|  |
| --- |
| **KERALA TECHNOLOGICAL UNIVERSITY**  http://ktu.edu.in/images/logo_final.png  **SCHEME AND SYLLABUS**  **FOR**  **M. Tech. DEGREE PROGRAMME**  **IN**  **COMPUTER SCIENCE AND ENGINEERING**  **WITH SPECIALIZATION**  **CYBER SECURITY**  **CLUSTER 05 (ERNAKULAM II)**  **KERALA TECHNOLOGICAL UNIVERSITY CET Campus, Thiruvananthapuram Kerala, India -695016**  **(2015 ADMISSION ONWARDS)** |

**KERALA TECHNOLOGICAL UNIVERSITY**

**SCHEME AND SYLLABUS FOR M. Tech. DEGREE PROGRAMME**

**Branch: COMPUTER SCIENCE AND ENGINEERING**

**Specialization: CYBER SECURITY**

**SEMESTER – I**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Exam Slot*** | ***Course No*** | ***Subjects*** | L-T-P | Internal Marks | End Semester Exam | | Credits |
| Marks | Duration  (hrs) |
| A | 05CS 6201 | Mathematical Foundations For Cyber Security | 3-1-0 | 40 | 60 | 3 | 4 |
| B | 05CS 6203 | Advanced Data Structures and Algorithms | 3-1-0 | 40 | 60 | 3 | 4 |
| C | 05CS 6205 | Operating Systems And Security | 3-1-0 | 40 | 60 | 3 | 4 |
| D | 05CS 6207 | Cryptographic Protocols and Standards | 2-1-0 | 40 | 60 | 3 | 3 |
| E | 05CS 621x | Elective I | 2-1-0 | 40 | 60 | 3 | 3 |
|  | 05CS 6277 | Research methodology | 1-1-0 | 100 | 0 | 0 | 2 |
|  | 05CS 6291 | Information Security Lab | 0-0-2 | 100 | 0 | 0 | 1 |

21

|  |  |
| --- | --- |
| **Elective – I** | |
| **Course No** | **Subjects** |
| 05CS 6211 | Mobile Network Security |
| 05CS 6213 | Information Risk Management |
| 05CS 6215 | Data Mining and Machine Learning |

**SEMESTER – II**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Exam Slot*** | ***Course No*** | ***Subjects*** | ***L-T-P*** | ***Internal Marks*** | ***End Semester Exam*** | | ***Credits*** |
| Marks | Duration (hrs) |
| A | 05CS 6202 | Cyber Forensics | 3-1-0 | 40 | 60 | 3 | 4 |
| B | 05CS 6204 | Secure Coding | 2-1-0 | 40 | 60 | 3 | 3 |
| C | 05CS 6206 | Ethical Hacking | 3-1-1 | 40 | 60 | 3 | 3 |
| D | 05CS 622x | Elective II | 2-1-0 | 40 | 60 | 3 | 3 |
| E | 05CS 623x | Elective III | 2-1-0 | 40 | 60 | 3 | 3 |
|  | 05CS 6266 | Seminar I | 0-0-2 | 100 | 0 | 0 | 2 |
|  | 05CS 6288 | Mini Project | 0-0-4 | 100 | 0 | 0 | 2 |
|  | 05CS 6292 | Ethical Hacking And Digital Forensic Tools Lab | 0-0-2 | 100 | 0 | 0 | 1 |

21

|  |  |
| --- | --- |
| **Elective – II** | |
| **Course No** | **Subjects** |
| 05CS 6222 | Coding and Information Theory |
| 05CS 6224 | Design of Secured Architecture |
| 05CS 6226 | Digital Watermarking |

|  |  |
| --- | --- |
| **Elective – III** | |
| **Course No** | **Subjects** |
| 05CS 6232 | Cryptanalysis |
| 05CS 6234 | Distributed and Cloud Computing |
| 05CS 6236 | Storage management and Security |

**SEMESTER – III**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Exam Slot*** | ***Course No*** | ***Subjects*** | ***L-T-P*** | ***Internal Marks*** | ***End Semester Exam*** | | ***Credits*** |
| Marks | Duration (hrs) |
| A | 05CS 724x | Elective IV | 2-1-0 | 40 | 60 | 3 | 3 |
| B | 05CS 725x | Elective V | 2-1-0 | 40 | 60 | 3 | 3 |
|  | 05CS 7267 | Seminar II | 0-0-2 | 100 | 0 | 0 | 2 |
|  | 05CS 7287 | Project (Phase 1) | 0-0-8 | 50 | 0 | 0 | 6 |

14

|  |  |
| --- | --- |
| **Elective – IV** | |
| **Course No** | **Subjects** |
| 05CS 7241 | Cloud Security |
| 05CS 7243 | Cyber Laws and Security Policies |
| 05CS 7245 | Biometric Security |
| **Elective – V** | |
| **Course No** | **Subjects** |
| 05CS 7251 | Internet Information and application security |
| 05CS 7253 | Database Security |
| 05CS 7255 | Dependable Distributed Systems |

**SEMESTER – IV**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Exam Slot*** | ***Course No*** | ***Subjects*** | ***L-T-P*** | ***Internal Marks*** | ***End Semester Exam*** | | ***Credits*** |
| *Marks* | *Duration(hrs)* |
|  | 05CS 7288 | Project  (Phase 2) | 0-0-21 | 70 | 30 | - | 12 |

12

Total :68

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6201** | | **MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * Introduces basic concepts and knowledge in number theory, together with a wide variety of interesting applications of discrete mathematics. * Train students to solve problems from algorithm design and analysis, coding theory etc and to apply techniques of number theory in cryptography.  COURSE OUTCOMES:  * Number theory is intended to introduce students to number theoretic problems and to different areas of number theory. * Number theory has many applications especially to coding theory and cryptography. * Understand the ideas of group, ring and an integral domain and be aware of examples of these structures in mathematics. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | NUMBER THEORY: Introduction - Divisibility - Greatest common divisor - Prime numbers – Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat’s theorem - Euler totient function - Euler’s theoerem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem. | | | | 9 |
| **INTERNAL TEST 1(Module 1)** | | | | | |
| **II** | ALGEBRAIC STRUCTURES: Groups – Subgroup, Cyclic groups, group homomorphisms, Permutation groups, Cosets, Modulo groups - Primitive roots – Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Rings of polynomials, factorization of polynomials over a field. Fields – Finite fields – GF (pn), GF(2n) - Classification - Structure of finite fields. | | | | 9 |
| **INTERNAL TEST 2(Module 2)** | | | | | |
| **III** | CODING THEORY: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes. | | | | 10 |
| **IV** | STOCASTIC PROCESS and PSEUDORANDOM NUMBER GENERATION: Random Variables – discrete and continuous- central Limit Theorem-Stochastic Process- Markov Chain. Pseudorandom number generation: Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **REFERENCES:**   1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, ‘An introduction to the theory of numbers’, John Wiley and Sons 2004. 2. Douglas Stinson, ‘Cryptography – Theory and Practice’, CRC Press, 2006. 3. Sheldon M Ross, “Introduction to Probability Models”, Academic Press, 2003. 4. C.L. Liu, ‘Elements of Discrete mathematics’, McGraw Hill, 2008. 5. Fraleigh J. B., ‘A first course in abstract algebra’, Narosa, 1990. 6. Joseph A. Gallian, ‘’Contemporary Abstract Algebra’, Narosa, 1998. | | | | | |
|  | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6203** | | **ADVANCED DATA STRUCTURES AND ALGORITHMS** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * Familiarize with advanced data structures based trees and heaps. * Learn to choose the appropriate data structure and algorithm design method for a specified application. * Study approaches used to analyze and design algorithms and to appreciate the impact of algorithm design in practice. * Learn different advanced algorithms in dynamic programming, flow network * and computational geometry  COURSE OUTCOMES: After completion of the course completion, the students will be able   * To compare different implementations of data structures and to recognize the advantages and disadvantages of the different implementations. * To design, write, and analyze the performance of programs that handle structured data and perform more complex tasks, typical of larger software projects. * To determine which algorithm or data structure to use in different scenarios. * To demonstrate analytical comprehension of concepts such as abstract data , algorithms and efficiency analysis | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Trees -Threaded Binary Trees, Selection Trees, Forests and binary search trees, Counting Binary Trees, Red-Black Trees, Splay Trees, Suffix Trees, Digital Search Trees, Tries- Binary Tries-patricia, Multiway Tries. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Priority Queues **-** Single and Double Ended Priority Queues, Leftist Trees, Binomial Heaps, Fibonacci Heaps, Pairing Heaps, Symmetric Min-Max Heaps, Interval Heaps | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Analysis of Algorithms-review of algorithmic strategies, asymptotic analysis, solving recurrence relations through Substitution Method, Recursion Tree, and Master Method  Dynamic Programming-Rod cutting-top down and bottom up approach, matrix chain multiplication-recursive solution, Longest common subsequence problem | | | | 10 |
| **IV** | Maximum Flow**-**Flow Networks, Ford-Fulkerson method-analysis of Ford-Fulkerson, Edmonds-Karp algorithm, Maximum bipartite matching  Computational Geometry**-** Line segment properties, Finding the convex hull **,** Finding the closest pair of points.  Implementations using Python have to be conducted and evaluated for data structures and algorithms. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **REFERENCES:**   1. Ellis Horowitz, SartajSahni, Susan Anderson Freed, Fundamentals of Data Structures in C, Second Edition, University Press, 2008 2. YedidyahLangsam, Moshe J. Augenstein, Aaron M. Tenenbaum, Data Structures using C and C++, Second Edition, PHI Learning Private Limited, 2010 3. Thomas Cormen, Charles, Ronald Rives, Introduction to algorithm,3rd edition, PHI Learning 4. Ellis Horowitz and SartajSahni, SanguthevarRajasekaran, Fundamentals of Computer Algorithms,Universities Press, 2nd Edition, Hyderabad . 5. Sara Baase& Allen Van Gelder , Computer Algorithms – Introduction to Design and   Analysis, Pearson Education..   1. AnanyLevitin, Introduction to The Design & Analysis of Algorithms, Pearson   Education, 2nd Edition, New Delhi, 2008.   1. Berman and Paul, Algorithms, Cenage Learning India Edition, New Delhi, 2008. 2. S.K.Basu , Design Methods And Analysis Of Algorithms ,PHI Learning Private Limited, New Delhi,2008. 3. Jon Kleinberg and Eva Tardos, Algorithm Design, Pearson Education, NewDelhi, 2006. 4. Hari Mohan Pandey, Design Analysis And Algorithms, University Science Press, 2008. 5. R. Panneerselvam, Design and Analysis of Algorithms, PHI Learning Private Limited, New Delhi, 2009. 6. UditAgarwal, Algorithms Design And Analysis, DhanapatRai& Co, New Delhi, 2009. 7. Aho, Hopcroft and ullman, The Design And Analysis of Computer Algorithms, Pearson Education, New Delhi, 2007. 8. S.E.Goodman and S. T. Hedetmiemi, Introduction To The Design And Analysis Of Algorithms, McGraw-Hill International Editions, Singapore 2000. 9. Richard Neapolitan, Kumarss N, Foundations of Algorithms, DC Hearth &company.   Sanjay Dasgupta, Christos Papadimitriou, UmeshVazirani, Algorithms, Tata McGraw-Hill Edition. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6205** | | **OPERATING SYSTEM AND SECURITY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * Introduce students to the field of threads and vulnerabilities in OS and how to provide security in different OS. * Focuses on the study of techniques of fundamentals of protection systems, Information flow and Security kernels. This course also deals with a couple of case studies.  COURSE OUTCOMES: Upon completion, the student will be able to   * Understand the basic of securing an operating system. * Understand the principles of trusted systems, Information flow integrity and securing commercial OS. * Understand the security challenges with the help of case studies. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson’s Access Matrix, Mandatory protection system. Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History  Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domainand type enforcement. | | | | 10 |
| **IV** | Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration.  Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **REFERENCES:**   1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008 2. Michael Palmer, Guide to Operating system Security Thomson 3. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition 4. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont 5. Reading: Nachenberg, Computer Virus-Antivirus Coevolution. Comm. ACM, 40(1), pp. 46-51, January 1997. 6. Paxson, Bro: A System for Detecting Network Intruders in Real-Time. Proc. 7th USENIX Security Symposium, San Antonio, TX, January 1998 | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6207** | | **CRYPTOGRAPHIC PROTOCOLS AND STANDARDS** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To Enable Learner to understand various goals for designing a secure authentication and key establishment protocols. * Analyze various existing protocols in terms of the goals.  COURSE OUTCOMES:  * Will able to design a key agreement or key transport or key establishment protocol satisfying various security goals. * Will able to verify the security of a cryptographic protocol designed and analyzes the complexity of it. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Goals for authentication and Key Establishment: Basic Goals, Enhanced Goals, Goals concerning compromised Keys, Formal Verification of Protocols, Complexity Theoretic Proofs of Security. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Protocols Using Shared Key Cryptography: Entity Authentication Protocols, Server-Less Key Establishment, Server-Based Key Establishment, Key Establishment Using Multiple Servers. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Authentication and Key Transport Using Public Key Cryptography: Design Principles for Public Key Protocols, Entity Authentication Protocol, Key Transport Protocols. Key Agreement Protocols: Key Control, Unknown Key-Share Attacks, Classes of Key Agreement: Diffie-Hellman Key Agreement, MTI Protocols, Diffie-Hellman-Based Protocols with Basic Message Format and with Enhanced Message Format. ID based schemes: Okamoto's scheme, Gunther's scheme, Girault's scheme. | | | | 10 |
| **IV** | Conference Key Protocols: Generalizing Diffie-Hellman Key Agreement, Conference Key Agreement Protocols, Identity-Based Conference Key Protocols, Conference Key Agreement without Diffie-Hellman, Conference Key Transport Protocols, Key Broadcasting Protocols | | | | 8 |

|  |
| --- |
| **END SEMESTER EXAM (ALL Modules)** |
| **REFERENCES:**   1. Collin Boyd and AnishMathuria, "Protocols for Authentication and Key Establishment", Springer; 2010. 2. Abhijith Das and C.E. VeniMadha van, "Public-key Cryptography, Theory and Practice", Pearson Education, 2009. 3. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6211** | | **MOBILE NETWORK SECURITY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:  The main objective of the course is to introduce the students to security and privacy problems in the realm of wireless networks   * Creates Understanding about the basics of wireless technologies and security. * Gain in - depth knowledge on wireless and mobile network security and its relation to the new security based protocols * Apply proactive and defensive measures to counter potential threats, attacks and intrusions * Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks  COURSE OUTCOMES: Upon completion, the student will be able to   * Identify and investigate in-depth both early and contemporary threats to mobile and wireless networks security. * Apply proactive and defensive measures to deter and repel potential threats, attacks and intrusions. * Develop a clear view of integrated security environments consisting of both similar and diverse wireless access technologies and security architectures. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Transmission Fundamentals: Antennas and Wave Propagation. Cellular Wireless networks, Third Generation Systems, 4G Long Term Evolutions, Signal Encoding Techniques, Spread Spectrum, Coding and Error Control, Multiple Access in Wireless Systems. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Satellite Networks, Wireless System Operations and Standards, Wi-Max an Ultra Wide Band technologies, Mobile IP and Wireless Access Protocol. Wireless LAN Technology, Wi-Fi and IEEE 802.11 Wireless LAN Standard, Blue-tooth and IEEE 802.15 standard. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Threats to Wireless networks, ESM, ECM and ECCM, Proliferation of device and technologies, Practical aspects, Wireless availability, Privacy Challenges, Risks: Denial of Service, Insertion Attacks, Interception and monitoring wireless traffic, MIS configuration, Wireless Attacks, Surveillance, War Driving, Client-to-Client Hacking, Rogue Access Points, Jamming and Denial of Service. | | | | 10 |
| **IV** | Authentication, Encryption/Decryption in GSM, Securing the WLAN, WEP Introduction, RC4 Encryption, Data Analysis, IV Collision, Key Extraction, WEP Cracking, WPA/ WPA2, AES, Access Point-Based Security Measures, Third- Party Security Methods, Funk's Steel-Belted Radius, WLAN Protection Enhancements, Blue-tooth Security Implementation, Security in Wi- MAX, UWB security, Satellite network security. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **REFERENCES:**   1. KavehPahlavan and PrashantKrishnamurthy,"Principles of Wireless Networks", Prentice -Hall, 2006. 2. Cyrus Peikari and Seth Fogie, "Maximum Wireless Security" Sams, 2002. 3. Hideki lmai, Mohammad GhulamRahman and KazukuniKobari "Wireless Communications Security", Universal Personal Communications of Artech House, 2006. 4. Stallings William, "Wireless Communications and Networks” Second Edition, Pearson Education Ltd, 2009. 5. Jon Edney and William A. Arbaugh, " Real 802.11 Security: Wi-Fi Protected Access and 802.11i" , Addison-Wesley Professional, 2003. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6213** | | **INFORMATION RISK MANAGEMENT** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To understand the processes and measures that is used to manage risk to business critical information in an increasingly challenging cyber security environment. * Examine the way in which business and society make an assessment of, control and transfer risk. * To engage students in active discovery of risk management principles.  COURSE OUTCOMES: Upon completion, the student will be able to   * Understand the structured process that is used to manage the risk to information and data. * Realize what a business must, should or could do to address its risks. * Recognize the challenges unique to deploying the security measures. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Information Risk Management: Definitions and relationships among different security components - threat agent, threat, vulnerability, risk, asset, exposure and safeguards; Governance models such as COSO and COBIT, ISO 27000 series of standards for setting up security programs. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Risk analysis and management, policies, standards, baselines, guidelines and procedures as applied to Security Management program, Information strategy objectives. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Security awareness and training. Security Architecture and Design: review of architectural frameworks (such as Zachman and SABSA), concepts of Security Models (such as Bell-LaPadula, Biba and Brewer-Nash), vulnerabilities and threats to information systems (such as traditional on-premise systems, web based multi-tiered applications, distributed systems and cloud based services), application of countermeasures to mitigate against those threats and security products evaluation. | | | | 10 |
| **IV** | Business Continuity and Disaster Recovery: Business Continuity Management (BCM) concepts, Business Impact Analysis, BC/DR Strategy development, backup and offsite facilities and types of drills and tests. An introduction to Operational Security and Physical security aspects. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **REFERENCES:**   1. Alan Calder and Steve G. Watkins, "Information Security Risk Management for IS027001 /IS027002", IT Governance Ltd, 2010. 2. Susan Snedaker, "Business Continuity and Disaster Recovery Planning for IT Professionals", Elsevier Science & Technology Books, 2007. 3. Harold F Tipton and Micki Krause, "Information Security Management Handbook", Volume 1, Sixth Edition, Auerbach Publications, 2003. 4. Andreas Von Grebmer, "Information and IT Risk Management in a Nutshell: A Pragmatic Approach to Information Security" Books on Demand, 2008. 5. Evan Wheeler, " Security Risk Management" ,Elsevier, 2011. 6. Ian Tibble,"Security De-Engineering: Solving the Problems in Information Risk Management", CRC Press, 2012. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6215** | | **DATA MINING AND MACHINE LEARNING** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * Introduce students to the field of data mining and machine learning process. * Focuses on the study of techniques of clustering, classification, association finding, feature selection and visualization to real world data and determining whether a real world problem has a data mining solution.  COURSE OUTCOMES: Upon completion, the student will be able to   * Understand the basic data mining and machine learning algorithms. * Apply supervised and unsupervised learning algorithms to prediction problems. * Accurately evaluate the performance of algorithms, as well as formulate and test hypotheses. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Introduction- Data Mining, Machine Learning, Review of Cybersecurity Solutions. Classical Machine-Learning Paradigms for Data Mining - Fundamentals of Supervised Machine-Learning, Popular Unsupervised Machine-Learning Methods, Improvements on Machine-Learning Methods, Challenges in Data Mining, Challenges in Machine Learning | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Supervised Learning for Misuse/Signature Detection- Machine-Learning Applications in Misuse Detection- Rule-Based Signature Analysis, Artificial Neural Network, Support Vector Machine, Genetic Programming, Decision Tree and CART, Bayesian Network. Machine Learning for Anomaly Detection- Anomaly Detection, Machine Learning in Anomaly Detection Systems, Machine-Learning Applications in Anomaly Detection. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Machine Learning for Hybrid Detection- Hybrid Detection, Machine Learning in Hybrid Intrusion Detection Systems, Machine-Learning Applications in Hybrid Intrusion Detection. Machine Learning for Scan Detection- Scan and Scan Detection, Machine Learning in Scan Detection, Machine-Learning Applications in Scan Detection, Other Scan Techniques, Machine Learning for Profiling Network Traffic- Network Traffic Profiling and Related Network Traffic Knowledge, Machine Learning and Network Traffic Profiling, Data-Mining and Machine-Learning Applications in Network Profiling. | | | | 10 |
| **IV** | Privacy-Preserving Data Mining- Privacy Preservation Techniques in PPDM, Workflow of PPDM, Data-Mining and Machine-Learning Applications in PPDM- Privacy Preservation Association Rules, Privacy Preservation Decision Tree, Privacy Preservation Bayesian Network, Privacy Preservation KNN, Privacy Preservation k-Means Clustering. Emerging Challenges in Cyber security- Network Monitoring, Profiling, and Privacy Preservation, Challenges in Intrusion Detection. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **REFERENCES:**   1. SumeetDua and Xian Du, “Data Mining and Machine Learning in Cyber security” CRC press, Auerbach Publications 2011. 2. Christopher Westphal,” Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies” CRC Press, 2008. 3. Marcus A. Maloof, “Machine Learning and Data Mining for Computer Security: Methods and Applications” Springer Science & Business Media, 2006. 4. Jesus Mena,” Machine Learning Forensics for Law Enforcement, Security, and Intelligence”, CRC Press, 2011. 5. Ian H. Witten, Eibe Frank, Mark A. Hall,” Data Mining: Practical Machine Learning Tools and Techniques”, Elsevier, 2011. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6277** | | **RESEARCH METHODOLOGY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * + Aware of the research process.   + Familiarize the tools and skills to investigate a research.   + Preparation of an effective report.  COURSE OUTCOMES:  * + Able to do research in a systematic way.   + Effective use of appropriate tools for samples and data collection.   + Write research proposals and reports. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Introduction-Tools for Planning Research, Finding resources,  internet research skills, Evaluating and citing resources,  publishing research- literature review – problem definition  Reproducible research-focus on the concepts and tools behind reporting modern data analyses in a reproducible manner.  (Students are expected set up a GitHub account and/or take part in collaborative projects such as Mozilla Science Lab,Linux Foundation , Wikis or technical blogging) | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Sampling fundamentals -Types of sampling: probability and non-probability sampling.  Sampling theory, sampling distribution and sample size determination. Tools and techniques of data collection: Questionnaire and schedule for field surveys, interview, observation,  simulation, experimental and case study methods. Collection, recording, editing, coding and  scaling of data. Scale classification and types. Measurement of validity, reliability and  practicality. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Descriptive and inferential statistics - Data analysis and interpretation –testing of hypothesis,  testing of population mean, variance and proportion –Z test – t test – F test - chi square test.–  standard error of the estimate. Testing goodness of fit. Brief introduction to non parametric  tests, factor analysis, discriminant analysis and path analysis (description only). | | | | 10 |
| **IV** | Meaning of interpretation and inference: importance and care for interpreting results.  Presentation of reports: structure and style. Parts of a research report. Guidelines for writing  research papers and reports –. Ethics in research. Use of computers and internet in research.  Familiarization with Online tools for computer science researchers  **Case Study:** Familiarize Latex software for report preparation. Students have to take up a case study on particular samples and conclude with some hypothesis. A report of the same has to be submitted by the student at the end of this course. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **REFERENCES:**  1. C. R. Kothari, Research Methodology, Methods and techniques (New Age International  Publishers, New Delhi, 2004).  2. R. Panneerseklvam, Research Methodology (Prentice Hall of India, New Delhi, 2011).  3. Ranjit Kumar, Research Methodology, A step by step approach (Pearson Publishers,  New Delhi, 2005.  4. Management Research Methodology : K. N. Krishnaswami, AppaIyer and M  Mathirajan, Pearson Education, Delhi, 2010  5. Hand Book of Research Methodology : M N Borse, SreeNivas Publications, Jaipur,  2004  6. Business Research Methods: William G Zikmund, South – Western Ltd, 2003  7. Research Methods in Social Science: P K Majumdar, Viva Books Pvt Ltd, New Delhi,  2005  8. Analyzing Quantitative Data: Norman Blaikie, SAGE Publications , London, 2003  **Web References:**  Module 1  http://help.library.ubc.ca/evaluating-and-citing-sources/evaluating-information-sources/  http://www.vtstutorials.ac.uk/detective/  http://connectedresearchers.com/online-tools-for-researchers/  https://www.ucl.ac.uk/isd/services/research-it/research-software/infrastructure/github/signup  https://www.mozillascience.org/training  https://www.ucl.ac.uk/isd/services/research-it  http://researchkit.org/  https://www.cs.ubc.ca/our-department/facilities/reading-room/research-publications/research-tools  Module 4  http://www.i-studentglobal.com/study-programmes/science-engineering-computing-technology/50-essential-online-tools-for-every-computer-science-student | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| COURSE CODE | COURSE NAME | L-T-P-C | YEAR |
| **05CS 6291** | **INFORMATION SECURITY LAB** | 3-1-0-4 | 2015 |
| COURSE OBJECTIVES:   * The main objective this practical session is that students will get the exposure to various tools and programming methods using in information security.  COURSE OUTCOMES: By the completion of this laboratory session Student   * Will gain the knowledge on perl and Shell scripting languages to implement various security attacks. * Will get the ideas in various ways to trace an attacker. * Will get the practical exposure to software firewall, port monitoring etc….   The following programs should be implemented preferably on platform Windows/Linux through perl, shell scripting language and other standard utilities available with LINUX systems. :-   1. Write a perl script to concatenate ten messages and transmit to remote server    1. Using arrays    2. Without using arrays. 2. Write a perl script to implement following functions:    1. Stack functions    2. File functions    3. File text functions    4. Directory functions    5. Shift, unshift, Splice functions. 3. Write a Perl script to secure windows operating systems and web browser by disabling Hardware and software units. 4. Write a perl script to implement Mail bombing and trace the hacker. 5. Write a shell script to crack LINUX login passwords and trace it when breaking is happened. 6. Working with Sniffers for monitoring network communication (Ethereal) 7. Understanding of cryptographic algorithms and implementation of the same in C or C++. 8. Using open SSL for web server - browser communication 9. Using GNU PGP 10. Performance evaluation of various cryptographic algorithms 11. Using IP TABLES on Linux and setting the filtering rules 12. Configuring S/MIME for e-mail communication 13. Understanding the buffer overflow and format string attacks 14. Using NMAP for ports monitoring 15. Implementation of proxy based security protocols in C or C++ with features like confidentiality, integrity and authentication   **FOLLOWING ARE SOME OF THE WEB LINKS, WHICH HELP TO SOLVE**  **THE ABOVE ASSIGNMENTS:**   * http://linuxcommand.org/man\_pages/openssl1.html * http://www.openssl.org/docs/apps/openssl.html * http://www.queen.clara.net/pgp/art3.html * http://www.ccs.ornl.gov/~hongo/main/resources/contrib/gpg-howto/gpg-howto.html * https://netfiles.uiuc.edu/ehowes/www/gpg/gpg-com-0.htm * http://www.ethereal.com/docs/user-guide/ | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6202** | | **CYBER FORENSICS** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:  The main objective of the course is to introduce the students to bring awareness in crimes and tracing the attackers.   * Define digital forensics from electronic media. * Describe how to prepare for digital evidence investigations and explain the differences between law enforcement agency and corporate investigations. * Explain the importance of maintaining professional conduct  COURSE OUTCOMES: Upon completion, the student will be able to   * Utilize a systematic approach to computer investigations. * Utilize various forensic tools to collect digital evidence. * Perform digital forensics analysis upon networks and network devices. * Perform web based investigations. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Cyber forensics Introduction to Cyber forensics, Type of Computer Forensics Technology- Type of Vendor and Computer Forensics Services. Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases, Analyzing Malicious software. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Digital Evidence in Criminal Investigations. The Analog and Digital World, Training and Education in digital evidence, the digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies. Computer Forensics Evidence and Capture- Data Recovery-Evidence collection and Data Seizure-Duplication and preservation of Digital Evidence-Computer image verification and Authentication | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics. Computer Forensics Analysis- Discovery of Electronic Evidence- Identification of data- Reconstructing Past events- networks | | | | 10 |
| **IV** | Countermeasure: Information warfare- Surveillance tool for Information warfare of the future-Advanced Computer Forensics.  Cyber forensics tools and case studies. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **REFERENCES:**   1. Understanding Cryptography: A Textbook for Students and Practitioners: Christofpaar, Jan Pelzl. 2. Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts Ali Jahangiri 3. Handbook of Digital and Multimedia Forensic Evidence [Paperback] John J. Barbara 4. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics) 5. Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk 6. Information warfare : Information warfare and security: (ACM Press) by Dorothy   Elizabeth Robling Denning   1. Cyberwar and Information Warfare : Springer's by Daniel Ventre 2. Computer forensics: computer crime scene investigation, Volume 1 ( Charles River Media, 2008) By John R. Vacca | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6204** | | **SECURE CODING** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * Students shall understand vulnerabilities in coding, identify, and remediate them.  COURSE OUTCOMES: Upon completion, the student will be able   * To utilize a systematic approach to secure coding java and web applications. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Introduction, Security concepts, Security Architecture - Principles, coding in C and C++, Strings - String Characteristics, Common String Manipulation Errors, String Vulnerabilities, Process Memory Organization, Stack Smashing, Code Injection, Arc Injection, Notable Vulnerabilities. Pointer Subterfuge - Data Locations, Function Pointers, Data Pointers, Modifying the Instruction Pointer, Global Offset Table, The .dtors Section , Virtual Pointers, The atexit() and on\_exit() Functions, The longjmp() Function, Exception Handling. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Dynamic Memory Management - Common Dynamic Memory Management Errors, Doug Lea's Memory Allocator, RtlHeap, Integer Security - Integers, Integer Conversions, Integer Error Conditions, Integer Operations, Vulnerabilities, Nonexceptional Integer Logic Errors, Notable Vulnerabilities in Dynamic Memory Management and Integer Security | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Formatted Output - Variadic Functions, Formatted Output Functions, Exploiting Formatted Output Functions, Stack Randomization. File I/O - Concurrency, Time of Check, Time of Use, Files as Locks and File Locking, File System Exploits. | | | | 10 |
| **IV** | Web Application, SQL Injection, Web Server–Related Vulnerabilities (XSS, XSRF, and Response Splitting), Web Client–Related Vulnerabilities (XSS), Use of Magic URLs, Predictable Cookies, and Hidden Form Fields:- Overview, CWE References, Affected Languages, Explain, Spotting the Pattern, Code Review, Testing Techniques, Redemption Steps. | | | | 8 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **References:**   1. Robert C. Seaford, "Secure Coding in C and C++", Addison-Wesley Professional, 2005. 2. Mark G. Graff, Kenneth R. van Wyk, "Secure Coding: Principles & Practices" O'Reilly, 2003 3. Michael Howard, David LeBlanc, and John Viega, "24 DEADLY SINS OF SOFTWARE SECURITY" McGraw-Hill Companies, 2010. 4. James A. Whittaker and Herbert H. Thompson, "How to Break Software Security", Addison Wesley, 2003. 5. John C. Mitchell and Krzysztof Apt, "Concepts in Programming Languages", Cambridge University Press, 2001. | | | | | |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6206** | | **ETHICAL HACKING** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To render all the techniques used for penetration testing for performing security auditing. * To transform the internet security industry by infusing professionalism and efficiency.  COURSE OUTCOMES: By the end of the course students will   * Learn various hacking methods. * Perform system security vulnerability testing. * Perform system vulnerability exploit attacks. * Produce a security assessment report * Learn various issues related to hacking. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Casing the Establishment - What is footprinting- Internet Footprinting. -Scanning-Enumeration - basic banner grabbing, Enumerating Common Network services. Securing permission - Securing file and folder permission. Using the encrypting file system. Securing registry permissions. Securing service- Managing service permission. Default services in windows 2000 and windows XP. Unix - The Quest for Root. Remote Access vs Local access. Remote access. Local access. After hacking root. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Dial-up ,PBX, Voicemail, and VPN hacking - Preparing to dial up. War-Dialing. Brude-Force Scripting PBX hacking. Voice mail hacking . VPN hacking. Network Devices – Discovery, Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability. Detecting Layer 2 Media. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Wireless Hacking - Wireless Foot printing. Wireless Scanning and Enumeration. Gaining Access. Tools that exploiting WEP Weakness. Denial of Services Attacks. Firewalls- Firewalls landscape- Firewall Identification-Scanning Through firewalls- packet Filtering- Application Proxy Vulnerabilities . Denial of Service Attacks - Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. Unix and Windows DoS | | | | 10 |
| **IV** | Remote Control Insecurities - Discovering Remote Control Software. Connection. Weakness.VNC . Microsoft Terminal Server and Citrix ICA .Advanced Techniques Session Hijacking. Back Doors. Trojans. Cryptography . Subverting the systems Environment. Social Engineering. Web Hacking. Web server hacking web application hacking. Hacking the internet User **-** Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global Counter measures to Internet User Hacking. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **References**:   * + - 1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.       2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6222** | | **CODING AND INFORMATION THEORY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * + Covers information theory and coding within the context of modern digital communications applications.   + To help students in quantify the notion of information in a mathematically and intuitively sound way.   + Explaining how this quantitative measure of information may be used in order to build efficient solutions to multitudinous engineering problems  COURSE OUTCOMES: By the end of the course students will   * Learn various coding methods. * Learn various error control methods. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Source Coding - Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Channel capacity and coding - channel models, channel capacity, channel coding, information capacity theorem, random selection of codes. Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDS codes. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Cyclic codes - polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes, golay codes, CRC codes, circuit implementation of cyclic codes. BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes. | | | | 10 |

|  |  |  |
| --- | --- | --- |
| **IV** | Convolutional codes - tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding. Trellis Coded Modulation - concept of coded modulation, mapping by set partitioning, ungerboeck’s TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels. | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | |
| **References**:   1. Lin S. and D. J. Costello, "Error Control Coding — Fundamentals and Applications", Second Edition, Pearson Education Inc., NJ., USA, 2004 2. Shu Lin and Daniel J. Costello, "Error Control Coding", Second Edition, Prentice Hall, 1983. 3. Ranjan Bose, "Information Theory, Coding and Cryptography", Tata McGraw-Hill, 2003. 4. E. R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, New York, 1968. 5. R. E. Blahut, "Algebraic Codes for Data Transmission", Cambridge University Press Cambridge, UK, 2003. 6. Ranjan Bose, “Information theory, coding and cryptography”, Tata McGraw Hill, 2002. 7. Viterbi, “Information theory and coding”, McGraw Hill, 1982. 8. John G. Proakis, “Digital Communications”, 2nd Edition, McGraw Hill, 1989. | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6224** | | **DESIGN OF SECURED ARCHITECTURES** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * Students shall gain an understanding of the techniques and architectural components used to provide a secure computing environment.  COURSE OUTCOMES: Upon completion, the student will be able   * To know the strengths and weaknesses of different security design techniques. * To specify a security solution to fulfill specific design requirements. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Architecture and Security **-** Architecture Reviews**-**Software Process-Reviews and the Software Development Cycle-Software Process and Architecture Models-Software Process and Security- Architecture Review of System-Security Assessments**-**Security Architecture Basics**-** Architecture Patterns in Security. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Low-Level Architecture **-** Code Review**-**importance of code review**-** Buffer Overflow Exploits- Countermeasures against Buffer Overflow Attacks-patterns applicable- Security and Perl- Byte code Verification in Java-Good Coding Practices Lead to Secure Code- Cryptography- Trusted Code - Secure Communications | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Mid-Level Architecture **-** Middleware Security**-** Middleware and Security- The Assumption of Infallibility. High-Level Architecture **-** Security Components**-** Secure Single Sign-On- Public-Key Infrastructures- Firewalls- Intrusion Detection Systems-LDAP and X.500 Directories- Kerberos- Distributed Computing Environment-The Secure Shell, or SSH-The Distributed Sandbox- Security and Other Architectural Goals**-** Metrics for Non-Functional Goals-Force Diagrams around Security- High Availability- Robustness- Reconstruction of Events- Ease of Use- Maintainability, Adaptability, and Evolution- Scalability- Interoperability- Performance- Portability. | | | | 10 |
| **IV** | Enterprise Security Architecture **-** Security as a Process-Security Data- Enterprise Security as a Data Management Problem- Tools for Data Management- David Isenberg and the “Stupid Network”-Extensible Markup Language- The XML Security Services Signaling Layer-XML and Security Standards- The Security Pattern Catalog Revisited-XML-Enabled Security Data-HGP: A Case Study in Data Management. Business Cases and Security: Building Business Cases for Security | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **References:**   1. Jay Ramachandran, “Designing Security Architecture Solutions”, Wiley Computer Publishing, 2010. 2. Markus Schumacher, “Security Patterns: Integrating Security and Systems Engineering”, Wiley Software Pattern Series, 2010. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6226** | | **DIGITAL WATERMARKING** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To make the students aware of the basic mathematical concept behind watermarking theory and its main applications. * Provides the knowledge about the applications of watermarking techniques used and teaches about Watermark security and cryptographic methods used.  COURSE OUTCOMES: Upon completion, the Students will be able to   * Understand and identify digital watermarking from other related fields. * Explain different types of watermarking applications and watermarking frameworks. * Design digital watermarking systems according to application domains. * Analyze the different type of watermarking security issues. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Watermarking host signals: Image, Video, and Audio. Multimedia compression and decompression, Lossless compression, Models watermarking, Communication-based models of watermarking, Geometric models of watermarking, modeling watermark detection by correlation | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Basic message coding, Mapping message in message vectors, Error correction coding, Detecting multi-symbol watermarks, Watermarking with side information, Inform( embedding, Informed coding. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Structured dirty-paper codes, Analyzing errors, Message errors, ROC curves, The effect of whitening on error rates, Analysis of normalized correlation, Using perceptual mode, Evaluating perceptual impact of watermarks. | | | | 10 |
| **IV** | General forms of perceptual model, Perceptual adaptive watermarking, Robust watermarking, Watermark security, Watermark security and cryptography, Content authentication, Exact authentication, Selective, authentication, Localization, Restoration. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **References:**   1. Cox I., M. Miller, J. Bloom, J. Fridrich and T Kalker, "Digit Watermarking and Steganography", Second Edition, Morg Kaufmann Publishers, 2008. 2. E. Cole, R. Krutz, and J. Conley, Network Security Bible, Wiley-Dreamtech, 2005. 3. W. Stallings, Cryptography and Network Security Principles and practice, 3/e, Pearson Education Asia, 2003. 4. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3/e, Pearson Education, 2003. 5. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6232** | | **CRYPTANALYSIS** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * + To enable learner to understand various risks, threats and vulnerabilities in a system.   + Also gives security awareness and countermeasures to mitigate various risks, threats and vulnerabilities in a system.  COURSE OUTCOMES:  * Will able to design and analyze the security architecture designed for any system. * Will able to identify the security flows in any multi-tiered applications, distributed systems and cloud based services and mitigate it. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Cryptanalysis of classical ciphers: Vigenere cipher, Affine cipher, Hill-cipher Linear Shift Register Random Bit Generator: Berlekamp- Massey algorithm for the cryptanalysis of LFSR, Correlation attack on LFSR based stream ciphers, Cryptanalysis of ORYX, Fast algebraic attack. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Cryptanalysis of Block Ciphers: Man in the middle attack double DES, Linear and Differential cryptanalysis. Algorithmic Number Theory: Stein's binary greatest common divisor algorithm, Shanks Tonelli algorithm for square roots in Fp, Stein's greatest common divisor algorithm for polynomials. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Algorithms for DLP: Pollard Rho method for DLP, Shank's baby step Giant step algorithm for DLP Silver-Pohling-Hellman algorithm for DLP, Index calculus for DLP algorithms: Trial division, Fermat method, Legendre-congruence, Continued fraction method, Pollard Rho method, Elliptic curve method, Quadratic sieve. | | | | 10 |
| **IV** | Lattice based Cryptanalysis. Direct attacks using lattice reduction, Coppersmith's attacks. Attacks on cryptographic hash functions: Birth day paradox, Birthday for paradox for multi collisions, Birthday paradox in two groups, Application of Birthday paradox in Hash functions, Multicollisions attack on hash functions. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **References:**   1. Antoine Joux, "Algorithmic Cryptanalysis", Chapman & Hall/CRC Cryptography and Series, 2009. 2. Song Y Yang, "Number Theory for Computing", Second Edition,SpringerVerlag, 2010. 3. Gregory V. Bard, "Algebraic Cryptanalysis", Springer, 2009. 4. Hffstein, Jeffray, Pipher, Jill and Silverman, "An Introduction to Mathematical Cryptography",Springer, 2010. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6234** | | **DISTRIBUTED AND CLOUD COMPUTING** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To expose the fundamentals of distributed computer systems, explore and acquire a critical understanding about the fundamental concepts of Cloud computing and its technologies. * Enable the learner to develop a firm grounding in the tools and principles of building distributed and cloud applications.  COURSE OUTCOMES: Upon Completion the students will be able to   * Create models for distributed systems. * To explain the basic information storage and retrieval concepts in a storage system. * To understand the emerging area of cloud computing, also learn about the cloud infrastructure services like PAAS, SAAS, IAAS etc.. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | **Systems Modeling, Clustering and Virtualization-** Distributed System Models and Enabling Technologies, Computer Clusters for Scalable Parallel Computing, Virtual Machines and Virtualization of Clusters and Data centers. Foundations:Introduction to Cloud Computing, Migrating into a Cloud, Enriching the ‘Integration as a Service’ Paradigm for the Cloud Era, The Enterprise Cloud Computing Paradigm. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | **Infrastructure as a Service (IAAS) & Platform and Software as a Service (PAAS / SAAS):** Virtual machines provisioning and Migration services, On the Management of Virtual machines for Cloud Infrastructures, Enhancing Cloud Computing Environments using a cluster as a Service, Secure  Distributed Data Storage in Cloud Computing. Aneka, Comet Cloud, T-Systems’, Workflow Engine for Clouds, Understanding Scientific Applications for Cloud Environments. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | **Monitoring, Management and Applications:** An Architecture for Federated Cloud Computing, SLA Management in Cloud Computing, Performance Prediction for HPC on Clouds, Best Practices in Architecting Cloud Applications in the AWS cloud, Building Content Delivery networks using Clouds, Resource Cloud Mashups. | | | | 10 |
| **IV** | **Governance and Case Studies:** Organizational Readiness and Change management in the Cloud age, Data Security in the Cloud, Legal Issues in Cloud computing, Achieving Production Readiness for Cloud Services. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **Reference:**   1. Cloud Computing: Principles and Paradigms by RajkumarBuyya, James Broberg and Andrzej M. Goscinski, Wiley, 2011. 2. Distributed and Cloud Computing, Kai Hwang, GeofferyC.Fox, Jack J.Dongarra, Elsevier, 2012. 3. Cloud Computing : A Practical Approach, Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, Tata McGraw Hill, rp2011. 4. Enterprise Cloud Computing, GautamShroff, Cambridge University Press, 2010. 5. Cloud Computing: Implementation, Management and Security, John W. Rittinghouse, James F.Ransome, CRC Press, rp2012. 6. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, George Reese, O’Reilly, SPD, rp2011. 7. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, Tim Mather, SubraKumaraswamy, ShahedLatif, O’Reilly, SPD, rp2011. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 6236** | | **STORAGE MANAGEMENT AND SECURITY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To enable students to understand, explore and acquire a critical understanding about managing information in storage system and effective security implementation on the corresponding platforms.  COURSE OUTCOMES:  * Introduce the students to various types of storage systems available and understand the importance of storage networking. * To explain the basic information storage and retrieval concepts in a storage system. * To understand the issues those are specific to efficient information retrieval. * To implement security issues while storing and retrieving information. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Introduction, History: computing, networking, storage, Need for storage networking , SAN, NAS, SAN/NAS Convergence, Distributed Storage Systems, Mainframe/proprietary vs. open storage, Storage Industry Organizations and Major Vendors Market, Storage networking strategy (SAN/NAS) Technology | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Storage components, Data organization: File vs. Block, Object; Data store; Searchable models; Storage Devices (including fixed content storage devices), File Systems, Volume Managers, RAID systems, Caches, Prefetching. Error management: Disk Error Management, RAID Error Management, Distributed Systems Error Management | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Large Storage Systems: Google FS/Big Table, Cloud/Web - based systems (Amazon S3), FS+DB convergence, Programming models: Hadoop. Archival Systems: Content addressable storage, Backup: server less, LAN free, LAN Replication issues, Storage Security, Storage Management, Device Management, NAS Management, Virtualization, Virtualization solutions, SAN Management: Storage Provisioning, Storage Migration | | | | 10 |
| **IV** | Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementation in Storage Networking. Managing the Storage Infrastructure, Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in Practice. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **References:**   1. EMC Education Services “Information Storage and Management: Storing, Managing, and Protecting Digital Information” , John Wiley & Sons, 2010 2. John Chirillo, ScottBlaul“ Storage Security: Protecting SANs, NAS and DAS”, Wiley, 2003. 3. David Alexander, Amanda French, Dave Sutton “Information Security Management Principles” BCS, The Chartered Institute, 2008. 4. [Gerald J. Kowalski](http://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor:%22Gerald+J.+Kowalski%22&source=gbs_metadata_r&cad=7), [Mark T. Maybury](http://www.google.co.in/search?tbo=p&tbm=bks&q=inauthor:%22Mark+T.+Maybury%22&source=gbs_metadata_r&cad=7)“ Information Storage and Retrieval Systems: Theory and Implementation, Springer, 2000. 5. Foster Stockwell , “A history of information storage and retrieval” McFarland, 2001. 6. R. Kelly Rainer, Casey G. Cegielski , “Introduction to Information Systems: Enabling and Transforming Business, John Wiley & Sons, 2010. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| COURSE CODE | COURSE NAME | L-T-P-C | YEAR |
| **05CS 6266** | **SEMINAR- I** | 3-1-0-4 | 2015 |
| Each student should present a seminar on any topic related to the core/elective courses offered in the first semester of the M. Tech. Program. The selected topic should be based on the papers published in reputed international journals preferably IEEE/ACM. The selected paper should be approved by the Program Coordinator/Faculty member before presentation. The students should undertake a detailed study on the topic and submit a report at the end of the semester. Marks will be awarded based on the topic, presentation, participation in the seminar and the report. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| COURSE CODE | COURSE NAME | L-T-P-C | YEAR |
| **05CS 6288** | **MINI PROJECT** | 3-1-0-4 | 2015 |
| The mini project is designed to develop practical ability and knowledge in tools/techniques to solve problems related to the industry, academic institutions and computer science research. Students can take up any application level/system level project pertaining to a relevant domain, preferably based on papers from IEEE/ACM journals. Projects can be chosen either from the list provided by the faculty or in the field of interest of the student. The topic should be approved by the Programme Co-ordinator / Faculty member before carrying out the work. For external projects, students should obtain prior permission after submitting the details of the guide and synopsis of the work. The project guide should have a minimum qualification of ME/M.Tech in Computer Science or related fields. At the end of each phase, presentation and demonstration of the project should be conducted, which will be evaluated by a panel of examiners. A detailed project report duly approved by the guide in the prescribed format should be submitted for end semester assessment. Marks will be awarded based on the report and their performance during presentations and demonstrations. Publishing the work in Conference Proceedings/Journals with National/International status with the consent of the guide will carry an additional weightage in the evaluation process. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| COURSE CODE | COURSE NAME | L-T-P-C | YEAR |
| **05CS 6292** | **ETHICAL HACKING AND DIGITAL FORENSIC TOOLS LAB** | 3-1-0-4 | 2015 |
| **Course Objectives:**   * The main objective this practical session is that students will get the exposure to various hacking and forensic tools.   **Course Outcomes:**  By the completion of this laboratory session Student   * Will gain the knowledge to implement various security attacks. * Will get the ideas in various ways to trace an attacker. * Will get the practical exposure to forensic tools.   **Part A: Ethical hacking**   1. Working with Trojans, Backdoors and sniffer for monitoring network communication 2. Denial of Service and Session Hijacking using Tear Drop, DDOS attack. 3. Penetration Testing and justification of penetration testing through risk analysis 4. Password guessing and Password Cracking. 5. Malware – Keylogger, Trojans, Keylogger countermeasures 6. Understanding Data Packet Sniffers 7. Windows Hacking – NT LAN Manager, Secure 1 password recovery 8. Implementing Web Data Extractor and Web site watcher. 9. Email Tracking. 10. Configuring Software and Hardware firewall. 11. Firewalls, Packet Analyzers, Filtering methods.   **Part B: Exposure on Digital Forensic tools**   1. Backup the images file from RAM using Helix3pro tool and show the analysis. 2. Introduction to Santhoku Linux operating system and features extraction. 3. Using Santoku operating system generates the analysis document for any attacked file from by taking backup image from RAM. 4. Using Santoku operating system generates the attacker injected viewing java files. 5. Using Santoku operating system shows how attackers opened various Firefox URL‟s and pdf document JavaScript files and show the analysis. 6. Using Santoku operating System files show how an attacker connected to the various network inodes by the specific process. 7. Using exiftool (-k) generate the any picture hardware and software. 8. Using deft\_6.1 tool recover the attacker browsing data from any computer. 9. Using Courier tool Extract a hacker secret bitmap image hidden data. 10. Using sg (Stegnography) cyber Forensic tool hide a message in a document or any file. 11. Using sg cyber Forensic tool unhide a message in a document or any file. 12. Using Helix3pro tool show how to extract deleted data file from hard disk or usb device. 13. Using Ghostnet tool hide a message into a picture or any image file. 14. Using kgbkey logger tool record or generate an document what a user working on system 15. Using pinpoint metaviewr tool extract a metadata from system or from image file. 16. Using Bulk Extractor tool extract information from windows file system. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 7241** | | **CLOUD SECURITY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To understand the Security aspects of cloud computing which have always been subjected to many criticisms. * Explaining the importance for any security professional to possess an understanding of the cloud architecture and study the methods to secure the same.  COURSE OUTCOMES: Upon completion, the student will be able to   * Understand the fundamentals of cloud computing and its architecture. * Understand the requirements for an application to be deployed in a cloud. * Become knowledgeable in the methods to secure cloud. * Analyze the issues and challenges faced to secure information in a cloud. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | **Cloud computing Fundamentals and Architecture**:- Essential characteristics, Architectural influences, Technological Influences, Operational influences, Outsourcing legal issues, BPO issues, IT server Management . Cloud architecture model – Cloud delivery model, SPI framework, SaaS, PaaS, Iaas, Deployment models –Public, community, Private, Hybrid Cloud. Alternative deployment models. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | **Cloud software security fundamentals**: – Security objective, security service, Cloud security design principles, Secure cloud software requirements, Secure development practice, Approaches of cloud software requirements engineering, Security policy implementation, Secure cloud software testing, penetration testing, Disaster recovery, Cloud for BCP/DCP. | | | | 9 |

|  |  |  |
| --- | --- | --- |
| **INTERNAL TEST 2 (Module 2)** | | |
| **III** | **Cloud Risk Issues and Challenges**:- CIA triad, Privacy and Compliance Risk, PCIDSS, Information privacy and privacy law, Common threats and vulnerabilities, Access control issues, service provider Risk. Security policy Implementation, Computer Security incident response team (CSIRT), Virtualization security Management- virtual threats, VM security recommendations, VM security techniques – hardening, securing VM remote access. | 10 |
| **IV** | **Cloud Security Architecture** :- General issues, Trusted cloud, Secure execution environments and communications, Micro architecture, Identity management, Access control, Autonomic security, protection, self-healing. Cloud life cycle issues – cloud standards, DMTF, ISO, ETSI, OASI, SNIA, OGF, OWASP, Incident response, Internet Engineering Task Force Incident- Handling Guidelines, Computer security and response team, Encryption and key management, VM Architecture, Key Protection, Hardware protection, VM life cycle. | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | |
| **References**   1. Ronald L. Krutz, Russell Dean Vines, Cloud Security, Wiley publication 2010. 2. Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, Inc., 2009. 3. Toby Velte, Anthony Velte, Robert Elsenpeter, Cloud Computing, A Practical Approach, Tata McGraw-Hill Education, 2009. 4. GautamShroff, Enterprise Cloud Computing Technology Architecture Applications, Cambridge University Press, 2010. | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 7243** | | **CYBER LAWS AND SECURITY POLICIES** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * + To enable learner to understand, explore, and acquire a critical understanding cyber law.   + Develop competencies for dealing with frauds and deceptions (confidence tricks, scams) and other cyber crimes for example, child pornography etc.  COURSE OUTCOMES:  * Make Learner Conversant With The Social And Intellectual Property Issues Emerging From Cyberspace. * Explore The Legal And Policy Developments In Various Countries To Regulate Cyberspace; * Develop The Understanding Of Relationship Between Commerce And Cyberspace; * Give Learners In Depth Knowledge Of Information Technology Act And Legal Frame Work Of Right To Privacy, Data Security And Data Protection. * Make Study On Various Case Studies On Real Time Crimes. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | **Introduction to Cyber Law Evolution of Computer Technology:** Emergence of Cyber space. Cyber Jurisprudence, Jurisprudence and law, Doctrinal approach, Consensual approach, Real Approach, Cyber Ethics, Cyber Jurisdiction, Hierarchy of courts, Civil and criminal jurisdictions, Cyberspace-Web space, Web hosting and web Development agreement, Legal and Technological Significance of domain Names, Internet as a tool for global access. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | **Information technology Act** : Overview of IT Act, 2000, Amendments and Limitations of IT Act, Digital Signatures, Cryptographic Algorithm, Public Cryptography, Private Cryptography, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature Certifying Authorities, Cyber Crime and Offences, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | **Cyber law and related Legislation :** Patent Law, Trademark Law, Copyright, Software – Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution , Online Dispute Resolution (ODR). | | | | 10 |
| **IV** | **Electronic Business and legal issues**: Evolution and development in E-commerce, paper vs paper less contracts E-Commerce models- B2B, B2C, E security. **Application area:** Business, taxation, electronic payments, supply chain, EDI, E-markets, Emerging Trends. **Case Study On Cyber Crimes:** Harassment Via E-Mails, Email Spoofing (Online A Method Of Sending E-Mail Using A False Name Or E-Mail Address To Make It Appear That The E-Mail Comes From Somebody Other Than The True Sender, Cyber Pornography (Exm.MMS),Cyber-Stalking. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **References:**   1. K.Kumar,” Cyber Laws: Intellectual property & E Commerce, Security”,1st Edition, Dominant Publisher,2011. 2. Rodney D. Ryder, “ Guide To Cyber Laws”, Second Edition, Wadhwa And Company, New Delhi, 2007. 3. Information Security policy &implementation Issues, NIIT, PHI. 4. Vakul Sharma, "Handbook Of Cyber Laws" Macmillan India Ltd, 2nd Edition,PHI,2003. 5. Justice Yatindra Singh, " Cyber Laws", Universal Law Publishing, 1st Edition,New Delhi, 2003. 6. Sharma, S.R., “Dimensions Of Cyber Crime”, Annual Publications Pvt. Ltd., 1st Edition, 2004. 7. Augastine, Paul T.,” Cyber Crimes And Legal Issues”, Crecent Publishing Corporation, 2007. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 7245** | | **BIOMETRIC SECURITY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To provide students with understanding of biometrics, biometric equipment and standards applied to security.  COURSE OUTCOMES:  * Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems. * Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications. * Be able to work effectively in teams and express their work and ideas orally and in writing. * Identify the sociological and acceptance issues associated with the design and implementation of biometric systems. * Understand various Biometric security issues. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Biometrics- Introduction- benefits of biometrics over traditional authentication systems benefits of biometrics in identification systems-selecting a biometric for a system –Applications – Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Physiological Biometric Technologies: Fingerprints - Technical description –characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan – Technical description - characteristics - weaknesses-deployment - Iris scan - Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern – Technical description – characteristics - strengths – weaknesses –deployment - Hand scan – Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Behavioral Biometric Technologies: Handprint Biometrics - DNA Biometrics - signature and handwriting technology - Technical description – classification - keyboard / keystroke dynamics - Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses- deployment. | | | | 10 |
| **IV** | Multi biometrics: Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan. Case studies on Physiological, Behavioral and multifactor biometrics in identification systems. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **REFERENCES:**   1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, “Biometrics -Identity verification in a network”, Wiley Eastern, 2002. 2. John Chirillo and Scott Blaul,” Implementing Biometric Security”, Wiley Eastern Publications, 2005. 3. John Berger,” Biometrics for Network Security”, Prentice Hall, 2004. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 7251** | | **INTERNET INFORMATION AND APPLICATION SECURITY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To give exposure to various security threats to web applications/ servers and providing security to web servers.  COURSE OUTCOMES: By the completion of this course, Student will   * Understand security concepts, security professional roles, and security resources in the context of systems and security development life cycle * Understand the business need for security, threats, attacks, top ten security vulnerabilities, and secure software development * Understand information security policies, standards and practices, the information security blueprint. * Analyze and describe security requirements for typical web application scenario. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Web application security- Key Problem factors – Core defense mechanisms- Handlinguser access- handling user input- Handling attackers – web spidering – Discovering hidden content. Transmitting data via the client – Hidden form fields – HTTP cookies – URL parameters – Handling client-side data securely – Attacking authentication – design flaws in authentication mechanisms –securing authentication Attacking access controls – Common vulnerabilities – Securing access controls | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Web server Hacking - Source code disclosure – Canonicalization attacks – Denial of service – Web application hacking – Web crawling Database Hacking – Database discovery – Database vulnerabilities | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | SQL Injection - How it happens - Dynamic string building - Insecure Database Configuration - finding SQL injection – Exploiting SQL injection – Common techniques – identifying the database – UNION statements – Preventing SQL injection Platform level defenses- Using run time protection - web application Firewalls – Using ModSecurity - Intercepting filters- Web server filters - application filters – securing the database – Locking down the application data – Locking down the Database server | | | | 10 |
| **IV** | Mod Security - Blocking common attacks – HTTP finger printing – Blocking proxies requests – Cross-site scripting – Cross-site request forgeries – Shell command execution attempts – Null byte attacks – Source code revelation – Directory traversal attacks – Blog spam – Website defacement – Brute force attack – Directory indexing – Detecting the real IP address of an attacker | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **References:**   1. DafyddStuttard, Marcus Pinto, The Web Application Hacker’s Handbook, 2nd   Edition, Wiley Publishing, Inc.   1. Stuart McClure Joel, ScambRay, George Kurtz, Hacking Exposed 7: Network   Security Secrets & Solutions, Seventh Edition, 2012, The McGraw-Hill Companies   1. Justin Clarke, SQL Injection Attacks and Defense, 2009, Syngress Publication Inc. 2. Magnus Mischel , ModSecurity 2.5, Packt Publishing | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 7253** | | **DATABASE SECURITY** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * The main objective of the course is cover topics related to database security and auditing. * The main areas of study is on the key components of information assurance as it relates to database systems – confidentiality, integrity, and availability, and how these components can be managed and measured.  COURSE OUTCOMES: Upon completion, the student will be able to   * Identify access control methods for secure database application development * Analyze vulnerabilities in the database. * Understand common attacks used against database confidentiality and explain how to defend against the attack. * Apply security audit methods to database communication and design secure database schema. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Introduction to databases: database modeling, conceptual database design, overview of SQL and relational algebra, Access control mechanisms in general computing systems: Lampson's access control matrix. Mandatory access control. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Authentication mechanisms in databases, DAC in databases: Griffiths and Wade, MAC mechanisms in databases: SeaView. RBAC in databases. Authentication and password security – Weak authentication options, Implementation options, Strong password selection method, Implement account lockout, Password profile. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | SQL Injection, Auditing in databases, Statistical inference in databases, Private information retrieval viewed as a database access problem. Privacy in data publishing, Virtual Private Databases, Security of outsourced databases. | | | | 10 |
| **IV** | Securing database to database communication – Monitor and limit outbound communication, Protect link usernames and passwords – Secure replication mechanisms. Trojans- Types of DB Trojans, Monitor for changes to run as privileges, Traces and event monitors. Encrypting data- in transit, Encrypt data-at-rest. Database security auditing categories. | | | | 8 |

|  |
| --- |
| **END SEMESTER EXAM (ALL Modules)** |
| **References:**   1. Ron Ben Natan, "Implementing Database Security and Auditing", Elsevier, 2005. 2. Hassan A. Afyouni, "Database Security and Auditing: Protecting Data Integrity and Accessibility", Course Technology, 2005. 3. Michael Gertz and SushilJajodia, "Handbook of Database Security-Applications and Trends", Springer, 2008. 4. Database Security, Cengage Learning; 1 edition (July 12, 2011),AlfredBasta . Melissa Zgola 5. Data warehousing and data mining techniques for cyber security, Springer's By AnoopSingha. 6. Carlos Coronel, Steven A. Morris, Peter Rob, "Database Systems: Design, Implementation, and Management", Cengage Learning, 2011. 7. Vijay Atluri, John Hale, "Research Advances in Database and Information Systems Security", Springer, 2000. 8. PierangelaSamarati, Ravi Sandhu," Database Security X: Status and prospects, Volume 10",Springer, 1997. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COURSE CODE | | COURSE NAME | L-T-P-C | YEAR | |
| **05CS 7255** | | **DEPENDABLE DISTRIBUTED SYSTEMS** | 3-1-0-4 | 2015 | |
| COURSE OBJECTIVES:   * To explore the state-of-the art principles, methods, and techniques for devising adaptive and dependable distributed systems. * Also explains the importance of learning the working of computers in a banking system and creates an awareness of various Biometric systems, their performance and the issues related to the security  COURSE OUTCOMES: Upon completion, the student will be able to   * Understand the Architectural and infrastructural principles for adaptive and dependable distributed systems. * Understand the Approaches to improve the scalability of dependable and adaptive systems. * Understand about the basic banking systems and the bookkeeping practices followed. * Gain a broader knowledge and understand the different Biometric techniques. | | | | | |
| MODULE | COURSE CONTENT (36 hrs) | | | | HRS |
| **I** | Dependability concepts - Faults and Failures – Redundancy – Reliability – Availability – Safety – Security – Timeliness - Fault-classification - Fault-detection and location - Fault containment - Byzantine failures - Fault injection - Fault-tolerant techniques - Performability metrics.  Fault-tolerance in real-time systems - Space-time tradeoff - Fault-tolerant techniques (N-version programming - Recovery block - Imprecise computation; (m,k)- deadline model) – Adaptive fault-tolerance - Fault detection and location in real-time systems. Security Engineering – Protocols - Hardware protection - Cryptography – Introduction – The Random Oracle model – Symmetric Crypto- primitives – modes of operations – Hash functions – Asymmetric crypto primitives. | | | | 9 |
| **INTERNAL TEST 1 (Module 1)** | | | | | |
| **II** | Distributed systems - Concurrency - fault tolerance and failure recovery – Naming. Multilevel Security – Security policy model – The Bell Lapadula security policy model – Examples of Multilevel secure system – Broader implementation of multilevel security system. Multilateral security – Introduction – Comparison of Chinese wall and the BMA model – Inference Control – The residual problem. | | | | 9 |
| **INTERNAL TEST 2 (Module 2)** | | | | | |
| **III** | Banking and bookkeeping – Introduction – How computers systems works – Wholesale payment system – Automatic teller Machine – Monitoring systems – Introduction – Prepayment meters – Taximeters, Tachographs and trunk speed limits. Nuclear Command and control – Introduction – The kennedy memorandum – unconditionally secure authentication codes – shared control security – tamper resistance and PAL – Treaty verification. Security printing and seals – Introduction – History – Security printing – packaging and seals – systemic vulnerability – evaluation methodology. | | | | 10 |
| **IV** | Bio metrics – Introduction – Handwritten signature – face recognition – fingerprints – Iris codes – Voice recognition. Emission Security – Introduction – Technical Surveillance and countermeasures – Passive Attacks – Active Attacks. Electronic and Information warfare – Introduction – Basics – Communication system – Surveillance and target acquisition – IFF system – Directed Energy Weapon – Information Warefare. Telecom Security – Introduction – Phone Breaking – Mobile phones – Network attack and defense - Protecting E-commerce systems- E – policy – Management issues – systems evaluation and assurance. | | | | 8 |
| **END SEMESTER EXAM (ALL Modules)** | | | | | |
| **References:**   1. Ross J Anderson and Ross Anderson, “Security Engineering: A guide to building dependable distributed systems”, Wiley, 2001. 2. David Powell, “A generic fault-Tolerant architecture for Real-Time Dependable Systems”, Springer, 2001. 3. Hassan B Diab and Albert Y. Zomaya, “Dependable computing systems: Paradigm, Performance issues and Applications”, Wiley series on Parallel and Distributed Computing, 2000. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| COURSE CODE | COURSE NAME | L-T-P-C | YEAR |
| **05CS 7267** | **SEMINAR – II** | 3-1-0-4 | 2015 |
| Each student shall present a seminar on any topic related to their miniproject or thesis work of the M. Tech. Program. The selected topic should be based on the papers published in reputed international journals preferably IEEE/ACM. They should get the paper approved by the Program Co-ordinator/Faculty member in charge of the seminar and shall present it in the class. Every student shall participate in the seminar. The students should undertake a detailed study on the topic and submit a report at the end of the semester. Marks will be awarded based on the topic, presentation, participation in the seminar and the report submitted. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| COURSE CODE | COURSE NAME | L-T-P-C | YEAR |
| **05CS 7287** | **PROJECT PHASE I** | 3-1-0-4 | 2015 |
| In Master’s thesis Phase-I, the students are expected to select an emerging research area in Computer Science or related fields, after conducting a detailed literature survey. A detailed design should be prepared based on the study, comparison, analysis and review of the research work and recent developments in the area. Recent National/International Conference Proceedings/Journals, preferably IEEE/ACM, should be referred for the selection of the topic.  Students should submit a copy of Phase-I thesis report covering the content discussed above and highlighting the features of work to be carried out in Phase-II of the thesis. Emphasis should be given for literature survey, scope and design of the proposed work along with the details of the preliminary work carried out on the thesis topic.  The candidate should present the current status of the thesis work and the assessment will be made on the basis of the work and the presentation, by a panel of examiners. This panel can be a committee headed by the head of the department with two other faculty members in the area of the project, of which one shall be the project supervisor .If the project is done outside the college, the external supervisor associated with the student will also be a member of the committee. The examiners should give their suggestions in writing to the students so that it should be incorporated in the Phase–II of the thesis. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| COURSE CODE | COURSE NAME | L-T-P-C | YEAR |
| **05CS 7288** | **PROJECT PHASE II** | 3-1-0-4 | 2015 |
| In the fourth semester, the thesis work approved and evaluated in third semester should be continued and carried out to successful completion . A detailed thesis report should be submitted at the end of phase II. The work carried out should lead to a publication in a National / International Conference or Journal. The papers received acceptance before the M.Tech evaluation will carry specific weightage.  Final evaluation of the project will be taken up only on completion of the project. This shall be done by a committee constituted by the principal of the college for the purpose. The concerned head of the department shall be the chairman of this committee. It shall have two senior faculty members from the same department, project supervisor and external supervisor of the student, if any and an external expert either from an academic /R&D organization or from industry as members. | | | |