SCHEME & SYLLABUS FOR PROGRAM M.TECH CYBER SECURITY

SCHEME

Department of Computer Engineering, NIT Kurukshetra (Haryana)

Proposed Scheme for the M.Tech Computer Engineering (Cyber Security)

Sr. No.	Code	Course Title	Teaching Schedule				Credit
			L	T	P	Total	
First Semester							
1.	COE-501	Advanced Data Structures and Algorithms	3	0	0	3	3
2.	COE-551	System and Network Security	3	0	0	3	3
3.	COE-553	Data Privacy	3	0	0	3	3
4.		Elective-1	3	0	0	3	3
5.		Elective -2	3	0	0	3	3
6.	COE-561	System and Network Security Laboratory	0	0	2	2	1
7.	COE-563	Data Privacy Laboratory	0	0	2	2	1
8.	COE-565	Seminar	0	0	2	2	1
Total						**21**	**18**
Second Semester							
1.	COE-552	Number Theory and Cryptology	3	0	0	3	3
2.	COE-554	Introduction to Cyberspace Operations and Design	3	0	0	3	3
3.		Elective-3	3	0	0	3	3
4.		Elective-4	3	0	0	3	3
5.		Elective-5	3	0	0	3	3
6.	COE-562	Number Theory and Cryptology Laboratory	0	0	2	2	1
7.	COE-564	Elective-3 Laboratory	0	0	2	2	1
8.	COE-566	Seminar	0	2	0	2	1
Total						**21**	**18**
Third Semester							
1.	COE-611	Preparatory Work for Dissertation	0	0	20	20	10
Total						**20**	**10**
Fourth Semester							
1.	COE-612	Dissertation	0	0	32	32	16
Total						**32**	**16**

List of Elective Courses

Elective-1		Elective-2		Elective-3		Elective-4		Elective-5	
Code	**Course Title**	**Code**	**Course Title**	**Code**	**Course Title**	**Code**	**Course Title**	**Code**	**Course Title**
COE-525	Pattern Recognition and Machine Learning	COE-531	Distributed Computing	COE-524	Soft Computing	COE-582	SCADA and DCS Security	COE-536	Research Methodology
COE-571	Intrusion Detection Systems	COE-581	System & Device Driver Programming	COE-572	Biometric Security	COE-584	Ethics and Law of Cyber Security	COE-538	Mobile Computing
COE-573	Information Theory and Coding	COE-583	Information Warfare	COE-574	Information Security Risk Management	COE-586	Fuzzing and Software Crash Analysis	COE-594	Ethical hacking
COE-575	Cloud Computing and Big Data	COE-585	Mobile and Wireless Network Security	COE-576	Proactive Security Tools and Techniques	COE-588	Advanced Operating System Design and Security	COE-596	Digital Forensics & Incident Response
COE-577	Vulnerability Discovery and Exploit Development	COE-587	Secure Coding	COE-578	Social Network Analysis	COE-590	BIOS and SMM Security	COE-598	Data Mining and Analysis
COE-579	Game Theory	COE-589	Special Topics in Security-I	COE-580	Enterprise Security & Management	COE-592	Disaster Recovery	COE-600	Special Topics in Security-II

SYLLABI

COE-501

Advanced Data Structures and Algorithms

Objectives:

To develop the understanding of advanced data structures and algorithms.

Learning Outcomes:-

On completion of this course students should have gained an understanding of algorithmic / data structure language and notation, including order notation, and how to calculate the running times of algorithms. Students should also understand how to estimate, profile, and measure algorithm complexity and performance. The Key Learning Outcomes are:

- Compare, contrast, and apply the key algorithmic design paradigms: brute force, divide and conquer, decrease and conquer, transform and conquer, greedy, dynamic.
- Compare, contrast, and apply key data structures: trees, lists, stacks, queues, hash tables, and graph representations.
- Define, compare, analyze, and solve general algorithmic problem types: sorting, searching, string processing, graphs, and geometric.
- Compare, contrast, and apply algorithmic tradeoffs: time vs. space, deterministic vs. randomized, and exact vs. approximate.
- Implement, empirically compare, and apply fundamental algorithms and data structures to real-world problems.

Syllabus:

Complexity of algorithms: worst case, average case, and amortized complexity. Algorithm analysis techniques, Amortized Analysis, Garbage collection, Analysis of Quick sort, Fibonacci Heaps, van Emde Boas Trees, Multithreaded Algorithms, Number Theoretic Algorithms, Strings and String Matching Algorithms, Computational Geometry, Lower Bound Theory–NP Completeness, Approximation Algorithms.

Text books:

1. Anne Benoit, Yves Robert, Frédéric Vivien. A Guide to Algorithm Design**:** Paradigms, Methods, and Complexity Analysis, Taylor & Francis, 2013.
2. OdedGoldreich. P, NP, and NP-Completeness: The Basics of Computational Complexity, Cambridge University Press, 2010.

Reference books:

1. A.V. Aho, J.E. Hopcroft, and J.D. Ullman, Data Structures and Algorithms, Addison Wesley, Reading Massachusetts, USA, 1983.
2. Donald Knuth. The Art of Computer Programming: Fundamental Algorithms, Third Edition. Addison-Wesley, 1997.
3. Donald Knuth. The Art of Computer Programming Volume 3: Sorting and Searching, Third Edition. Addison-Wesley, 1997. ISBN 0-201-89685-0.
4. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Third Edition. MIT Press and PHI, 2010.
5. Samet, Hanan, Foundations of multidimensional and metric data structures. Morgan Kaufmann, 2006, ISBN 978-0-12-369446-1.
6. Dinesh Mehta and SartajSahni Handbook of Data Structures and Applications, Chapman and Hall/CRC Press, 2007.
7. M.A. Weiss, Data Structures and Algorithms Analysis in C++, Benjamin/Cummins, Redwood City, California, USA, 1994.

COE-551

System and Network Security

Objectives:

The purpose of this course is to provide understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptop to large-scale infrastructures.

Learning Outcomes:

On completion of this course, students should have gained a good understanding of the concepts and foundations of computer security, and identify vulnerabilities of IT systems. The students can use basic security tools to enhance system security and can develop basic security enhancements in stand-alone applications.

Syllabus:

Computer Security Concepts- Introduction to Information Security, Introduction to Data and Network Security, Integrity, and Availability, NIST FIPS 199 Standard, Assets and Threat Models, Examples

Control Hijacking– Attacks and defenses, Buffer overflow and control hijacking attacks
Exploitation techniques and fuzzing- Finding vulnerabilities and exploits
Dealing with Legacy code- Dealing with bad (legacy) application code: Sandboxing and Isolation.
Least privilege, access control, operating system security- The principle of least privilege, Access control concepts, Operating system mechanisms, Unix, Windows, Qmail, Chromium, and Android examples.
Basic web security model- Browser content, Document object model (DOM), Same-origin policy.
Web Application Security- SQL injection, Cross-site request forgery, Cross-site scripting, Attacks and Defenses, Generating and storing session tokens, Authenticating users, The SSL protocol, The lock icon, User interface attacks, Pretty Good Privacy.
Network Protocols and Vulnerabilities- Overview of basic networking infrastructure and network protocols, IP, TCP, Routing protocols, DNS.
Network Defenses- Network defense tools, Secure protocols, Firewalls, VPNs, Tor, I2P, Intrusion Detection and filters, Host-Based IDS vs Network-Based IDS, Dealing with unwanted traffic: Denial of service attacks.
Malicious Software and Software Security- Malicious Web, Internet Security Issues, Types of Internet Security Issues, Computer viruses, Spyware, Key-Loggers, Secure Coding, Electronic and Information Warfare.
Mobile platform security models- Android, iOSMobile platform security models, Detecting Android malware in Android markets.
Security Risk Management- How Much Security Do You Really Need, Risk Management, Information Security Risk Assessment: Introduction, Information Security Risk Assessment: Case Studies, Risk Assessment in Practice.
The Trusted Computing Architecture- Introduction to Trusted Computing, TPM Provisioning, Exact Mechanics of TPM.

Text books and References:

1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
2. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison Wesley, 2011.
3. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
4. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.

COE-553

Data Privacy

Course objectives:
The objective of this course is to create architectural, algorithmic and technological foundations for the maintenance of the privacy of individuals, the confidentiality of organizations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.

Learning outcomes:
After successful completion of this course, students will be able to:

- Understand the concepts of privacy in today's environment.
- Obtain the understanding of how automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security.
- Obtain the knowledge of the role of private regulatory and self-help efforts.
- Have an understanding of how emerging issues are affecting society and business, with a concentration on how information security must shape corporate practices.

Syllabus:

Introduction- Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, etc.
Data explosion- Statistics and Lack of barriers in Collection and Distribution of Person-specific information, Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements, Demographics and Uniqueness.
Protection Models- Null-map, k-map, Wrong map
Survey of techniques- Protection models (null-map, k-map, wrong map), Disclosure control, Inferring entity identities, Strength and weaknesses of techniques, entry specific databases.
Computation systems for protecting delimited data- MinGen, Datafly, Mu-Argus, k-Similar, Protecting textual documents**:** Scrub.
Technology, Policy, Privacy and Freedom- Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.

Text books and References:

1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation, Auerbach Pub, 2013.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT Computer Science, 2002.

COE-525

Pattern recognition and machine learning

Objective: The aim of this course is to first review the theory of probability and statistics, and then to cover the major approaches of pattern recognition and machine learning.

Learning Outcomes: At the end of this course, students will be able to:

- Identify and describe existing pattern recognition and machine learning approaches for different human interaction modalities (voice, gesture, etc.)
- Discuss and compare different methods for activity recognition along with their strengths and weaknesses
- Evaluate and select the best machine learning approach for the recognition of specific activity
- Compare and identify the best technological solution for designing and implementing a complete activity recognition system based on machine learning approach
- Identify a set of business use--cases using machine learning technology and discuss related advantage and drawbacks

Syllabus:

Parameter Estimation and Classification: Maximum Likelihood Estimation, Maximum A-Posteriori (MAP) Estimation, Maximum Entropy Estimation, Minimum Relative Entropy Estimation, Maximum Mutual Information Estimation (MMIE); Model Selection, Akaike Information Criterion (AIC)Bayesian Information Criterion (BIC); Linear Models for Classification, Discriminant Functions, Two classes, Multiple classes, Least squares for classification, Fisher's linear discriminant, Relation to least squares, Fisher's discriminant for multiple classes, The perceptron algorithm; Probabilistic Generative Models, Continuous inputs, Maximum likelihood solution, Discrete features, Exponential family; Probabilistic Discriminative Models, Fixed basis functions, Logistic regression, Iterative reweighted least squares, Multiclass logistic regression, Probit regression, Canonical link functions.

Clustering and Learning: Learning Algorithms, Risk Minimization, Empirical Risk Minimization, Capacity and Bounds on Risk, Structural Risk Minimization; Decision and Regression Trees, Vector Quantization (VQ); Basic Clustering Techniques, Standard k-Means (Lloyd) Algorithm, Generalized Clustering, Over-partitioning, Merging, Modifications to the k-Means Algorithm, k-Means Wrappers, Rough k-Means, Fuzzy k-Means, k-Harmonic Means Algorithm, Hybrid Clustering Algorithms; Estimation using Incomplete Data, Expectation Maximization (EM); Semi-Supervised Learning.

Kernel Methods and Support Vector Machines: The Two-Class Problem, Dual Representation, Soft Margin Classification; Origins of Kernel methods, Kernel Mapping, The Kernel Trick; Constructing Kernels, Support Vector Machines: Formulation and Computation; Radial Basis Function Networks; Positive Semi-Definite Kernels, Linear Kernel, Polynomial Kernel, Gaussian Radial Basis Function (GRBF) Kernel, Cosine Kernel, Fisher Kernel, GLDS Kernel, GMM-UBM Mean Interval (GUMI) Kernel.

Text books:

1. HomayoonBeigi ,Fundamentals of Speaker Recognition, Springer,2011
2. K.P. Soman, R.Loganathan, V.Ajay, Machine Learning with SVM and other Kernel methods, PHI Learning Private Limited,2009

Reference books:

1. Christopher M. Bishop ,Pattern Recognition and Machine Learning,Springer,2006
2. Tom Mitchell,Machine Learning, McGraw Hill, 1997.
3. Petra Perner. Machine Learning and Data Mining In Pattern Recognition, Springer Science & Business Media, 2009.

COE-571

Intrusion Detection Systems

Objective: The objective of this course is to provide an in depth introduction to the science and art of intrusion detection. The course covers methodologies, techniques, and tools for monitoring events in computer system or network, with the objective of preventing and detecting unwanted process activity and recovering from malicious behavior.

Learning Outcomes:

At the end of this course, students will be able to:

- Obtain comprehensive knowledge on the subject of intrusion detection
- Understand the state of the art of intrusion detection research
- Get a hands-on exposure to the principles and techniques used in intrusion detection, as well as the technical challenges and fundamental limitations of intrusion detection
- become either a capable practitioner or independent researcher in intrusion detection

Syllabus:

Overview of intrusions, system intrusion process, dangers of system intrusions, history and state of the art of intrusion detection systems (IDSs): anomaly detection, misuse detection, types of IDS: Network-Based IDS. Host-Based IDS, Hybrid IDS, Intrusion Prevention Systems (IPS): Network-Based IPS, Host-Based IPS, Intrusion Detection Tools, the limitations and open problems of intrusion detection systems, advanced persistent threats, case studies of intrusion detection systems against real-world threats and malware.

Statistical and machine approaches to detection of attacks on computers - Techniques for studying the Internet and estimating the number and severity of attacks, network based attacks, host based attacks. Statistical pattern recognition for detection and classification of attacks, and techniques for visualizing network data, etc.

Text books:

1. Roberto Di Pietro**,** Luigi V. Mancini**,** Intrusion Detection System, Springer ,2008

Reference books:

1. Anderson, Ross (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons. pp. 387–388. ISBN 978-0-471-38922-4.
2. Anderson, James P., "Computer Security Threat Monitoring and Surveillance," Washing, PA, James P. Anderson Co., 1980.

COE-573

Information Theory and Coding

Objective:

The objective of this course is to introduce the basic concepts of information theory and coding, including information, source coding, channel model, channel capacity, channel coding and so on.

Learning Outcomes:

The students at the end of the course will be able to:

- Understand and explain the basic concepts of information theory, source coding, channel and channel capacity, channel coding and relation among them.
- Describe the real life applications based on the fundamental theory.
- Calculate entropy, channel capacity, bit error rate, code rate, steady-state probability and so on.
- Implement the encoder and decoder of one block code or convolutional code using any program language

Syllabus:

Overview; Basic Concepts - Entropy and Mutual information; Lossless Source Coding – Source entropy rate; Kraft inequality; Huffman code; Asymptotic equipartition property; Universal coding; Noisy Channel Coding - Channel capacity; Random channel codes; Noisy channel coding theorem for discrete memory-less channels; Typical sequences; Error exponents; Feedback; Continuous and Gaussian channels; Lossy Source Coding - Rate- Distortion functions; Random source codes; Joint source-channel coding and the separation theorem.

Source coding- Text, Audio and Speech: Adaptive Huffman Coding, Arithmetic Coding, LZW algorithm – Audio: Perceptual coding, Masking techniques, Psychoacoustic model, MEG Audio layers I,II,III, Dolby AC3 - Speech: Channel Vocoder, Linear Predictive Coding

Source coding- Image and Video: Image and Video Formats – GIF, TIFF, SIF, CIF, QCIF – Image compression: READ, JPEG – Video Compression: Principles-I,B,P frames, Motion estimation, Motion compensation, H.261, MPEG standard

Error control coding- Block codes: Definitions and Principles: Hamming weight, Hamming distance, Minimum distance decoding - Single parity codes, Hamming codes, Repetition codes - Linear block codes,

Cyclic codes - Syndrome calculation, Encoder and decoder – CRC

Error control coding- convolution codes: code tree, trellis, state diagram - Encoding – Decoding: Sequential search and Viterbi algorithm – Principle of Turbo coding

Text books:

1. Mark Kelbert(Author), Yuri Suhov, Information Theory and Coding by Example, Cambridge University Press,2013

Reference books:

1. Simon Haykin and Michael Moher, Communication Systems, 5th Edition, Wiley, 2010
2. T.M. & Thomas, J.A. (2006). Elements of information theory. New York: Wiley.
3. Ad´amek, Foundations of coding, Wiley Interscience, 1991.
4. T. M. Cover and J. A. Thomas, Elements of information theory, Wiley, 1991.

COE-575

Cloud computing and big data

Objective:

Objective of this course is to understand the advantages, challenges, security issues of cloud computing and interrelationships between cloud computing and big data.

Learning Outcomes:

At the end of this course, students will be able to:

- Explain the core concepts of the cloud computing paradigm: how and why this paradigm shift came about, the characteristics, advantages and challenges brought about by the various models and services in cloud computing.
- Apply the fundamental concepts in datacenters to understand the tradeoffs in power, efficiency and cost.

- Identify resource management fundamentals, i.e. resource abstraction, sharing and sandboxing and outline their role in managing infrastructure in cloud computing.
- Illustrate the fundamental concepts of cloud storage and demonstrate their use in storage systems such as Amazon S3 and HDFS.
- Analyze various cloud programming models and apply them to solve problems on the cloud.

Syllabus:

Cloud Computing Fundamentals: What Cloud Computing, Essential Characteristics, Architectural Influences, Technological Influences.
Cloud Computing Architecture: Cloud Delivery Models, Cloud Deployment Models, Expected Benefits.

Cloud Computing Software Security Fundamentals: Cloud Information Security Objectives, Cloud Security Services, Relevant Cloud Security Design Principles, Secure Cloud Software Requirements.

Cloud Computing Risk Issues: Privacy and Compliance Risks, Threats to Infrastructure, Data, and Access Control, Cloud Service Provider Risks,

Cloud Computing Security Challenges: Security Policy Implementation, Virtualization Security Management, VM Security Recommendations, VM-Specific Security Techniques.

Cloud Computing Security Architecture: Architectural Considerations, Identity Management and Access Control, Autonomic Security.

Data storage in the cloud: Understanding cloud-based data storage, cloud-based backup system, Understanding File storage, Industry specific cloud-based data storage, Cloud-based database solutions, Cloud-based block storage.

Collaboration in the cloud: Web based collaborations, Collaborating via web Logs(Blogs), Using social media for collaboration, Using streaming video content to collaborate.

Text books:

1. Kris Jamsa, Cloud Computing, Jones & Bartlett,2012
2. Russell Dean Vines and Ronald L. Krutz ,Cloud Security: A Comprehensive Guide To Secure Cloud Computing, Wiley India Pvt Ltd, 2010

Reference books:

1. Barrie Sosinsky, Cloud Computing Bible, Wiley India,2011

COE-577

Vulnerability Discovery & Exploit Development

Objectives:

Objective of this course is to focus on a comprehensive coverage of software exploitation. In addition, this course will present different domains of code exploitation and how they can be used together to test the security of an application.

Learning Outcome:

Upon completion of this course, students will be able to:

- Understand how to exploit a program and different types of software exploitation techniques
- Understand the exploit development process
- Search for vulnerabilities in closed-source applications
- Write their own exploits for vulnerable applications

Syllabus:

Background- Vulnerability Discovery Methodologies, What is Fuzzing, Fuzzing Methods and Fuzzer Types, Data Representation and Analysis, Requirements for Effective Fuzzing

Targets and Automation- Automation and Data Generation, Environment Variable and Argument Fuzzing, Environment Variable and Argument Fuzzing: Automation, Web Application and Server Fuzzing, Web Application and Server Fuzzing: Automation, File Format Fuzzing, File Format Fuzzing: Automation on UNIX, File Format Fuzzing: Automation on Windows, Network Protocol Fuzzing, Network Protocol Fuzzing: Automation on UNIX, Network Protocol Fuzzing: Automation on Windows, Web Browser Fuzzing, Web Browser Fuzzing: Automation, In-Memory Fuzzing, In-Memory Fuzzing: Automation

Advanced Fuzzy Technologies- Fuzzing Frameworks, Automated Protocol Dissection, Fuzzer Tracking, Intelligent Fault Detection.

Advanced Linux Exploitation-Linux heap management, constructs, and environment, Navigating the heap, Abusing macros such as unlink() and frontlink(), Function pointer overwrites, Format string exploitation, Abusing custom doubly-linked lists, Defeating Linux exploit mitigation controls, Using IDA for Linux application exploitation, Patch Diffing, one day Exploits and Return Oriented Shellcode, The Microsoft patch management process and Patch Tuesday, Obtaining patches and patch extraction, Binary diffing with BinDiff, patchdiff2, turbodiff, and darungrim, Visualizing code changes and identifying fixes, Reversing 32-bit and 64-bit applications and modules, Triggering patched vulnerabilities, Writing one-day exploits, Handling modern exploit mitigation controls.

Windows Kernel Debugging and Exploitation- Understanding the Windows Kernel, Navigating the Windows Kernel, Modern Kernel protections, Debugging the Windows Kernel, WinDbg, Analysing Kernel vulnerabilities and Kernel vulnerability types, Kernel exploitation techniques.

Windows Heap Overflows and Client-Side Exploitation- Windows heap management, constructs, and environment, Browser-based and client-side exploitation, Remedial heap spraying, Understanding C++, vftable/vtable behavior, Modern heap spraying to determine address predictability, Use-After-Free attacks and dangling pointers, Determining exploitability, Defeating ASLR, DEP, and other common exploit mitigation controls

Android Exploitation- Android Basics, Android Security Model, Introduction to ARM, Android Development Tools, Engage with Application Security, Android Security Assessment Tools, Exploiting Applications, Protecting Applications, Secure Networking, Native Exploitation and Analysis.

iOS exploitation-Introduction to iOS hacking, iOS User Space Exploitation, iOS Kernel Debugging and Exploitation

Text books and References:

1. Hack I.T. - Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, ISBN: 0-201-71956-8
2. Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni
3. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm

COE-579

Game Theory

Course Objectives:

Objective of the course is to teach students some strategic considerations to take into account making their choices. In addition, aim is to predict how other people or organizations behave when they are in strategic settings and to apply these tools to settings from economics and from elsewhere.

Learning Outcomes:

After successful completion of this course, students will be able to:

- Train in the logic and strategic decision making involved in the theory of games.
- To solve strategic games between two and more agents in non-cooperative scenario.
- To analyze and solve both simultaneous-moves and sequential-moves games and will be familiarized with different solution concepts..
- Learn different methods to solve games.
- Apply the concepts and ideas that constitute these various game types and their solutions, and apply them to the problems at hand.

Syllabus:

Introduction- Fundamental Concepts, Definitions, and Classification of Games.

Games with Sequential moves-Game tree representation, Actions & Strategies, Advantage in moving first or last, Backward Induction.
Simultaneous moves Games (Pure strategies)-Normal form representation, Nash equilibrium, Dominance, Minimax solution concept for ZerosumGames, Rationalizability, Multiple equilibria, No equilibria, Discrete and Continuous strategies, 3-player games.
Simultaneous and Sequential moves Games- Converting game trees to Normal form, and vice versa. Changing order of moves, Games withboth Sequential and Simultaneous moves.
Simultaneous moves games (Mixed strategies)-Mixing to keep the opponent guessing, Mixing in non-Zero-sum games, Expected values &utility, Mixing with 3 strategies.
Prisoners' Dilemma, Repeated Games and Collective Action- Finite and Infinite repetition, Leadership, Folk Theorem, Application: Price Matching, CollectiveAction and Inaction.
Strategic Moves- Credibility, Commitments, Threats, Promises, Burning Bridges.
Application Voting-Voting Rules, Paradoxes, Strategic Manipulation.
ApplicationBargaining-Nash Bargaining Solution, Ultimatum game, Alternating-offers game, Threat Points, Bargaining Shares.

Text books and References:

1. Dixit and B. Nalebuff. Thinking Strategically, Norton 1991
2. J. Watson. Strategy: An Introduction to Game Theory, Norton 2002
3. P.K. Dutta. Strategies and Games: Theory And Practice, MIT 1999

COE-531

Distributed Computing

Objective:

To understand fundamental concepts of distributed computing and to acquire knowledge about development of fault tolerant protocols for middleware design.

Learning Outcomes:

After completion of this course**,** student should be able to apply these course concepts to:

- Develop, test and debug RPC based client-server programs in Unix.
- Design and build application programs on distributed systems.
- Improve the performance and reliability of distributed programs.
- Design and build newer distributed file systems for any OS.

Syllabus:-

Fundamental issues in Distributed Systems, Distributed System Models and Architectures, Classification of Failures in Distributed Systems, Basic Techniques for Handling Faults in Distributed Systems, Logical and Physical Clocks, Physical Clock Synchronization, Interprocess Communication, Message Ordering Protocols, Naming in Distributed Systems, Global State,

Termination, and Distributed Deadlock Detection, Distributed Mutual Exclusion, Leader Election, Agreement Protocols, Consensus, FLP impossibility, Fault-Tolerance Issues, Z-path and Z-cycles, Byzantine Generals Problem, Distributed Scheduling and Load Balancing. Distributed File Systems, and Distributed Shared Memory, Security.

Text books:

1. Ajay D. Kshemkalyani, Mukesh Singhal, Distributed Computing: Principles, Algorithms, and Systems, Cambridge University Press, 2011.
2. Su Kumar Boss, Distributed Systems and Algorithmic Approach, Chamal & Hall,2006

Reference books:

1. G Colouris, J Dollimore, T Kindberg , Distributed Systems :Concepts and Design; 3/e, Pearson Ed. 2002.
2. Distributed Systems: Principles and Paradigm; Andrew S Tanenbaum, Maarten van Steen 3/e Pearson Ed. 2002.
3. Principles of Distributed Systems, VK Garg, Kluwer Academic Publishers, 1996.

COE-581

System & Device Driver Programming

Objective:

This subject aims to start with the study of system resource management and deals with the programming aspects of the operating system and extending its functionality alongwith the use of device driver to interact with real hardware components.

Learning Outcomes:

After successful completion of this course, students will be able to:

- Write System Software
- Understand purpose, types and configuration of device drivers
- Implement different System Calls
- Do advanced file and process management

Syllabus:

Introduction, Lab & Software Setup, Windows Driver Model Overview, Windows Basic Device Driver Implementation (IRQL, Memory Pool), Debugging Kernel mode driver and Windows/Linux/OSX Boot Process With WinDbg and KD IDApro, IOCTL implementation, File System/Network/Keyboard Filter Driver, TDI/Winsock driver Implementation, NDIS 6.1 TCP/IP Stack Implementation, Introduction to Display Drivers, Drivers for Enumerating File/Process/Port/Registry (Assuagement for hiding), File System Implementation, Bus/DMA Driver, Linux Driver Introduction, Enumeration of Process file and registry and port, MAC/OSX Driver Introduction, Enumeration of Process file and registry and port.

Text books and References:

1. R. Love, Linux System Programming: Talking Directly to the Kernel and C Library. O'Reilly Media, Inc., 2013.
2. Russinovich, Solomon, "Windows Internals". Microsoft Press, 4thEdition, 2012.
3. N. Wilt, The CUDA Handbook: A Comprehensive Guide to GPU Programming.Reading, MA, USA: Addison-Wesley, 2013.
4. M. Barr and A. Massa, Programming Embedded Systems: With C and GNU Development Tools, 2nd ed. Sebastopol, CA:O'Reilly, 2006.

COE-583

Information Warfare

Objective:

This course addresses some of the unique and emerging policy, doctrine, strategy, and operational requirements of conducting cyber warfare at the nation-state level. It provides students with a unified battle-space perspective and enhances their ability to manage and develop operational systems and concepts in a manner that results in the integrated, controlled, and effective use of cyber assets in warfare.

Learning Outcomes:

On completion of this course, students should be able to:

- explain the theory of data, information and knowledge as they pertain to information warfare
- apply strategies of using information as a weapon and a target
- apply the principles of offensive and defensive information warfare for a given context
- discuss the social, legal and ethical implications of information warfare
- evaluate contemporary information warfare concepts for their application in a corporate environment

Syllabus:

Introduction and Models of Information Warfare- Information Resources, The Value of Resources, Players, The Offense, The Defense, A Dual Role, Offensive Information Warfare, Increased Availability to Offensive Player, Decreased Availability to Defensive Player, Decreased Integrity, Other Classification Schemes, Defensive Information Warfare, Types of Defense, Information Security and Information Assurance, The CIA Model and Authorization, Playgrounds to Battlegrounds, Play, Motivation, Culture, More than Child's Play, Intellectual Property Crimes, Fraud, Computer Fraud and Abuse. Fighting Crime, Individual Rights, National Security, Foreign Intelligence, War and Military Conflict, Terrorism, Netwars, Protecting National Infrastructures.

Open Sources- Open Source and Competitive Intelligence, Privacy, Snooping on People Through Open Sources, Web Browsing, Privacy Regulations, Piracy, Copyright Infringement, Trademark Infringement, Dark Sides.

Psyops and Perception Management- Lies and Distortions, Distortion, Fabrication, Hoaxes, Social Engineering, Denouncement, Conspiracy Theories, Defamation, Harassment, Advertising, Scams, Spam Wars, Censorship, United States Restrictions.

Inside the Fence- Traitors and Moles, State and Military Espionage, Economic Espionage, Corporate Espionage, Privacy Compromises, Business Relationships, Visits and Requests, Fraud and Embezzlement, Bogus Transactions, Data Diddling, Inside Sabotage, Physical Attacks, Software Attacks, Penetrating the Perimeter, Physical Break-ins and Burglaries, Search and Seizure, Dumpster Diving, Bombs.

Computer Break-Ins and Hacking- Accounts, Getting Access, Tools and Techniques, A Demonstration, Network Scanners, Packet Sniffers, Password Crackers, Buffer Overþows and Other Exploits, Social Engineering, Covering up Tracks, Information Theft, Gathering Trophies, More than Trophies, Tampering, Web Hacks, Domain Name Service Hacks, Takedown, Remote Shutdown Extent.

Text books:

1. Daniel Ventre, Cyberwar and Information Warfare, John Wiley & Sons.2012
2. Daniel Ventre, Information Warfare, Wiley - ISTE (2009) (ISBN 9781848210943).

Reference books:

1. Information Warfare and Security, Dorothy E. Denning, Denning Edition 1, 1998 Addison-Wesley.
2. Dorothy Denning, Information Warfare and Security, Addison-Wesley (1998.)

COE-585

Mobile and Wireless Network Security

Objective:

The main learning objectives of this course are: To conceptualize the wireless environment idiosyncrasies in terms of security and privacy; to impart state-of-the-art technologies of wireless network security; to analyze the various categories of threats, vulnerabilities, countermeasures in the area of wireless and mobile networking; to familiarize students with the issues and technologies involved in designing a wireless system that is robust against attacks.

Learning Outcomes:

On completion of this course, students should be able to:

- attain knowledge of advanced security and privacy issues in wireless systems, including cellular and wireless LAN and MAN networks
- impart state-of-the-art technologies and protocols of wireless network security
- identify and investigate in-depth both early and contemporary threats to mobile and wireless networks security
- to apply proactive and defensive measures to deter and repel potential threats, attacks and intrusions
- to develop an understanding of security issues towards 4G architectures

Syllabus:

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 non-repudiation; Power management and selfishness issues, attacks in wireless networks; DoS and DDoS attacks, reaction to attacks, information processing for sensor networks.

Text books:

1. Lei Chen, Jiahuang Ji, Zihong Zhang, Wireless Network Security, Springer Science & Business Media,2013
2. Noureddine Boudriga, Security of Mobile Communications, 2010.

Reference books:

1. Levente Buttyán and Jean-Pierre Hubaux, Security and Cooperation in Wireless Networks, 2008. [Available Online]
2. James Kempf, Wireless Internet Security: Architectures and Protocols, 2008.
3. Patrick Traynor, Patrick McDaniel, and Thomas La Porta, Security for Telecommunications Networks, 2008.
4. Frank Adelstein, Sandeep K.S. Gupta, Golden G. Richard III, and Loren Schwiebert, Fundamentals of Mobile and Pervasive Computing, 2005.

COE-587

Secure Coding

Course Objective: This course aims to provide an understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities. It gives an outline of the techniques for developing a secure application.

Learning Outcomes

On successful completion of this course, students will be able to:

- To implement security as a culture and show mistakes that make applications vulnerable to attacks.
- To understand various attacks like DoS, buffer overflow, web specific, database specific, web-spoofing attacks.
- To demonstrate skills needed to deal with common programming errors that lead to most security problems and to learn how to develop secure applications.
- To identify the nature of the threats to software and incorporate secure coding practices throughout the planning and development of the product.
- Able to properly handle application faults, implement secure authentication, authorization and data validation controls used to prevent common vulnerabilities.

Syllabus:

Introduction: Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks. IP Spoofing, Tear drop,DoS, DDoS,XSS, SQL injection, Smurf, Man in middle, Format String attack. Types of Security Vulnerabilities- buffer overflows, Invalidated input, race conditions, access-control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.

Need for secure systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC) , Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline.

Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defence in Depth and Principle of Least Privilege.

Secure Coding Techniques: Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices In Java Technology. ARP Spoofing and its countermeasures. Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors,FormatString Bugs. Security Issues in C Language: String Handling, Avoiding Integer Overflows and Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks,Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM

Database and Web-specific issues: SQL Injection Techniques and Remedies,Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and

Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters.

Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers

Text books and References:

1. Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press, 2nd Edition, 2004
2. Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckar,Syngress,1st Edition, 2005
3. Threat Modeling, Frank Swiderski and Window Snyder,Microsoft Professional, 1st Edition, 2004.

COE-589

Special Topics in Security-I

Course Objectives:

Objective of this course is to:

- Provide information to the students regarding emerging web application vulnerabilities.
- Deliver the information regarding tools which are utilized for the exploitation of the cyber security vulnerabilities.
- Secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage.
- Understand key terms and concepts in cyber law, intellectual property and cyber crimes, trademarks and domain theft.
- Determine computer technologies, digital evidence collection, and evidentiary reporting in forensic acquisition.

Learning Outcomes

Upon completion of this course, students will be able to:

- Describe and analyze the hardware, software, components of a network and the interrelations.
- Explain networking protocols and their hierarchical relationship hardware and software. Compare protocol models and select appropriate protocols for a particular design.
- Manage multiple operating systems, systems software, network services and security. Evaluate and compare systems software and emerging technologies.
- Develop solutions for networking and security problems, balancing business concerns, technical issues and security.
- Explain concepts and theories of networking and apply them to various situations, classifying networks, analyzing performance and implementing new technologies.

Syllabus:

Internet of Things (IOT): IoT architectures, IoT enabling technologies, IoT Big Data Analytics, IoT security and privacy concerns.

Computing paradigms: Virtualization Vulnerabilities, Hypervisor Security-Related Issues, Side Channel Attacks, Data Segregation, ubiquitous, grid, cloud, pervasive, green, ad hoc (*mobile*, *vehicular*, *flying*) networks.

Spear Phishing: Advanced Persistent Threats, Reconnaissance.

Digital Rights Management (DRM): Usage Rights, Rights Expression Language, Open Digital Rights Language.

Android-based Smartphone Security, Stepping Stone Detection, Broken Authentication and Session Management Vulnerabilities, Computer Forensic Investigation, Cyber Terrorism.

Text books and References:

1. Gunter Ollmann 2007. The Phishing Guide Understanding & Preventing Phishing Attacks. IBM Internet Security Systems.
2. Thomas Erl, Ricardo Puttini, ZaighamMahmood, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.
3. RajkumarBuyya, Christian Vecchiola, S. ThamaraiSelvi, Mastering Cloud Computing, Tata McGraw-Hill Education, 2013.
4. M. N. Omar et al, "Hybrid Stepping Stone Detection Method," in the proceeding of 1st IEEE Conference on Distributed Framework and Applications (DFmA – 2008), pp. 134–138, 2008
5. J. Yang, Shou-Hsuan Stephen Huang, "Matching TCP packets and its application to the detection of long connection chains on the Internet," in the proceeding of 19th IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 1005-1010,2005
6. Rosenblatt B., Tripp B., Mooney S., "Digital Rights Management: Business and Technology", John Wiley & Sons, 2001.

COE-552

Number Theory and Cryptology

Objective:

The objective of this course is:

- To introduce the student to elementary number theory, as required for further study of important cryptographic protocols.
- To introduce the student to the fundamentals of modern symmetric cryptography.
- To enable the student to appreciate the significance of cryptography as a means of securing information in the modern world.

Learning Outcomes:

On successful completion of this course, students will be able to:

- Understand the significance of cryptography to the modern world and the internet.
- Understand the rationale behind block cipher design.
- Perform the cryptanalysis of a simple block cipher.
- Integrate cryptographic algorithms into software projects.
- Solve elementary problems in number theory relating to cryptography.
- Build on number theoretic basics to further their knowledge of advanced methods of cryptography.

Syllabus:

Basic Cryptography Concepts- Basic Cryptography Concepts: Symmetric Encryption Algorithms, Purpose of Cryptography, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES).

Classical methods: Caesar cipher, Vigenere cipher, The one-time pad, Mechanical rotor systems

Modern ciphers: Block ciphers and their applications, Structure of a block cipher, The Fiestel structure, Key and block size length, The Data Encryption Standard (DES), The Advanced Encryption Standard (AES)

Hash Functions: One-way hash functions and their applications, SHA-1 and its successors.

Cryptanalysis: Linear cryptanalysis, Differential cryptanalysis, Meet-in-the-middle attacks.

Key Distribution: The key distribution problem, The Diffie-Hellman method, RSA and related methods

Elementary Number Theory: Finite fields, Modular arithmetic, Efficient algorithms for modular arithmetic, Fermat's little theorem, Euler's criteria, Euler's totient function

Advanced Number Theory: Primality testing, prime factorisation, The Chinese remainder theorem, Quadratic residues and calculating modular square roots and cube roots, The Jacobi symbol

Text Books:

1. A Course in Number Theory and Cryptography, Â Neal Koblitz, (Springer 2006)
2. An Introduction to Mathematical Cryptography, Jill Pipher, Jeffrey Hoffstein, Joseph H. Silverman (Springer, 2008)
3. An Introduction to theory of numbers, Niven, Zuckerman and Montgomery, (Wiley 2006)
4. Elliptic curves: number theory and cryptography, Lawrence C. Washington, (Chapman & Hall/CRC 2003)

Reference Books:

1. An Introduction to Cryptography, R.A. Mollin (Chapman & Hall, 2001)
2. Rational Points on Elliptic Curves, Silverman and Tate (Springer 2005)
3. Guide to elliptic curve cryptography Hankerson, Menezes, Vanstone (Springer, 2004)
4. Elementary Number Theory, Jones and Jones (Springer, 1998)

COE-554

Introduction to Cyberspace Operations and Design

Objective:

This course provides a basic understanding of full-spectrum cyberspace operations, the complexities of the cyberspace environment, as well as planning, organizing, and integrating cyberspace operations. The course will consist of presentations and exercises that will teach students how to develop a cyber-operations design and bring it to fruition. At the conclusion of the course, students will have a fundamental understanding of how to analyze, plan for, and execute cyberspace operations.

Learning Outcomes:

In this course, students will gain a better understanding of cyber operations (CO) for the deployment of computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE), against an adversary to achieve objectives and cause effects in support of a mission set.

This course, founded on concept operations and real cyber capabilities, provides students with the understanding, tools, and processes needed to conduct malware analysis with real-world malicious code samples to dissect. Students will be able to prepare and plan an effective offensive and defensive strategy, as well as evaluate covert protocols. Analysis of system specific, non-descript tools will be introduced to aid in attack and defense. After attending this course students will have the knowledge of following topics

1. Understanding of Cyberspace Environment and Design
2. Cyberspace Operational Approaches
3. Cyberspace Operations
4. Cyberspace Integration
5. Building Cyber Warriors and Warrior Corps
6. Designing Cyber Related Command
7. Training and Readiness for Cyber Related Commands

Syllabus:

Understanding the Cyberspace Environment and Design- Cyberspace environment and its characteristics, Developing a design approach, Planning for cyberspace operation

Cyberspace Operational Approaches- Foundational approaches that utilize cyberspace capabilities to support organizational missions, The pros and cons of the different approaches

Cyberspace Operations- Network Operations (NETOPS), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Defense and Diversity of Depth network design, Operational methodologies to conduct cyberspace operations

Cyberspace Integration- Design a cyberspace operation and integrate it with a Joint Operations plan, Practice the presented methodologies in a practical application exercise

Building Cyber Warriors and Warrior Corps- The warrior and warrior corps concept as applied to cyber organizations, The challenges of training and developing a cyber-workforce from senior leadership to the technical workforce

Designing Cyber Related Commands- Mission statements, Essential tasks, Organizational structures, Tables of organizations

Training and Readiness for Cyber Related Commands- Mission Essential Tasks (METs), Developing the cyber workforce, Plan your own training programs within your organization.

Text books and References:

1. Paulo Shakarian et al. "Introduction of Cyber Warfare: A Multidisciplinary Approach," syngress, Elsevier 2013.
2. Jeffery carr et al, "Inside Cyber Warfare: Mapping the Cyber Underworld," O'Reilly Publication December 2012.
3. Jason Andress et al. "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners" Syngress, Elsevier 2013.
4. R. A. Clarke, Robert Knake "Cyber War: The Next Threat to National Security and What to Do About It" Haper Collins Publisher 2010.

COE-524

Soft Computing

Objective:-This syllabus covers the different domains of soft computing techniques like neural networks, fuzzy logic, genetic algorithm and swarm optimization.

Learning Outcomes:- After completion of this course, **s**tudents will be able design robust and low-cost intelligent machines.

Syllabus:-

Soft Computing and Artificial Intelligence: Introduction of Soft Computing, Soft Computing vs. Hard Computing, Various Types of Soft Computing Techniques, Applications of Soft Computing, AI Search Algorithm, Predicate Calculus, Rules of Interference, Semantic Networks, Frames, Objects, Hybrid Models.

Artificial Neural Networks and Paradigms : Introduction, Neuron Model, Neural Network Architecture, Learning Rules, Perceptrons, Single Layer Perceptrons, Multilayer Perceptrons, Back propagation Networks: Kohnen'sself organizing networks, Hopfield network, Applications of NN.

Fuzzy Logic: Introduction, Fuzzy sets and Fuzzy reasoning, Basic functions on fuzzy sets, relations, rule based models and linguistic variables, fuzzy controls, Fuzzy decision making, applications of fuzzy logic.

Neuro - Fuzzy Modeling : Adaptive Networks Based Fuzzy Interface Systems, Classification and Regression Trees, Data Clustering Algorithms, Rule Based Structure Identification, Neuro-Fuzzy Controls, Simulated Annealing, Evolutionary Computation.

Genetic Algorithms and Swarm Optimizations: Introduction, Genetic Algorithm, Fitness Computations, Cross Over, Mutation, Evolutionary Programming, Classifier Systems, Genetic Programming Parse Trees, Variants of GA, Applications, Ant Colony Optimization, Particle Swarm Optimization, Artificial Bee Colony Optimization.

Text books:

1. Srikanta Patnaik, Baojiang Zhong, Soft Computing Techniques in Engineering Applications,Springer 2014
2. Anupam Shukla, Real Life Applications of Soft Computing, CRC Press, 2010

Reference books:

1. Saroj Kaushik, Artificial Intelligence, Cengage Learning, 2007.
2. Zimmermann, "Fuzzy Set Theory and its Application", 3rd Edition, 2001.
3. Jang J.S.R., Sun C.T. and Mizutani E, "Neuro-Fuzzy and Soft computing", Prentice Hall, 1998.
4. Timothy J. Ross, "Fuzzy Logic with Engineering Applications", McGraw Hill, 1997.
5. D.E. Goldberg, "Genetic Algorithms: Search, Optimization and Machine Learning", Addison Wesley, N.Y, 1989.

COE-572

Biometric Security

Objective:

To provide students with understanding of biometrics, biometric equipment and standards applied to security

Learning Outcomes:

Successful completion of this course will prepare the students to:

- Explain different biometrics parameters
- Evaluate and design security systems incorporating biometrics
- Perform R&D on biometrics methods and systems
- Understand the privacy challenges of Biometrics
- Explain the errors generated in biometric measurements
- Understand the technology of biometrics for public policy matters involving security and privacy.

Syllabus:

Overview of Biometrics: Definitions, biometric modalities, basic applications, access control, security
Biometric System Architecture: Scanning/digitizing, enhancement, feature extraction, classification, matching, searching and verification.
Probability, statistics and estimation Random variables, discrete and continuous distribution - pattern classification and recognition - Signals in time and frequency domain – multivariate statistical analysis.
Algorithms Face recognition Voice Recognition Fingerprint Recognition Iris Recognition
Other biometric modalities: Retina, signature, hand geometry, gait, keystroke
Quantitative analysis on the biometrics, Performance evaluation in Biometrics – false acceptance rate; false rejection rate.
Multimodal Biometric systems Biometric system integration, multimodal biometric systems: theory and applications, performance evaluation of multimodal biometric systems.
Biometric System Security: Biometric attacks/tampering; solutions; biometric encryption;

Text books:

1. Benjamin Muller, Security, Risk and the Biometric State: Governing Borders and Bodies, 1st Edition, Routledge, 2010.
2. Anil K jain, Patrick Flynn, Arun A. (Eds.), Handbook of Biometrics, Springer, 2008.

Reference books:

1. Julian D. M. Ashbourn, Biometrics: Advanced Identify Verification: The Complete Guide, Springer-verlag, 2000.
2. Davide Maltoni, Handbook of Fingerprint Recognition.
3. Biometric Systems: Technology, Design and Performance Evaluation, Editors: J. Wayman, A. Jain, D. Maltoni and D. Maio, Springer, 2005

COE-574

Information Security Risk Management

Objective:

To understand and development of concepts required for risk-based planning and risk management of computer and information systems.

Learning Outcomes:

After completion of this course, students will be able to learn:

- The cognitive skills and ability to identify, analyze and articulate the importance of managing IS-related risk and security issues in organizations, and the relationship between these and the achievement of business value from IS/IT investments
- The cognitive skills and ability to identify, analyze, synthesize and evaluate the costs of not appropriately identifying and managing risk and security concerns in projects and organizations, resulting in IS/IT failures, dysfunctional systems, and systems which fail to deliver value to key stakeholders
- The cognitive skills and practical ability to develop and document IS/IT risk and security management plans that detail contingency planning strategies and practices
- The cognitive skills and ability to identify, analyze, synthesize and articulate the major theories and concepts associated with IS failure and the management of IS risk, including factors argued to lead to unsatisfactory outcomes with respect to IS/IT and Information Security

Syllabus:

An Introduction to Risk Management: Introduction to the Theories of Risk Management; The Changing Environment; The Art of Managing Risks.

The Threat Assessment Process: Threat Assessment and its Input to Risk Assessment; Threat Assessment Method; Example Threat Assessment;

Vulnerability Issues: Operating System Vulnerabilities; Application Vulnerabilities; Public Domain or Commercial Off-the-Shelf Software; Connectivity and Dependence; Vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response, vulnerability of critical infrastructures;

The Risk Process: What is Risk Assessment? Risk Analysis; Who is Responsible?

Tools and Types of Risk Assessment: Qualitative and Quantitative risk Assessment; Policies, Procedures, Plans, and Processes of Risk Management; Tools and Techniques; Integrated Risk Management; Future Directions: The Future of the Risk Management.

Text books:

1. Malcolm Harkins, Managing Risk and Information Security, Apress, 2012.
2. Daniel Minoli, Information Technology Risk Management in Enterprise Environments, Wiley, 2009.

Reference books:

1. Andy Jones, Debi Ashenden ,Risk Management for Computer Security: Protecting Your Network & Information Assets, , 1st Edition, Butterworth-heinemann, Elsevier, 2005.
2. Andreas Von Grebmer, Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security, 2008, Books On Demand Gmbh.

COE-576

Proactive Security Tools and Techniques

Objective: The objective of this course is the use and application of security tools and techniques on real life scenarios such as cyber security consultancy and forensics. In addition to this, students will be able to improve their technical skill-sets and enhance their learning experiences through the use of various cyber tools.

Learning Outcomes:

After completion of this course, students will be able to:

- Understand how important security principles must be adhered to when securing the infrastructures
- Understand the importance of balancing security, operational effectiveness and cost
- Analyze and to aptly secure the cyber perimeter of the infrastructures against cyber attacks

Syllabus:

Network Security tool taxonomy: Reconnaissance tools, attack and penetration tools, defensive tools.

High, Medium, Low and Virtual honeypots, NMAP, TCPDUMP, Wireshark, Reverse firewalling, securing honeypots, sebek, Argos, Honeywall.

Hybrid systems, client honeypots, Botnets, tracking botnets, analysing malware.

Capturing malware using honeypots, implementing honeypots, medium interaction and high interaction honeypots.

Security metrics: What is a security metric? Metric and measurement, Designing effective security metrics, Data sources for security metrics, Analysis of security metrics data, Designing the security measurement project, Measuring security cost and value, Different context for security process management.

Text books:

1. Gary M. Jackson, Predicting Malicious Behavior, John Wiley & Sons, 2012.
2. Niels Provos, Thorsten Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison Wesley, 2007.
3. IT Security Metrics, Lance Hayden, Tata McGraw Hill.

Reference books:

1. Lance Spitzner, Know Your Enemy: Learning about Security Threats (2nd Edition), 2004.
2. Building Open Source Network Security Tools: Components and Techniques, Mike Schiffman.

COE-578

Social Network Analysis

Objectives:

To learn about structure and evolution of networks, to build a framework of network analysis that covers measures such as density, centrality, clustering, centralization, and spatialization.

Learning Outcomes:

On completion of this course, students will be able to:

- Understand various concepts in networks like nodes, edges, various topologies, node degrees
- Understand dynamics and evolution of social networks
- Understand the development of social structures
- Understand the framework of network analysis
- Compare and study various random network models
- Understand the concept of network centrality with various concepts like betweenness, closeness, page ranks etc.
- Know about various community concepts like: clustering, community structure, modularity
- Understand how various social media networks are working and using SNA in their infrastructure

Syllabus:

Networks- Concepts: nodes, edges, adjacency matrix, one and two-mode networks, node degree

Random network models: Erdos-Renyi and Barabasi-Albert- Concepts: connected components, giant component, average shortest path, diameter, breadth-first search, preferential attachment

Network centrality- Concepts: Betweenness, closeness, eigenvector centrality (+ PageRank), network centralization

Community- Concepts: clustering, community structure, modularity, overlapping communities

Small world network models, optimization, strategic network formation and search- Concepts: small worlds, geographic networks, decentralized search

Contagion, opinion formation, coordination and cooperation- Concepts: simple contagion, threshold models, opinion formation**,** unusual applications of SNA

SNA and online social networks- Concepts: how services such as Facebook, LinkedIn, Twitter, Couch Surfing, etc. are using SNA to understand their users and improve their functionality

Text books and References:

1. John Scott, Social Network Analysis, 3rd Edition, SAGE, 2012.
2. Wouter de Nooy, Andrej Mrvar, Vladimir Batagelj, Exploratory Social Network Analysis with Pajek, 2nd Revised Edition, Cambridge University Press, 2011.
3. Patrick Doreian, Frans Stokman, Evolution of Social Networks, Routledge, 2013.
4. David Easley and Jon Kleinberg, Networks, Crowds, and Markets: Reasoning About a Highly Connected World, Cambridge University Press, 2010.

COE-580

Enterprise Security & Management

Course Objectives

The main objective of this course is to study and understand the essentiality of the security in organizations that deal with data and are connected to the Internet. This course will help to understand risks involvement in managing and storing information assets in organizations.

Learning Outcomes

Upon successful completion of this course, students should be able to:

- Understand basics of enterprise security
- Understand need of enterprise security
- Study various possible cyber attacks and its adverse effects on organization
- Understand various risks in enterprise security

Syllabus

Introduction to Enterprise Security, Identifying information assets and organization risk exposure, Discovering security holes in organization, Defining corporate risks and risk management issues, Business risks related to privacy and regulatory considerations, Conceptual review of detection, assessment, hardening techniques, Possible attacks on enterprises, Active Defense Mechanisms, Corporate Security Policies, Conducting Vulnerability Analysis, Security Automation Technologies, Security Content Automation Protocol (SCAP) technologies and standards

Text books and References:

1. Jake Kouns, Daniel Minoli, Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams, John Wiley & Sons, 2011
2. Dave Tyson, Security Convergence: Managing Enterprise Security Risk, Butterworth-Heinemann, 2011
3. Malcolm Harkins, Managing Risk and Information Security: Protect to Enable, Apress, 2012

4. Greg Witte, Melanie Cook, Matt Kerr, Shane Shaffer, Security Automation Essentials: Streamlined Enterprise Security Management & Monitoring with SCAP, McGraw Hill Professional, 2012

COE-582

SCADA & DCS Security

Objective:

The subject aims to start with the study of basic concepts of SCADA communication systems and related protocols alongwith vulnerability detection and testing.

Learning Outcomes:

On completion of this course, students will have proper understanding of:

- Fundamentals of SCADA protocols.
- Basic working knowledge of SCADA & DCS.
- SCADA & DCS Security Management Implementation and Guidelines.
- Risk Assessment and Cyber Security concerns.

Syllabus:

Scada Basics- Scada and ICS Architecture, PLC and HMI Basics, RTOS - real time operating systems

Scada Related Protocols- Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC DA/HAD, SCADA protocol fuzzing

Finding Vulnerabilities in HMI software- Buffer Overflows, Shellcode

Previous attacks Analysis- Stuxnet, Duqu.

Hardware Testing- Jtag, GNU/Radio for Exploiting Radio Frequencies, SCADA RTOS firmware reversing

Text books and References:

1. T. Macaulay and B. L. Singer, Cyber security for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, Auerbach Publications, 2011.
2. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.

3. Robert Radvanovsky and Jacob Brodsky, editors. Handbook of SCADA/Control Systems Security. CRC Press, 2013.
4. A.W. Colombo, T. Bangemann, S. Karnouskos, S. Delsing, P. Stluka, R. Harrison, *et al.* Industrial cloud-based cyber-physical systems Springer International Publishing, 2014.
5. D. Bailey, Practical SCADA for Industry. Burlington, MA: Newnes, 2003.

COE-584

Ethics and Law of Cyber Security

Objective:
To understand the basics of cyber law, its related issues and ethical laws of computer for different countries.

Learning Outcomes:

The students of this course will be able to:

- Understand key terms and concepts in cyber law, intellectual property and cyber crimes, trademarks and domain theft.
- Determine computer technologies, digital evidence collection, and evidentiary reporting in forensic acquisition.
- Secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage.
- Incorporate approaches for incident analysis and response.

Syllabus:

Introduction-Cyber Security and its problem-Intervention Strategies: Redundancy, Diversity and Autarchy.

Introduction to the Legal Perspectives of Cybercrimes and Cyber security, Cybercrime and the Legal Landscape around the World, Why Do We Need Cyber laws, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Digital Signatures and the Indian IT Act, Cybercrime and Punishment, Cyber law, Technology and Students: Indian Scenario.

Private ordering solutions, Regulation and Jurisdiction for global Cyber security, Copy Right-source of risks, Pirates, Internet Infringement, Fair Use, postings, criminal liability, First Amendments, Data Losing.

Ethics, Legal Developments, Cyber security in Society, Security in cyber laws case studies, General lawand Cyber Law-a Swift Analysis.

Text books:

1. Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives, Wiley India Pvt. Ltd, 2011.

Reference books:

1. Mark F Grady, Fransesco Parisi, "The Law and Economics of Cyber Security", Cambridge University Press, 2006
2. Jonathan Rosenoer, "Cyber Law: The law of the Internet", Springer-Verlag, 1997.

COE-586
Fuzzing and Software Crash Analysis

Objective:
The objective of this course is to learn and understand basics concepts of fuzzing & methods of fuzzing. This course also provides knowledge of different fuzzing techniques and advance fuzzing concepts. By taking this course students will be able to understand and find the software security vulnerabilities.

Learning Outcomes:

After attending this course students will be able to:

- Discover zero-day vulnerabilities in programs running on fully-patched modern operating systems.
- Create exploits to take advantage of vulnerabilities through a detailed penetration testing process.
- Use the advanced features of IDA Pro and write your own IDC and IDA Python scripts.
- Perform remote debugging of Linux and Windows applications.
- Understand and exploit Linux heap overflows.
- Write Return-Oriented Shellcode.
- Perform patch diffing against programs, libraries, and drivers to find patched vulnerabilities.
- Perform Windows heap overflows and use-after-free attacks.
- Use precision heap sprays to improve exploitability.
- Perform Windows Kernel debugging up through Windows 8 64-bit.
- Jump into Windows kernel exploitation.

Syllabus:

Windows Exploit Development- Stack based Overflows, SEH based exploits, Unicode based Exploits, Bypassing Stack Cookies, SafeSeh, SEHOP, HW DEP and ASLR, Egg HuntersWriting W32 shellcode, Shellcode Injection (PE infection), Return Oriented Programming, Spraying the Heap, Introduction to Kernel Exploitation, Remote Kernel Exploitation on Windows 7 using

ROP, Introduction to exploits on 64-bit systems, Advanced Heap Spray techniques with Flash and HTML5, Leaked memory pointers and Dynamic ROP chains.

Windows Kernel Exploitation- Basics of Kernel Debugging with Windbg, Microsoft Kernel Vulnerabilities Overview, Null/Various Pointer Dereference Exploitation, Arbitrary Memory Overwrite Exploitation, Stack-Based Buffer Overflow Exploitation, Race Condition Exploitation, Recent Exploit Mitigation Technologies Overview, Pool Overflow/Corruption Exploitation, Hardcore Pool Overflow/Corruption Exploitation, Advanced Memory Corruption Techniques.

Linux Exploit Development- Introduction to Linux Exploit Development, Linux Format String Exploitation, Stack overflow in Linux, Stack Overflow ASLR bypass Using ret2reg, ASCII-Armor and ret2libc, Linux Shellcode development.

Text books and References:

1. Ari Takanen et al, "Fuzzing for Software Security Testing and Quality Assurance," Artech House, 2008.
2. Michael Sutton et al, "Fuzzing: Brute Force Vulnerability Discovery," Addison-wesley, 2007.

COE-588

Advanced Operating System Design and Security

Objective:

The aim of this course is to study, learn, and understand the main concepts of secure advanced operating systems design and Hardware and software features that support these systems.

Learning Outcomes:
After completion of this course, the students will be able to:

- Identify and define key terms related to operating systems
- Learn, and understand the main concepts of advanced operating systems design
- Learn OS issues related to the Internet, intranets, pervasive computing, embedded systems, mobile systems and wireless networks.
- Learn to design a secure operating systems

Syllabus:

Introduction, Access Control Fundamentals, Multics, Security in Ordinary Operating Systems, Verifiable Security Goals, Security Kernels, Securing Commercial Operating Systems, Solaris

Trusted Extensions, Building a Secure Operating System for Linux, Secure Capability Systems, Secure Virtual Machine Systems, System Assurance,.

Fault tolerance issues. OS issues related to the Internet, intranets, pervasive computing, embedded systems, mobile systems and wireless networks. Case studies of contemporary operating systems.
Comparative study of OS; UNIX, Multics, Unix File System + Measurements, The Log-Structured File System, Server less Network File Systems, The Coda File System, AFS, Virtual Memory, User-Level Virtual Memory, Software Fault Isolation. Issues of Security in OS, Cryptographic file systems.

Text books and References:

1. Mukesh Singhal and Niranjan Shivaratri, Advanced Concepts in Operating Systems, McGraw-Hill, 2011.
2. Trent Jaeger, Operating System Security, Morgan & Claypool Publishers, 2008.

COE-590

BIOS and SMM Security

Objectives:

To understand BIOS boot environments and how they interact with the platform architecture. To understand How System Management Mode (SMM) is instantiated and must be protected.

Learning Outcomes:

On completion of the course, students will be able to:

- Understand introductory concepts of BIOS UEFI/EFI boot process, System Management Mode (SMM), chipset architecture
- Understand how CPU caching can actually undermine SMM security
- Learn to fish so student can take their newly-acquired knowledge to further security research in this area
- Understand how the BIOS flash chip should be locked down
- Understand how the BIOS interacts with the Trusted Platform Module (TPM) and the measured boot process
- Understand details of System Management Interrupt (SMI) handlers

- Study various detection methods

Syllabus:

Introduction- Introduction to BIOS concepts UFFI/EFI Boot Process, Chipset architecture, Input/output (including PCI) and how the BIOS uses it to configure the system, PCI Option ROMs, BIOS' interaction with the TPM and the Measured Boot process, BIOS' lockdown of the serial flash where the BIOS itself resides, System Management Mode (SMM), CPU caching, Introduction to UEFI BIOS, The UEFI phases and security parameters specific to UEFI, Reverse engineering UEFI modules, Useful tools and methods for analyzing potentially malicious UEFI drivers

Reverse engineering System Management Interrupt (SMI) handlers: Brief Overview of BIOS Firmware, Overview of System Management Mode (SMM), Extracting binary of BIOS SMI Handlers, Hooking SMI handlers.

Text books and References:

1. Bryan Parno, Jonathan M. McCune, Adrian Perrig, Bootstrapping Trust in Modern Computers, Springer Science & Business Media, 2011.
2. Dave Shackleford, Virtualization Security: Protecting Virtualized Environments, John Wiley & Sons, 2012.
3. BRAGG, Network Security: The Complete Reference, McGraw Hill Professional, 2012.
4. Vincent Zimmer, Michael Rothman, Suresh Marisetty, Beyond BIOS: Developing with the Unified Extensible Firmware Interface, Intel Press, 2010.

COE-592

Disaster Recovery

Objectives:

The objective of this course is to provide students with:

- Understanding of the roles of the various phases of disaster management and issues concerning planning and policies in those phases.
- Understanding of comprehensive emergency management from a planning and policy Perspective.
- Understanding of the role of federal, state, and local governments in disaster planning and policies.
- Knowledge of mitigation planning and policy strategies.
- Understanding of comprehensive emergency management and related plans
- Understanding of factors affecting short and long-term recovery and rebuilding and the role of planners and policy-makers.

- Understanding of the factors that give rise to disaster vulnerabilities (e.g. natural, physical, social, economic, policies, and governance).
- Understanding of the factors that give rise to differential vulnerabilities and levels of community resilience
- Knowledge and capabilities to assess and manage these vulnerabilities through disaster planning and policy-making.
- Data, methods, tools, and geospatial techniques (including GIS) that can enhance vulnerability assessments and knowledge building.
- Competencies to utilize mapping in mitigation planning and response operations

Learning Outcomes:

After completing this course, you will be able to:

- Affirm the usefulness of integrating management principles in disaster mitigation work
- Distinguish between the different approaches needed to manage pre- during and post-disaster periods
- Explain the process of risk management
- Relate to risk transfer

Syllabus

Introduction: Hazards and Disasters: Planning and Policies, Disaster Mitigation Policies and Planning, Mitigation Planning and Policy Strategies: Local, State, and Federal Level, Measuring and Mapping Vulnerability, Social, Economic, and Political Vulnerabilities, Community Resilience, Emergency Management Planning, Communication and Risk Management (Policies and Plans), Disaster Response: Planning for Response, Supporting Emergency Response Operations using Geospatial Technologies, Collaboration and Coordination in Emergency Response Planning & Management, Disaster Recovery and Rebuilding, Long-term recovery, Post-Disaster Recovery Planning and Reconstruction, Post-Disaster Housing Planning.

Text books and References:

1. Waugh, William L. Jr. (2000). Living with Hazards, Dealing with Disasters: An Introduction to Emergency Management. Armonk, New York: M.E. Sharpe.
2. Burby, Raymond (1998). Cooperating with Nature: Confronting natural hazards with land-use planning for sustainable communities. Joseph Henry Press.
3. Birkland, Thomas. 2006. Lessons of Disaster: Policy Change after Catastrophic Events. Washington,D.C.: Georgetown University Press.
4. Drabek, Thomas. 2010. The Human Side of Disaster. Taylor and Francis

COE-536

Research Methodology

Objectives: Objective of this course is to make students able to:

- Understand research terminology
- To gain insights into how scientific research is conducted.
- To help in critical review of literature and assessing the research trends, quality and extension potential of research and equip students to undertake research.
- To critically analyze published research
- To learn and understand various research methods.
- To identify the influencing factor or determinants of research parameters.
- To test the significance, validity and reliability of the research results.
- To help in documentation of research results.
- To learn legal or ethical issues for an investigation.

Learning Outcomes:

At the end of this course, the student should be able to:

- Learn how scientific research is conducted
- Identify and justify an appropriate research methodology for an investigation.
- Conduct a literature review and use this to construct a research question suitable for conducting research at Masters level.
- Prepare a research proposal which includes justification of the chosen topic and an indication of the methods to be used.
- Able to learn legal and professional ethics.

Syllabus:

Introduction: Meaning and significance of research and scholarship; difference between undergraduate and research education; skills, habits and attitudes for research; status of research in India; course objectives.

Thinking skills: Problem solving, creativity, problem finding and formulation, Levels and styles of thinking; common-sense and scientific thinking; examples.Problem solving strategies – reformulation or rephrasing, techniques of representation, logical thinking, division into sub-problems, verbalization, awareness of scale; Importance of graphical representation; examples. Creativity – some definitions, illustrations from day to day life; intelligence versus creativity; gift or skill; creative process; requirements for creativity – role of motivation and open vs closed minds; multiple approaches to a problem, analytical vs analogical reasoning, puzzle solving; examples; prepared mind; Creative problem solving using Triz. Problem finding and literature survey, Information gathering – reading, searching and documentation; types, attributes and sources of research problems; problem formulation. Prescriptions for developing creativity and problem solving.

Experimental and modeling skills: Scientific method; role of hypothesis in experiment; units and dimensions; dependent a n d independent variables; control in experiment; precision and accuracy; need for precision; definition, detection, estimation and reduction of random errors;

statistical treatment of data; definition, detection and elimination of systematic errors; design of experiments; experimental logic; documentation; Types of models; stages in modeling; types of models; curve fitting; the art of making approximations; problem representation; logical reasoning; mathematical skills; finite element and Monte Carlo techniques of numerical simulation; Two case studies illustrating experimental and modeling skills.

Effective communication - oral and written: Examples illustrating the importance of effective communication; stages and dimensions of a communication process.Oral communication –verbal and non-verbal, casual, formal and informal communication; interactive communication; listening; form, content and delivery; various contexts for speaking- conference, seminar etc; visual aids Written communication - form, content and language; layout, typography and illustrations; contexts for writing – paper, thesis, reports etc.Prescriptions for developing communication skills.

Publishing and patenting: Difference between publishing and patenting; relative importance of various forms of publication; choice of journal and reviewing process; stages in the realization of a paper or a patent and how to handle these

Stress and time management, Interpersonal skill, professional ethics: Psychological phases of a PhD process; stress points; aims of supervisors; mismatches between scholar and supervisor and related problems. Managing self; empathy; managing relationships with your supervisor, colleagues, and supporting staff; listening; assertiveness; teamwork; sense of humor.Duration and stages of a PhD process; long term and short term goals; time tabling and deadlines. Profession; integrity, objectivity, fairness and consistency; loyalty; plagiarism and research ethics; safety

Text books:

1. E. M. Phillips and D. S. Pugh, "How to get a PhD - a handbook for PhD students and their supervisors", Viva books Pvt Ltd, 2010.

Reference books:

1. Handbook of Science Communication, compiled by Antony Wilson, Jane Gregory, Steve Miller, Shirley Earl, Overseas Press India Pvt Ltd, New Delhi, 1st edition, 2005.
2. G. L. Squires, "Practical physics", Cambridge University Press.

Related Links:

1. http://www.cs.virginia.edu/~robins/YouAndYourResearch.html Richard hamming, "You and your research",
2. http://www.apastyle.org/authorship.html"Reflections on Determining Authorship Credit and Authorship Order on faculty–student Collaborations"
3. http://abcnews.go.com/Technology/story?id=1831398"Where do good ideas come from?"

COE-538

Mobile Computing

Objective:

To understand modern trend of mobile computing and to acquire knowledge about the methodology followed in developing secure computing applications for cellular, MANET, and sensor environment.

Learning Outcomes:

At the end of this course, students will be able to learn recent development of mobile computing and to acquire knowledge about the methodology followed in developing secure computing applications for cellular, MANET, and sensor environment.

Syllabus:

Challenges in mobile computing, cellular Vs ad hoc mobile computing environments, coping with uncertainties, resource scarcity, bandwidth, and mobility, Routing in MANETs, TORA, TORA-based computing protocols, Fundamental problems, Synchronization, Mutual exclusion, Coordinator election, Agreement problems, Termination in cellular systems and MANETs, Handling fundamental challenges in faulty distributed environments, Causal message delivery, Publish/Subscribe, Concepts of graph theory applicable to MANETs, Minimum spanning tree, Ring, Tree, Hybrid architectures, Fault tolerance, Coordinated and Uncoordinated Check pointing, No blocking protocols.

Text books:

1.Prashant Kumar Pattnaik, Rajib Mall, Fundamental of mobile computing, PHI Learning Pvt. Ltd, 2012.
2.Mohd. Ilyas & Imad Mahgoub, Mobile Computing Handbook, CRC Press/Aurbach Publications, Boca Raton USA, 2005.

Reference books:

1.Theodore S. Rappaport, Wireless Communications: Principles and Practice, Second Edition, Prentice Hall, 2002.
2. Ivan Stojmenovic, Handbook of Wireless Networks and Mobile Computing, John Wiley & Sons, 2002.

COE-594

Ethical hacking

Objective:

Aim of this course is to teach students how to think like a hacker, providing them with a deep understanding of security issues and concerns. In addition, this course also provides the students with specialist knowledge and experience of advanced hacking techniques and their countermeasures.

Learning Outcomes:

Upon completion of this course, the students will be able to:

- Critically evaluate the potential countermeasures to advanced hacking techniques.
- Analyze and critically evaluate techniques used to break into an insecure web application and identify relevant countermeasures.
- Demonstrate a critical evaluation of an advanced security topic with an independent project.

Syllabus:

Introduction: Understanding the importance of security, Concept of ethical hacking and essential Terminologies-Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking, Foot printing, Scanning, System Hacking, Session Hijacking.

Buffer Overflows: Significance of Buffer Overflow Vulnerability, Why Programs/Applications are vulnerable. Reasons for Buffer Overflow Attacks. Methods of ensuring that buffer overflows are trapped.

Sniffers: Active and passive sniffing. ARP poisoning and countermeasures. Man in the middle attacks, Spoofing and Sniffing attacks. Sniffing countermeasures.

SQL Injection: Attacking SQL Servers, Sniffing, Brute Forcing and finding Application Configuration Files, Input validation attacks. Preventive Measures. Web Application Threats, Web Application Hacking, Cross Site Scripting / XSS Flaws / Countermeasures Correct Web Application Set-up.

Web Application Security: Core Defence Mechanisms. Handling User Access, Authentication, Session Management, Access Control.

Web Application Technologies: HTTP Protocol, Requests, Responses and Methods. Encoding schemes.Server side functionality technologies (Java, ASP, PHP).

Attacking Authentication: Attacking Session Management, Design Flaws in Authentication Mechanisms Attacking Forgotten Password Functionality, attacking Password change functions. Countermeasures to authentication attacks

Attacking other users: Reflected XSS Vulnerabilities, Stored XSS Vulnerabilities, DOM-Based XSS Vulnerabilities, HTTP Header Injection. Countermeasures to XSS.

Text books:

1. Patrick Engebretson, The Basics of Hacking and Penetration Testing, Elsevier, 2013.
2. Network Security and Ethical Hacking, Rajat Khare, Luniver Press, 2006.

Reference books:

1. Network intrusion alert: an ethical hacking guide to intrusion detection, Ankit Fadia, Manu Zacharia, Thomson Course Technology PTR, 2007.
2. Ethical Hacking, Thomas Mathew, OSB Publisher, 2003.
3. Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and George Kurtz, McGraw-Hill, 2005.

COE-596

Digital Forensics & Incident Response

Objective:

Aim of this course is to teach deep understanding of security issues and digital forensics & incident response. In addition, this course also provides the students with specialist knowledge and experience of various digital forensics techniques and incident response.

Learning Outcomes:

Upon completion of this course, the students will be able to:

- Understanding of various digital forensics techniques and its usage for the potential countermeasures or incident response.
- Demonstrate a critical evaluation and use of digital forensics technique to do incident response with an independent project.

Syllabus:

Forensics Overview: Computer Forensics Fundamentals, Benefits of Computer Forensics, Computer Crimes, Computer Forensics Evidence and the Courts, Legal Concerns and Privacy Issues

Forensics Process: Forensics Investigation Process, Securing the Evidence and Crime Scene, Chain of Custody, Law Enforcement Methodologies, Forensics Evidence, Evidence Sources. Evidence Duplication, Preservation, Handling, and Security, Forensics Soundness, Order of Volatility of Evidence, Collection of Evidence on a Live System, Court Admissibility of Volatile Evidence

Acquisition and Duplication: Sterilizing Evidence Media, Acquiring Forensics Images, Acquiring Live Volatile Data, Data Analysis, Metadata Extraction, File System Analysis, Performing Searches, Recovering Deleted, Encrypted, and Hidden files, Internet Forensics, Reconstructing Past Internet Activities and Events, E-mail Analysis, Messenger Analysis: AOL, Yahoo, MSN, and Chats

Mobile Device Forensics: Evidence in Cell Phone, PDA, Blackberry, iPhone, iPod, and MP3. Evidence in CD, DVD, Tape Drive, USB, Flash Memory, Digital Camera, Court Testimony, Testifying in Court, Expert Witness Testimony, Evidence Admissibility

Text books:

1. Jason Luttgens, Matthew Pepe, Kevin Mandia, Incident Response & Computer Forensics, McGraw-Hill Osborne Media, 3rd edition , 2014.
2. Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Real Digital Forensics: Computer Security and Incident Response, Paperback – Import, 2005.

Reference books:

1. John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Paperback, February 24, 2012.
2. Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and George Kurtz, McGraw-Hill, 2005.

COE-598

Data Mining and Analysis

Objectives: The objective of this course is:

- To introduce students to the basic concepts and techniques of Data Mining.
- To develop skills of using recent data mining software for solving practical problems.
- To gain experience of doing independent study and research.
- To demonstrate their ability to implement typical data mining techniques.
- To accurately evaluate the performance of algorithms, as well as formulate and test hypotheses.
- To implement and apply basic algorithms for supervised and unsupervised learning.

Learning Outcomes:

On completion of this course you should have gained a good understanding of the basic concepts, principles and techniques of data mining. Specifically, you should be able to:

- Define knowledge discovery and data mining.
- Recognize the key areas and issues in data mining.
- Apply the techniques of clustering, classification, association finding, feature selection and visualization to real world data.
- Determine whether a real world problem has a data mining solution.
- Apply evaluation metrics to select data mining techniques.

Syllabus:

Introduction to pattern recognition, Bayes Decision Theory, Linear Classifiers: Least square methods, Support Vector Machines, Non Linear Classifiers: Back Propagation Algorithm, Radial Basis Function Networks, Decision Trees, Random Forest, Combining Classifiers Algorithm, Association Rules Mining: Apriori algorithm, Partition algorithm, Dynamic inset counting algorithm, FP – tree growth algorithm, Generalized association rule, Temporal Data mining: Basic concepts of temporal data Mining, The GSP algorithm, Feature Generation, Feature Selection, Template Matching Techniques, Clustering Algorithms: Sequential Algorithms, Hierarchical clustering algorithms, Clustering algorithms based of cost function optimization, Clustering algorithms based on Graph Theory, Clustering algorithms based on competitive learning, Data Mining for Intrusion detection, Futuristic Technologies for Cyber Security

Text books and References:

1. Jiawei Han and Micheline Kamber, Data Mining: Concepts and Techniques, Morgan Kaufman Publishers, Third Edition, 2011.
2. F. Provost and T. Fawcett: Data Science for Business. O'Reilly Media, 2013.
3. Bing Liu: Web data Mining - Exploring Hyperlinks, Contents and Usage Data, Second Edition, Springer, 2011.
4. Pang-Ning Tan, Michael Steinbach, Vipin Kumar: Introduction to Data Mining, Pearson/Addison Wesley.
5. David Hand, Heikki Mannila, Padhraic Smyth: Principles of Data Mining, the MIT Press.

COE-600

Special Topics in Security-II

Objectives:

The students of this course will be able to:

- Incorporate approaches to secure networks, firewalls, intrusion detection systems, and intrusion prevention systems.
- Examine secure software construction practices.
- Understand principles of web security.
- Incorporate approaches for incident analysis and response.
- Incorporate approaches for risk management and best practices.

Learning Outcomes:

Upon completion of this course, students will be able to:

- Identify infrastructure components and the roles they serve, and design infrastructure including devices, topologies, protocols, systems software, management and security. Analyze performance of enterprise network systems.

- Effectively communicate technical information verbally, in writing, and in presentations.
- Use appropriate resources to stay abreast of the latest industry tools and techniques analyzing the impact on existing systems and applying to future situations.
- Explain the concepts of confidentiality, availability and integrity in Information Assurance, including physical, software, devices, policies and people. Analyze these factors in an existing system and design implementations.
- Cite and comply with relevant industry and organizational codes of conduct and ethics.

Syllabus:

Injection Vulnerabilities: Structured Query Language (SQL), Cross-Site Scripting (XSS).

Botnets: Measurement and Disinfection, Botnet Communication Topologies, Intelligence Resources, Sandboxed Tools.

Quantum Cryptography: Quantum Logic Gates, Quantum Algorithms, Physical Realization of Cubits, Single Photons, EPR Pairs.

Cyber Incident Analysis and Response: Incident Preparation, Incident Detection and Analysis, Containment, Eradication, and Recovery

Network Forensic Investigation: Forensic Technologies, Digital Evidence Collection, Evidentiary Reporting

GPS and Geo-Tagging, Forced Disclosure of Encryption Keys, Quantum Cryptography, Visual Cryptography, Biometrics in Cyber Physical Systems, Information hiding in iOS, Hyper-visor based Malware protection.

References:

1. Seth Fogie, Jeremiah Grossman, Robert Hansen, XSS Attacks: Cross Site Scripting Exploits and Defense, Syngress, 2007.
2. N. Namekata, S. Mori, and S. Inoue, “Quantum key distribution over an installed multimode optical fiber local area network”, Optical Express, 2005.
3. T.M.T. Nguyen, M. A. Sfaxi, and S. Ghernaouti-Hélie, "Integration of Quantum Cryptography in 802.11 Networks”, Proceedings of the FirstIntenationalConference on Availability, Reliability and Security (ARES), pp. 116-123, Vienna, April 2006.
4. Nagaraj V. Dharwadkar , B.B. Ambedker, S.R. Joshi, “Visual Cryptography for Color Image using Color Error Diffusion”, ICGSTGVIPJournal ,volume 10, issue 1,February 2010.