	Lec.	Lab	Marks		Total Marks
						Intl	Extl	
CSCF3201	Advanced Operating Systems Concepts	C	4	3	3	50	50	100
CSCF3202	Network Security	C	4	3	3	50	50	100
CSCF3203	Seminar	C	1	0	3	50	-	50
	Elective 3	E	3	3	0	50	50	100
	Elective 4	E	3	3	0	50	50	100
	Elective 5	E	3	3	0	50	50	100
	Total for Semester II		**18**	**15**	**9**	**300**	**250**	**550**

Semester III

Course Code	Name of Course	Core/ Elective	Credits	Lec.	Lab	Marks		Total Marks
						Intl	Extl	
CSCF3301	Project & Viva Voce	C	18	0	24	200	200	400
	Total for Semester III		**18**	**0**	**24**	**200**	**200**	**400**

Semester IV

Course Code	Name of Course	Core/ Elective	Credits	Lec.	Lab	Marks		Total Marks
						Intl	Extl	
CSCF3401	Project & Viva Voce	C	18	0	24	200	200	400
	Total for Semester IV		**18**	**0**	**24**	**200**	**200**	**400**

List of Electives

Course Code	Name of Course
CSCF3104	Applied Cryptography
CSCF3105	File System Forensics Analysis
CSCF3106	Information Security Basics
CSCF3107	Software Forensics
CSCF3204	Virtual Forensics
CSCF 3205	Information Security Governance
CSCF3206	Malware Forensics
CSCF3207	Windows and Linux Forensics Analysis
CSCF3208	Ethical Hacking

SEMESTER I - CORE SUBJECTS

CSCF 3101 Engineering Mathematics and Statistics for Forensic Science

Unit 1:

Counting- Basic counting-The Sum Principle, Abstraction, Summing consecutive integers, The Product Principle, Two-Element subsets, Important Concepts, Formulas, and Theorems, Counting Lists, Permutations and Subsets- Using the Sum and Product Principles, Lists and functions, The Bijection Principle, *k*-element permutations of a set, Counting subsets of a set, Binomial coefficients-Pascal's Triangle , A proof using the Sum Principle, The Binomial Theorem, Labeling and trinomial coefficients, equivalence relations and counting-The Symmetry Principle, Equivalence Relations, The Quotient Principle, Equivalence class counting, Multisets, The bookcase arrangement problem, The number of *k*-element multisets of an *n*-element set, Using the quotient principle to explain a quotient.

Unit 2:

Functions, Functions as relations, One -to-One, Onto and Invertible functions, Mathematical functions, Exponential and Logarithmic functions, Sequences, Indexed classes of Sets, Recursion, First order linear recurrences, Iterating a recurrence, Geometric series, First order linear recurrences, Recursively defined functions, Cardinality, Algorithms and functions, Complexity of algorithms, Mathematical Induction, Strong Induction, Induction in general, Graphs- The degree of a vertex, Paths, Connectivity, Cycles, Trees, Other Properties of Trees, Multigraphs, Planar graphs, Representing graphs in computer memory, Graph algorithms, Directed graphs, Basic definitions, Spanning trees, Rooted Trees, Warshall'salgorithm: Shortest paths, Linked representation of directed graphs, Pruning algorithm for shortest path, Dijkstra's shortest path algorithm, Matching Theory- The idea of a matching, Making matchings bigger, Matching in Bipartite Graphs, The Augmentation-Cover algorithm.

Unit 3:

Cryptography and Modular Arithmetic, Introduction to Cryptography, Private Key cryptography, Public-key Cryptosystems, Arithmetic modulo *n*, Cryptography using multiplication mod *n*, Solutions to Equations and Inverses mod *n* , Inverses mod *n* , Converting Modular Equations to Normal Equations, GCD, Euclid's Division Theorem, The GCD Algorithm, Extended GCD algorithm, Computing Inverses, Exponentiation mod *n* , The Rules of Exponents, Fermat's Little Theorem, The RSA Cryptosystem, The Chinese Remainder Theorem, Practical Aspects of Exponentiation mod *n* ,Finding large primes.

Unit 4:

Recursion Trees, Three Different Behaviors, Master Theorem, Solving More General Kinds of Recurrences, Recurrence Inequalities, Recurrences and Selection, The idea of selection, A recursive selection algorithm, Selection without knowing the median in advance, An algorithm to find an element in the middle half, Uneven Divisions.

Unit 5:

Introduction to Probability, Some examples of probability computations, Complementary probabilities, Probability and hashing, The Uniform Probability Distribution, The probability of a union of events, Principle of inclusion and exclusion for probability, The principle of inclusion and exclusion for counting, Conditional Probability, Independence, Tree diagrams, What are Random Variables?, Binomial Probabilities, Expected Value, Expected Values of Sums and Numerical Multiples, Probability Calculations in Hashing, Conditional Expectations, Recurrences and Algorithms, Probability Distributions and Variance.

Text books

1. Discrete Mathematics for Computer Science- Kenneth Bogart, Clifford Stein, Key Curriculum Press, 2006
2. Schaum's Outline Discrete Mathematics - Seymour Lipschutz and Marc Lipson,Third Edition, McGraw Hill, 2007.

References

1. Discrete Mathematics using a Computer- John O' Donnell, Cordelia Hall, Rex Page, Springer- Verlag, 2006
2. Discrete Mathematics with Algorithms- M.O. Albertson, J.P.Hutchinson, John Wiley & Sons, 1988
3. Miquel A. Lerma, Notes on Discrete Mathematics
4. Keneth H. Rosen: Discrete Mathematics and Its Applications, Fifth Edition, 2003, McGraw Hill.

CSCF 3102 Computer Algorithms

Unit 1:

The role of algorithms in computing, Insertion sort, Analyzing algorithms, Designing algorithms, Growth of functions- Asymptotic notations, Standard notations & common functions, Divide-and-Conquer – The maximum-subarray problem, Strassen's algorithm for matrix multiplication, The substitution method for solving recurrences, The recursion-tree method for solving recurrences, The master method for solving recurrences, Proof of the master theorem, Probabilistic analysis and randomized algorithms- The Hiring problem, Indicator random variables, Randomized algorithms, Probabilistic analysis and further uses of indicator random variables.

Unit 2:

Heap sort- Heaps, Maintaining the Heap property, Building a heap, The heapsort algorithm, Priority queues, Quicksort- Description of quick sort, Performance of quick sort, A randomized version of quicksort, Analysis of quicksort, Sorting in Linear time - Lower bounds for sorting, Counting sort, Radix sort, Bucket sort, Medians and Order statistics- Minimum and Maximum, Selection in expected linear time, Selection in worst-case linear time.

Unit 3:

Hash tables- Direct-address tables, Hash tables, Hash functions, Open addressing, Perfect hashing, Binary search trees, Randomly built binary search trees, Red-black tree- Properties, Insertion, Deletion, Rotations, Augmenting Data Structures- Dynamic order statistics, Interval trees, Dynamic programming- Rod cutting, Matrix chain multiplication, Longest common subsequence, Optimal binary search trees, Greedy Algorithms- An activity selection problem, Elements of the greedy strategy, Huffman codes, Matroids and greedy methods, A task scheduling problem as a matroid, Amortized analysis- Aggregate analysis, the Accounting method, The potential method, Dynamic tables.

Unit 4:

B-Trees, Fibonacci Heaps, van Emde Boas trees, Data structures for disjoint sets, Graph Algorithms – BFS, DFS, Topological sort, strongly connected components, Growing a minimum spanning tree, The algorithms of Kruskal and Prim, The Bellman-Ford algorithm, Single-source shortest paths in directed acyclic graphs, Dijkstra's algorithm, Difference constraints and shortest paths, Proofs of shortest-paths properties, Shortest paths and matrix multiplication, The Floyd-Warshall algorithm, Johnson's algorithm for sparse graphs, Flow networks- The Ford-Fulkerson method, Maximum bipartite matching, Push-relabel algorithms, The relabel-to-front algorithm.

Unit 5:

The basics of dynamic multithreading, multithreaded matrix multiplication, multithreaded merge sort, Symmetric positive-definite matrices and least squares approximation, The simplex algorithm, Duality, The naive string-matching algorithm, The Rabin-Karp algorithm, String matching with finite automata, The Knuth-Morris-Pratt algorithm, Line-segment properties, segments intersections, convex hull, closest pair of points, Polynomial-time verification, NP-completeness and reducibility, NP completeness proofs, The vertex-cover problem, The travelling-salesman problem, The set-covering problem, The subset-sum problem

Text Books:

1. Computer Algorithms- Horowitz, Sahni, Rajasekharan, Silicon Press, 2nd edition, 2008
2. Cormen, Thomas H, Leiserson, Charles E & Rivest, Ronald L, 'Introduction to Algorithms', Prentice Hall of India Private Limited, New Delhi, Third Edition, 2009

References:

1. Algorithms- Robert Sedgewick, Kevin Wayne, Pearson Education, 2011
2. Sahni, 'Data Structures, Algorithms and Applications in C++', Silicon Press, 2nd edition, 2004
3. Algorithm Design: Jon Kleinberg and Eva Tardos, AW (2005)
4. Anany V. Levitin. Introduction to the Design & Analysis of Algorithms (2nd Ed): A W (2006)
5. TheAlgorithm Design Manual(2nd Ed): Steven S. Skiena, Springer(2008)
6. Computer Algorithms: Introduction to Design and Analysis (3rd Ed): Sara Baase and Allen Van Gelder. AW (1999)

CSCF 3103 Cyber Forensics Basics

Unit 1:

Introduction to Computer Forensics, history of computer forensics, understanding case law, developing computer forensics resources, preparing for computer investigations, understanding law enforcement agency investigations, understanding corporate investigations, maintaining professional conduct, Understanding Computer Investigations -Preparing a computer investigation, taking a systematic approach, procedures for corporate high tech investigations, understanding data recovery workstations and software, conducting an investigation, completing the case, Requirements for forensic lab certification , determining the physical requirements for a computer forensics lab, selecting a basic forensic workstation, building a business case for developing a forensic lab.

Unit 2:

Data Acquisition - storage formats for digital evidence, determining the best acquisition method, contingency planning for image acquisitions, using acquisition tools, validating data acquisitions, performing RAID data acquisitions, using remote network acquisition tools, using other forensic acquisition tools, Processing Crime and Incident Scene-identifying digital evidence, collecting evidence in private sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene . Seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash.

Unit 3:

Working with windows and DOS systems- file systems, exploring Microsoft file structures, examining NTFS disks, whole disk encryption, the windows registry, Microsoft and Ms-DOS start up tasks, virtual machines, Evaluating Computer Forensic s Tool needs, computer forensics software and hardware tools, validating and testing forensics software. the Macintosh file structure and boot process, examining UNIX and LINUX disk structures and boot processes, examining CD data structures, examining SCSI Disk, examining IDE/EIDE and SATA devices.

Unit 4:

Analysis and validation -determining what data to collect and analyze, validating forensic data, addressing data -hiding techniques, performing remote acquisitions. Recovering Graphics Files-Recognizing ,locating and recovering graphic files, understanding data compression, copy rights issues with graphics, identifying unknown file formats, copyright issues with graphics. Network Forensics-overview, performing live acquisitions, developing standard procedures for network forensics, using network tools. Email Investigations-role of E-mail in investigations, exploring the roles of the client and server, investigating e-mail crimes and violations, understanding E-mail servers, specialized E-mail forensic tools. Cell Phone and Mobile Device forensics- Mobile device forensics, acquisition procedures for cell phones and mobile devices.

Unit 5:

Report writing for high tech investigations – importance of reports, guidelines for writing, generating report findings with forensics software tools. Expert Testimony in High Tech Investigations- Preparing for testimony, testifying in court, preparing for a deposition or hearing, preparing Forensic evidence for testimony. Ethics for the Expert Witness-applying ethics and codes to expert witnesses, organizations with codes of ethics, ethical difficulties in expert testimony.

TEXT BOOK:

1. Computer Forensics and Investigations- Bill Nelson, Amelia Phillips, Frank Enfinger, Christofer Steuart , Second Indian Reprint 2009, Cengage Learning India Private Limited**.**

2. Digital Evidence and Computer Crime – Eoghan Casey, Edition 3, Academic Press,2011

3. Computer Forensics and Cyber Crime : An Introduction – Marjie Britz, Edition 2, Prentice Hall, 2008

REFERENCES :

1. Practical guide to Computer Forensics- David Benton and Frank Grindstaff , 2006, Book Surge Publishing, 2006

2. Computer Evidence: Collection & Preservation- Christopher L.T Brown Charles River Media publishing, Edition 1, 2005

3. Computer Investigation (Forensics, the Science of crime-solving) – Elizabeth Bauchner, Mason Crest Publishers, 2005

4. Real Digital Forensics- Keith J. Jones, Richard Bejtlich and Curtis W. Rose, Addison-Wesley publishers, 2005

5. Forensic Computer Crime Investigation (International Forensic Science and Investigation)-Thomas A. Johnson, CRC Press, 2005

SEMESTER I - ELECTIVE SUBJECTS

CSCF 3104 Applied Cryptography

Unit 1:

Introduction and preliminaries, Cryptographic protocols, Protocol Building Blocks- Communication using symmetric cryptography, One-way functions, One-way Hash functions, Communications using Public key cryptography, Digital signatures with encryption, Random and pseudo-random sequence generation, Basic protocols- Authentication and key exchange, Formal analysis of authentication and key exchange protocols, Multiple- key Public-key cryptography, Secret splitting, Secret sharing, cryptographic protection of databases.

Unit 2:

Intermediate protocols - Time stamping services, Subliminal channel, Undeniable digital signatures, Designated Confirmer signatures, Proxy signatures, Group signatures, Fail-stop digital signatures, Computing with encrypted data, Bit Commitment, Fair coin flips, Mental Poker, One-way accumulators, All-or-nothing disclosure of secrets, Key escrow, Advanced protocols- Zero-knowledge proofs, Blind Signatures, Identity-Based public-key cryptography, Oblivious transfer, Oblivious signatures, Simultaneous contract signing, Digital certified mail, Simultaneous exchange of secrets. Esoteric protocols- Secure elections, Secure multiparty computation, Anonymous message broadcast, Digital cash.

Unit 3:

Cryptographic techniques- Key Length- Symmetric key length, Public-key key length, Birthday attacks against One-Way Hash functions, Caveat Emptor, Key Management- Generating keys, Nonlinear keyspaces, Transferring ,Verifying, Using, Updating and Storing keys, Backup Keys, Compromised keys, Lifetime of keys, Destroying keys, Public-key management.

Unit 4:

Algorithms types and Modes- Electronic Codebook mode, Block replay, Cipher block chaining mode, Stream ciphers - Self-synchronizing, Cipher feedback mode, Synchronous ciphers, Output feedback mode, Counter mode, Other block-cipher modes, Choosing a cipher mode, Interleaving, Choosing an algorithm, Public key cryptography versus Symmetric cryptography, Encrypting communication channels, Encrypting data for storage, Hardware versus software encryption.

Unit 5:

Cryptographic algorithms- Information theory, Complexity theory, Number theory, Data Encryption and Standard-Description, Security, Differential and Linear cryptanalysis, DES variants, Block Ciphers- Lucifer, NewDES, FEAL,RC2, IDEA, MMB, Other Block algorithms, Theory of Block Cipher Design, Using One-Way Hash functions, Choosing a block algorithm, One-Way Hash Functions- MD2, MD4,MD5, SHA,HAVAL, Using symmetric key algorithms, Using public key algorithms, Knapsack, RSA, DSA, Secret-sharing algorithms.

Textbooks:

1. Applied Cryptography: Protocols, Algorithms and Source code in C- Bruce Schneieir, John Wiley & Sons, Edition, 1996

2. Cryptography A Primer- Alan G Konhein, John Wiley & sons, 1981

3. Handbook of Applied Cryptography- Alfred Menezes, Paul van Oorschot, Scott Vanstone, CRC Press, Edition 1, 1996

References:

1. Introduction to Modern Cryptography- Jonathan Katz, Yehuda Lindell, Chapman and Hall/CRC; Edition 1, 2007

2. Understanding Cryptography- Chritof Paar, Jan Pelzl, Bart Preneel, Springer; Edition 2, 2010

3. Cryptography: A New Dimension in Computer Data Security- Carl Meyer, SM Matyas, John Wiley & Sons, 1982

CSCF 3105 File System Forensic Analysis

Unit 1:

Digital investigation foundation- Digital investigations and evidence, Digital crime scene investigation process, Data analysis, overview of toolkits, Computer foundations- Data organizations, booting process, Hard disk technology, Hard disk data acquisition- introduction, reading the source data, writing the output data, a case study.

Unit 2:

Volume Analysis- introduction, background, analysis basics, PC based partitions- DOS partitions, Analysis considerations, Apple partitions, removable media, Server based partitions- BSD partitions, Sun Solaris slices, GPT partitions, Multiple disk volumes- RAID, Disk Spanning.

Unit 3:

File system analysis- What is a file system, File system category, Content category, Metadata category, File name category, Application category, Application-level search techniques, Specific file systems, FAT concepts and analysis- Introduction, File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check. FAT data structure- Boot sector, FAT 32 FS info, FAT, Directory entries, Long file name directory entries.

Unit 4:

NTFS concepts- Introduction, Everything is a file, MFT concepts, MFT entry attribute concepts, Other attribute concepts, Indexes, Analysis tools, NTFS Analysis- File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check. NTFS data structure- Basic concepts, Standard file attributes, Index attributes and data structures, File system metadata files.

Unit 5:

Ext2 and Ext3 concepts- File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check. Ext2 and Ext3 data structures- Super block, group descriptor tables, Block bitmap, Inodes, Extended attributes, Directory Entry, Symbolic Link, Hash trees, Journal data structures, UFS1 and UFS2 concepts and analysis- Introduction, File system category, Content category, Metadata category, File name category, The big picture File recovery, determining the type, Consistency check, UFS1 and UFS2 data structures- UFS1 superblock, UFS2 superblock, Cylinder group summary, UFS1 group descriptor, UFS2 group descriptor, Block and fragment bitmaps, UFS1 Inodes, UFS2 Inodes, UFS2 Extended attributes, Directory entries.

Textbooks:

1. File System Forensic Analysis – Brian Carrier, Addison Wesley, 2005

2. Digital Evidence and Computer Crime- Casey, Eoghan , edition 2, Academic Press, 2004.

3. Computer Forensics- Kruse, Warren and Jay Heiser, Addison Wesley, 2002.

References:

1. Guide to Computer Forensics and Investigations- Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, Thomson Course Technology, 2004

2. Forensic Discovery – Dan Farmer &Wietse Venema, Addison Wesley, 2005

3. Incident Response and Computer Forensics- Mandia, Kevin, Chris Prosise, Matt Pepe, McGraw Hill/Osborne, 2003.

4. A Fast File System for UNIX-McKusick, William N. Joy, Samuel J. Leffler, Robert S. Fabry , ACM Transactions on Computer Systems , August 1984, pp 181-197. **http://docs.freebsd.org/44doc/smm/05.fastfs/paper.pdf**

5. The Common Vulnerabilities and Exposures database, entry CVE-2000-0666. **http://cve.mitre.org/**

CSCF 3106 Information Security Basics

Unit 1:

Introduction to Information Security, The history of Information security, What is security, CNSS security model, Component s of an Information system, Balancing Information security and access, Approaches to Information security implementation, The systems development life cycle, The security systems development life cycle, Security professionals and the organization, The need for security- Introduction, Business needs first, Threats-Compromises to individual property, Deliberate software attacks, Deviations in quality of service, Espionage, Sabotage, Theft, Attacks-Malicious code, Hoaxes, Back doors, Password crack, Brute force, Dictionary, Denial of service and Distributed denial of service, Spoofing, Man-in-the-middle, Spam, Mail bombing, Sniffers. Social Engineering, Pharming, Timing attack, Secure software development.

Unit 2:

Laws and ethics in Information security, General computer crime laws, Privacy, Export and espionage law, State and local regulations, International laws and legal bodies, Ethical differences across cultures, Ethical decision evaluation, Ethics and education, Deterring unethical and illegal behavior, An overview of risk management, Risk identification, Risk assessment, Risk control strategies, Selecting a risk control strategy, Quantitative versus qualitative risk control practices, Risk appetite, Residual risks, Documenting results.

Unit 3:

Information security planning and governance- Planning levels, Planning and the CISO, Information security governance, Information security policy, standards and practices- Definitions, EISP, ISSP, SysSP, Policy management, The Information security blueprint, Designing of security architecture, Security education training and awareness program, Continuity strategies, Security technology- Firewalls and VPNs, Access control- Identification, Authentication, Authorization , Accountability, Firewall processing modes, Firewalls categorized by generation, Firewalls categorized by structure, Firewall architectures, Selecting the right firewall, Configuring and managing firewalls, Content filters, Protecting remote connections- Remote access, VPNs.

Unit 4:

Intrusion detection and prevention systems- Why IDPS?, types, detection models, response behavior , strengths and limitations, deployment and implementation, measuring the effectiveness. Honeypots, Honeynets and padded cell systems- Trap-and-trace systems, Active intrusion prevention, Scanning and analysis tools- Port scanners, Firewall analysis tools, operating system detection tools, Vulnerability scanners, Packet Sniffers, wireless security tools, Effectiveness and acceptability of biometrics.

Unit 5:

Foundations of Cryptology, Cipher methods- Substitution cipher, Transposition cipher, Exclusive OR, Vernam Cipher, Book or running key cipher, Hash functions, Crytographic algorithms- Symmetric encryption, Asymmetric encryption, encryption key size, Cryptographic tools- PKI, Digital signatures,Digital certificates, Hybrid cryptographic systems, Steganography, Securing Internet communication with S-HTTP and SSL, Securing e-mail with S/MIME, PEM and PGP, Securing web transactions with SET, SSL and S-HTTP, Securing wireless networks with WEP and WPA, Securing TCP/IP with IPSec and PGP, Attacks on Cryptosystems-Man-in-the-middle attacks, Correlation attacks, Dictionary attacks, Timing attacks, Defending against attacks.

Textbooks:

1. Principles of Information Security- Michael E. Whitman, Herbert J. Mattord, Cengage Learning, Fourth edition, 2011

2. Computer Security basics- Rick Lehtinen, O'Reilly, 2nd edition, 2006

3. Absolute beginner's guide to Security, Spam, Spyware & Viruses- Andy Walker, Que publishers, 2005

References:

1. Information Security Management Principles- Andy Taylor, David Alexander, Amanda Finch, David Sutton, BCS publishers, 2008

2. Guide to Computer forensics and Investigations- B. Nelson, A. Phillips, F. Enfinger, C. Steuart, Cengage Learning, 4th edition, 2010

3. Applied Information security: A Hands-On guide to Information security- R. Boyle, Prentice Hall, 2010

4. Fundamentals of Network Security- E. Maiwald, McGraw- Hill, 2004

5. Managing Information Security- John R. Vacca, Elsevier Inc, 2010

SEMESTER II - CORE SUBJECTS

CSCF 3201 Advanced Operating System Concepts

Unit 1:

Processes and threads, Symmetric multiprocessing, Microkernels, Concurrency, Mutual Exclusion, Semaphores, Readers/Writers problem, Monitors, Message Passing, Deadlocks, Concurrency mechanism-Case studies in Linux, Windows, Memory management, Virtual Memory-Hardware and Control structures, case studies in Linux and Windows.

Unit 2:

Uniprocessor scheduling- Scheduling algorithms, case studies in Linux and Windows, Multiprocessor scheduling- Real-Time scheduling, case studies in Linux and Windows,I/O Management and Disk scheduling-Organization of the I/O function, Operating system design issues, Disk scheduling, RAID, case studies in Linux and Windows, File Management-Organization, Access, Sharing, File system security- case studies in Linux and Windows.

Unit 3:

Distributed processing-Types of distributed systems, Architectures, Architectures versus middleware , Self management in distributed systems, threads in distributed systems, Virtualization- role in distributed systems, architecture of virtual machines, clients, servers, code migration, communication-layered protocols, types, RPC, message-oriented communication, stream-oriented communication, multicast communication.

Unit 4:

Distributed operating systems - Architecture, theoretical foundation, clock synchronization- Physical clocks, The Berkeley algorithm, The Happened-Before Relationship, Logical clocks, Vector Timestamps, Global states, Election algorithms - Traditional algorithms, elections in wireless environments, elections in large scale systems, Distributed Mutual Exclusion- Requirements, Centralised, Decentralised algorithms, Ricart and Agrawala's Algorithm, Maekawa's Algorithm, Token Based Dist ME.

Unit 5:

Consistency- Data -Centric consistency models, Strict consistency, Sequential consistency, Casual consistency, FIFO consistency , Client-centric consistency models- Eventual consistency, Replica Management , Replication- Update propagation, Epidemic algorithms, Consistency protocols. Fault tolerance- Failure models, Process resilience, Reliable client-server communication, reliable group communication, distributed commit, recovery.

Textbooks:

1. Advanced Concepts in Operating Systems- Mukesh Singhal , Niranjan Shivarathri, TataMcGrawHill , Edition 1, 2001

2. Distributed systems, Principles and Paradigms- Tannenbaum, Maarten Van Steen, Prentice Hall, Edition 2, 2007

3. Distributed Computing, Fundamentals, Simulations and Advanced Topics – Hagit Attiya, Jennifer Welch, McGraw-Hill, 1997

References:

1. Modern Operating systems – Andrew S. Tannenbaum, PH, Edition 2, 2001

2. Operating Systems: Internals and Design Principles- Stallings , PH,2011

3. Distributed Operating System: Concepts and Design- Sinha, Wiley- IEEE Press, 1996

4. Distributed Operating Systems: Concepts and Practice- Doreen L. Galli, PHI, 1999

CSCF 3202 Network Security

Unit 1:

State of Network Security, Cyber Security, New approaches to cyber security, Interfacing with the organization, Information security principles- Key principles of network security, Formal Processes, Risk Management, Calculating and managing risk, Information System Security Management- Security policies, Security awareness, Managing the Technical effort, Configuration Management, Business Continuity and Disaster Recovery Planning, Physical Security, Legal and Liability Issues, Access Control-Control Models, Types of Access Control Implementations, Identification and Authentication, Remote access, Attacks and threats-Malicious code, Review of common attacks, External attack methodologies overview, Internal threat overview.

Unit 2:

Windows Security- Windows Security at the heart of the defense, Out-of-the-box Operating system hardening, Installing applications, Putting the workstation on the network, Operating Windows safely, Upgrades and Patches, Maintain and test the security, Attacks against the Windows workstation, Linux Security- Physical security, Controlling the configuration, Operating Linux safely, Hardening Linux, Web Browser and Client risk, How a web browser works, Web browser attacks, Operating safely, Web Browser configurations, Web security- How HTTP works, Server and Client contents, State, Attacking Web servers, Web Services, E-mail security- The e -mail risk, Protocols, Authentication, Operating safely when using e-mail, Security Issues with DNS, DNS attacks, Server security-Risks, Security by design, Operating servers safely, Multi-level security and digital rights management.

Unit 3:

VoIP, Wireless Security- The Cellular phone network, Wireless transmission systems, Pervasive Wireless Data Network Technologies, IEEE Wireless LAN specification, Bluetooth, WAP, Network segments-Perimeter Defense, NAT, Basic architecture issues, Subnetting, switching and VLANs, Address Resolution protocol and media access control, zero configuration networks, system design and architecture against insider threats, Firewalls-types, rules, personal firewalls, Intrusion detection systems, responses to intrusion detection, emerging technologies in intrusion detection systems.

Unit 4:

Cryptography- Principles, four cryptographic primitives, Proprietary versus open source algorithms, Attacks on Hash functions, Quantum cryptography, Steganography- overview, history, Core areas of network security and their relation to steganography, Certification and accreditation, DIACAP, Penetration testing, Auditing and Monitoring.

Unit 5:

Integrated cyber security- Validating your security- overview, Current state of penetration testing, Formal penetration testing methodology, Steps to explore a system, Data Protection, Endpoint security, Insider threats and data protection, Critical problems facing organizations, general tips for protecting a site, security best practices.

Textbooks:

1. Network Security Bible- Eric Cole, Ronald Krutz, James W. Conley, Edition 2, Wiley India Pvt Ltd, 2010

2. Network Security Essentials – William Stallings, Edition 4, Pearson Education, 2011

3. Cryptography and Network Security: Principles and Practice-William Stallings, Edition 3, Pearson education, 2003

References:

1. Hacking Exposed- Network Security secrets and solutions, Joel Scambray, McGraw Hill, Edition 5, 2005

2. Wireless Security : Models, Threats and Solutions- Randall K. Nichols, Panos C. Lekkas, McGraw Hill, Edition 1, 2001

3. Secrets and Lies: Digital Security in a Networked world- Bruce Schneier, Wiley publishers, Edition 1, 2004

4. Network Analysis, Architecture and Design- James D. McCabe, Morgam Kaufman, Edition 3, 2007

CSCF 3203 SEMINAR

SEMESTER II - ELECTIVE SUBJECTS

CSCF 3204 Virtual Forensics

Unit 1:

Requirement of virtualization, How virtualization works- virtualizing operating systems, hardware platforms and servers, hypervisors- bare-metal, embedded, hosted, categories of virtualization- full virtualization, paravirtualization, hardware-assisted virtualization , operating system virtualization, application server virtualization , application virtualization , network virtualization , storage virtualization , service virtualization , benefits of virtualization, cost of virtualization, Purpose of server virtualization, server virtualization the bigger picture, differences between desktop and server virtualization, common virtual servers.

Unit 2:

What is desktop virtualization, common virtual desktops, virtual appliances and forensics, virtual desktops as a forensic platform, portable virtualization-MajoPac, MokaFive, preconfigured virtual Environments, virtual appliance providers, Jumpbox virtual appliances, virtual Box, virtualization hardware devices, virtual privacy machine, virtual emulators. Investigating dead Virtual environments – Install files, Remnants, registry , Microsoft disk image format, data to look for.

Unit 3:

Fundamentals of investigating live virtual environments, artifacts, processes and ports, log files, VM memory usage, memory analysis, Microsoft analysis tools, trace collection for a virtual machine, separate swap files for different virtual machines in a host computer, profile based creation of virtual machine in a virtualization environment, system and methods for enforcing software license compliance with virtual machine as well as for improving memory locality of virtual machines, mechanisms for providing virtual machines for multiple users.

Unit 4:

Detecting Rogue virtual machines, alternate data streams and Rogue virtual machines, virtual machine traces- prefetch file, link files, registry files, imaging virtual machines, snapshots and snapshot files, VMotion, Identification and conversion tools, Environment to environment conversion , Virtual environment and compliance- standards,compliance, regulatory requirements, discoverability of virtual environment, legal and protocol document language, organizational chain of custody, data retention policies, backup and datarecovery.

Unit 5:

Virtualization challenges- Data Centers, Storage Area networks, Direct attached storage and network attached storage, cluster file systems, Analysis of cluster file systems, security considerations- technical guidance, VM threats, Hypervisors, virtual appliances, Malware and virtualization- detection, Red Pill, Blue Pill, No Pill, Other methods of finding VMs, Additional challenges- encryption, solid-state drives, new file systems and disk types, compression and data deduplication, virtualization drawbacks.

Text books:

1. Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments, Diane Barrett, Greg Kipper, Elsevier Science & Technology, 2010

2. Introduction to Virtualization e-book

3. Cloud Computing: Automating the Virtualized Data Center-Venkata Josyula, Malcolm Orr & Greg Page, Cisco Press, 2011

References:

1. Cloud Computing : Insights into new- era infra structure-Dr Kumar Saurabh, Wiley Publishers, April 2011

2. Hacking Exposed: Virtualization & Cloud Computing: Secrets & Solutions- Hoff Christofer, Mogull Rich & Balding Craig, McGraw Hill,

CSCF 3205 Information Security Governance

Unit 1:

Governance Overview—Basics, Origins of Governance , Governance Definition , Information Security Governance, Six Outcomes of Effective Security Governance, Defining Information, Data, Knowledge, Value of Information. Why Governance?- Benefits of Good Governance, Aligning Security with Business, Objectives, Providing the Structure and Framework to Optimize, Allocations of Limited Resources, Providing Assurance that Critical Decisions are Not, Based on Faulty Information, Ensuring Accountability for Safeguarding Critical Assets, Increasing Trust of Customers and Stakeholders, Increasing the Company's Worth, Reducing Liability for Information Inaccuracy or Lack of Due Care in Protection, Increasing Predictability and Reducing Uncertainty of Business Operations, A Management Problem. Legal andRegulatory Requirements- Security Governance and Regulation. Roles and Responsibilities- The Board of Directors, Executive Management , Security Steering Committee, The CISO.

Unit 2:

Strategic Metrics -Governance Objectives, Strategic Direction, Ensuring Objectives are Achieved, Risks Managed Appropriately, Verifying that Resources are Used Responsibly. Information Security Outcomes - Defining Outcomes, Strategic Alignment—Aligning Security Activities in Support of Organizational Objectives, Risk Management—Executing Appropriate Measures to Manage Risks and Potential Impacts to an Acceptable Level, Business Process Assurance/Convergence—Integrating, All Relevant Assurance Processes to Improve Overall Security and Efficiency, Value Delivery—Optimizing Investments in Support of Organizational Objectives, Resource Management—Using Organizational Resources Efficiently and Effectively, Performance Measurement— Monitoring and Reporting on Security Processes to Ensure that Objectives are achieved.

Unit 3:

Security Governance Objectives - Security Architecture, Managing Complexity, Providing a Framework and Road Map, Simplicity and Clarity through Layering and Modularization, Business Focus Beyond the Technical Domain, Objectives of Information Security Architectures, SABSA - SABSA Development Process, SABSA Life Cycle, National Cybersecurity Task Force, Information Security Governance: A Call to Action. Risk Management Objectives - Risk Management Responsibilities, Managing Risk Appropriately, Determining Risk Management Objectives, Recovery Time Objectives. Current State - Current State of Security, SABSA, CobiT, CMM, ISO/IEC 27001, 27002, Cyber Security Taskforce Governance Framework, Current State of Risk Management, Gap Analysis—Unmitigated Risk.

Unit 4:

Developing a Security Strategy - Failures of Strategy, Attributes of a Good Security Strategy, Strategy Resources , Utilizing Architecture for Strategy Development , Using CobiT for Strategy Development, Using CMM for Strategy Development , Strategy Constraints, Contextual Constraints, Operational Constraints. Sample Strategy Development - The Process. Implementing Strategy - Action Plan Intermediate Goals, Action Plan Metrics, Reengineering , Inadequate Performance, Elements of Strategy, Policy Development, Standards.

Unit 5:

Security Program Development Metrics-Information Security Program Development Metrics, Program Development Operational Metrics. Information Security Management Metrics-Management Metrics, Security Management Decision Support Metrics, CISO Decisions, Strategic Alignment—Aligning Security Activities in Support of Organizational Objectives, Risk Management—Executing Appropriate Measures to Manage Risks and Potential Impacts to an acceptable Level, Metrics for Risk Management, Assurance Process Integration, Value Delivery— Optimizing Investments in Support of the Organization's Objectives, Resource Management—Using Organizational Resources Efficiently and Effectively, Performance Measurement— Monitoring and Reporting on Security Processes to Ensure that Organizational Objectives are Achieved, Information Security Operational Metrics. Incident Management and Response Metrics- Incident Management Decision Support Metrics.

Textbooks:

1. Information Security Governance- A practical development and implementation approach by Krag Brotby, 2009.
2. Information Security Governance byS.H. von Solms**,** Rossouw von Solms, 2008

References:

1. Information Security Governance byTodd Fitzgerald, 2011
2. Management of Information Security, by Michael E.Whitman, Herbert J.Mattord, Cengage Learning,2010
3. Applied Information security: A Hands-On guide to Information security- R. Boyle. Prentice Hall, 2010
4. Managing Information Security- John R. Vacca, Elsevier Inc, 2010
5. Information Security Management Principles- Andy Taylor, David Alexander, Amanda Finch, David Sutton, BCS publishers, 2008

CSCF 3206 Malware Forensics

Unit 1:

Malware Incident response: Volatile Data Collection and Examination on a Live Windows / Linux System-Volatile Data collection methodology-Preservation of volatile data, Collecting Subject System details, Identifying Users logged into the system, Inspect Network Connections and activity, Current and recent network connections, Collecting process information, Process to executable program mapping , Dependencies loaded by running processes, Correlate open ports with running processes and programs, Identifying servers and drivers, Determining scheduled tasks, Collecting Clipboard contents, Non-volatile Data collection from a live Windows system, Forensic duplication of storage media on a live Windows system, Forensic preservation of Select Data on a Live Windows System, Incident Response Tool Suites for Windows, Assess Security configuration, Collect Logon and System Logs.

Unit 2:

Memory Forensics: Analyzing Physical and Process Dumps for Malware Artifacts- Memory Forensics methodology, Old School Memory Analysis, Windows Memory Forensics Tools, Active, Inactive and Hidden Processes, How Windows Memory Forensics Tools work, Process Memory Dumping and Analysis on a Live Windows System, Capturing Process and Analyzing Memory, Linux Memory Forensics Tools, How Linux Memory Forensics Tools work, Process Memory Dumping and Analysis on a Live Linux System, Capturing and Examining Process Memory in Linux System.

Unit 3:

Post-Mortem Forensics: Discovering and Extracting Malware and Associated Artifacts from Windows Systems and Linux systems- Forensic Examinations of Compromised Windows / Linux Systems, Functional Analysis Resuscitating a Windows / Linux Computer, Malware Discovery and Extraction from a Windows/ Linux system, Inspect services, Drivers Auto-starting Locations, and scheduled jobs.

Unit 4:

Legal considerations- Framing the issues, Sources of Investigative authority, Statutory limits of authority, protected data, Tools for acquiring data, Acquiring data across Borders, Involving Law Enforcement, Improving chances for admissibility.

Unit 5:

File Identification and profiling: Initial Analysis of a suspect file on a Windows / Linux system-

Overview of the File Profiling process, Working with Executables-Compilation, Linking- Static, Dynamic, System details, Hash values, File similarity indexing, File signature identification and classification- File types, Tools, Embedded artifact extraction, Symbolic and Debug information, File Obfuscation: Packing and Encryption Identification-Packers, Cryptors, Wrappers, Elf File structure, Analysis of a suspect program: Windows/ Linux- Analysis Goals, Guidelines for examining a malicious executable program, establishing the environment baseline, Pre -execution preparation: system and network monitoring, Observing, File system, Embedded Artifact Extraction revisited, Exploring and verifying specimen functionality and purpose, Event reconstruction and artifact review: File system, Registry, Process and Network Activity Post-run Data Analysis.

Textbooks:

1. Malware Forensics Investigating and Analyzing Malicious code-James M. Aquilina, Eoghan Casey, Cameron H. Malin, Syngress Publishing, 2008

2. Malware Analyst's Cookbook Tools and Techniques for fighting malicious code- Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Wiley Publishing Inc, 2011

References:

1. Unix and Linux Forensic Analysis DVD ToolKit - Chris Pogue, Cory Altheide, Todd Haverkos, Syngress Inc. , 2008

2. Windows Forensic Analysis DVD Toolkit- Harlan Carvey, Edition 2, Syngress Inc. , 2007

3. Windows Forensic Analysis- Harlan Carvey , Dave Kleiman, Syngress Inc. , 2007

4. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry - Harlan Carvey, Syngress Inc, Feb 2011

5. File System Forensic Analysis- Brian Carrier, Addison Wesley, Edition 1, 2005

6. Handbook of Digital Forensics and Investigation- Eoghan Casey, Academic Press, 2009

7. Digital Forensics with Open Source Tools- Cory Altheide,
Harlan Carvey, Syngress Inc, Edition 1, April 2011

CSCF 3207 Windows and Linux Forensic Analysis

Unit 1:

Windows Forensic Analysis- Live Response: Data Collection- Introduction , Live Response- Locard's Exchange Principle, Order of Volatility ,When to Perform Live Response ,What Data to Collect- System Time, Logged-on Users , Open Files, Network Information , Network Connections ,Process Information, Process-to-Port Mapping, Process Memory, Network Status, Nonvolatile Information, Live-Response Methodologies, Live Response: Data Analysis- Data Analysis, Agile Analysis, Windows Memory Analysis-Collecting Process Memory, Dumping Physical Memory, Alternative Approaches for Dumping Physical Memory, Analyzing a Physical Memory Dump.

Unit 2:

Registry Analysis- Inside the Registry, Registry Analysis- RegRipper, System Information, Autostart Locations, USB Removable Storage Devices, Mounted Devices, Portable Devices, Finding Users, Tracking User Activity, Redirection, Virtualization, Deleted Registry Keys, File Analysis-Log Files, Event Logs, Other Log files, Recycle Bin, XP System Restore Points, Vista Volume Shadow Copy Service, Prefetch and Shortcut files, File Metadata, File Signature Analysis, NTFS Alternate Data Streams, Alternative Methods of Analysis, Executable File Analysis- Static Analysis, Dynamic Analysis.

Unit 3:

Rootkits, Rootkit Detection-Live Detection, GMER, Helios, MS Strider GhostBuster, F-Secure BlackLight, Sophos Anti-Rootkit, Postmortem Detection, Prevention, Case studies, Performing Analysis on a Budget-Documenting Your Analysis, Tools-Acquiring Images, Image Analysis, File Analysis, Network Tools, Search Utilities.

Unit 4:

Linux Forensic Analysis- Live Response Data Collection- Prepare the Target Media, Format the Drive, Gather Volatile Information, Acquiring the Image, Initial Triage and Live Response: Data Analysis- Log Analysis, Keyword Searches, User Activity, Network Connections, Running Processes, Open File Handlers, The Hacking Top Ten, Reconnaissance Tools, The /Proc File System- Introduction , Process IDs,

Unit 5:

File Analysis- The Linux Boot Process, System and Security Configuration Files- Users, Groups, and Privileges, Cron Jobs , Log Files, Identifying Other Files of Interest- . SUID and SGID Root Files, Recently Modified/Accessed/Created Files, Modified System Files, Out -of-Place inodes, Hidden Files and Hiding Places, Malware- Introduction, Viruses, Storms on the Horizon, Scanning the Target Directory.

Textbooks:

1. Unix and Linux Forensic Analysis DVD ToolKit - Chris Pogue, Cory Altheide, Todd Haverkos, Syngress Inc. , 2008

2. Windows Forensic Analysis DVD Toolkit- Harlan Carvey, Edition 2, Syngress Inc. , 2009

References:

1. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry - Harlan Carvey, Syngress Inc, Feb 2011

2. File System Forensic Analysis- Brian Carrier, Addison Wesley, Edition 1, 2005

3. Handbook of Digital Forensics and Investigation- Eoghan Casey, Academic Press, 2009

4. Digital Forensics with Open Source Tools- Cory Altheide,
Harlan Carvey, Syngress Inc, Edition 1, April 2011

CSCF 3208 Ethical Hacking

Unit 1

Ethical Hacking overview, Network and computer attacks, Footprinting and social Engineering, Port Scanning, Enumeration, programming for security professionals, Desktop and server OS vulnerabilities. Embedded Operating Systems: the hidden threat, legal resources, Virtualisation and ethical hacking.

Unit 2

Exploitation- techniques, buffer overflows, BASH, Format strings. Networking- OSI Model, Sockets, network sniffing, TCP/IP Hijacking. Hacking web servers, Hacking Wireless Networks, Network Protection Systems, Shell code, Counter measures .

Unit 3

Dumpster Diving, Tailgating, Shoulder Surfing- basics, locations, electronic deduction, killer real life surfing sessions. Physical Security-Introduction, Lock bumping. Social Engineering- basics, human nature and weakness, the mind of a victim, countering social engineering attacks.

Unit 4

Google Hacking Showcase- Introduction, greek stuff, open network devices, applications, cameras, telco gear, power, sensitive info, social security numbers. P2P Hacking, People Watching, Kiosks, Vehicle Surveillance, Badge Surveillance, Epiloque top ten ways to shut down No-Tech hackers.

Unit 5

End point and server hacking- hacking windows, UNIX, cyber crime and advanced persistent threats. Infrastructure hacking- remote connectivity and VOIP hacking, wireless hacking, hacking hardware. Reconaissance, Web-based Exploitation, Maintaining Access with Backdoors and Rootkits.

Text Books:

1. Hands on ethical hacking and network defense by Michael T Simpson, Kent Backman, James Corley, Cengage Learning, 2 edition, 2010

2. The Basics of Hacking and Penetration Testingby Patrick Engebretson, Syngress Basics Series, edition 01, 2011

3. NoTech Hacking : A Guide to Social Engineering, Dumpster Diving and Shoulder Surfing by Johnny Long, Syngress publishers, 1st edition, 2008

4. Hacking: The Art of Exploitation, 2nd Edition byJon Erickson, William Pollock publishers, 2008

References:

1. Hackers Beware by Eric Cole, New Riders publishing, 2002

2. An unofficial guide to ethical hacking by Ankit Fadia, Macmillan publishers, 2nd edition, 2006

3. Hacking: 01 Edition by S. Pankaj, A P H Publishers, 2005

4. Hacking Exposed 7: Network Security Secrets & Solutions byStuart McClure, Joel Scambray, edition 7, McGraw-Hill publishing, 2012