M. TECH - CYBER SECURITY

TIFAC-Centre of Relevance and Excellence (CORE) in Cyber Security

Cyber security is a very fast moving field. A program in security that aims to be on the forefront has to necessarily have a companion-advanced program that has a good balance between theoretical and practical aspects, analytical methods and system architectures, academic ideas and industry practices.

The Centre for Cyber Security was identified by TIFAC (Department of Science and Technology, Govt. of India) as a CORE in Cyber Security in September 2005. The TIFAC CORE gives significant thrust to the frontier areas of Cyber Security, including technology, practice, management, and policy issues. Research areas of the TIFAC CORE are organized into four broad categories, namely: Enterprise Wide Security, Data Center Security, Language-Based Security, and Hardware and Embedded Systems Security. These categories represent four horizontal layers of security in a typical information system /network that a practitioner would normally encounter in today's industrial settings and corporate environments. CORE also focuses on theory and practice of authentication, authorization, and access control techniques.

This M. Tech program provides a good blend of theory and industrial practice; necessary theoretical background, insight into general and technical aspects of Cyber Security, analytical methods and management practices in the field of Cyber Security are the areas receiving detailed attention. It aims at moulding the student into an Information Security professional. Practicing industry professionals and enterprise experts with little or no knowledge in Cyber Security too can benefit from this program.

CURRICULUM

First Semester

Course Code	Type	Course	L T P	Cr
MA 610	FC	Mathematical Foundations for Cyber Security	4 0 0	4
CY 602	FC	Design and Analysis of Algorithms	3 0 1	4
CY 611	SC	Internetworking- Protocols and Security	3 0 1	4
CY 612	SC	Cryptography	3 0 1	4
CY 613	SC	Concepts in System Security	3 0 1	4
HU 601	HU	Cultural Education *		P/F
			Credits	**20**

* Non-Credit Course

Second Semester

Course Code	Type	Course	L T P	Cr
CY 614	SC	Cryptographic Protocols and Standards	3 0 1	4
CY 603	FC	Pattern Recognition and Machine Learning	2 0 1	3
CY 604	FC	Secure Coding	3 0 1	4
	E	Elective I	2 0 1	3
	E	Elective II	2 0 1	3
EN 600	HU	Technical Writing*		P/F
			Credits	**17**

* Non-Credit Course

Third Semester

Course Code	Type	Course	L T P	Cr
	E	Elective III	3 0 1	4
	E	Elective IV	2 0 1	3
CY 799	P	Dissertation		10
			Credits	**17**

Fourth Semester

Course Code	Type	Course	L T P	Cr
CY 799	P	Dissertation		12
			Credits	**12**

Total Credits: 66

List of Courses

Foundation Core

Course Code	Course	L T P	Cr
MA 610	Mathematical Foundations for Cyber Security	4 0 0	4
CY 602	Design and Analysis of Algorithms	3 0 1	4
CY 603	Pattern Recognition and Machine Learning	2 0 1	3
CY 604	Secure Coding	3 0 1	4

Subject Core

Course Code	Course	L T P	Cr
CY 611	Internetworking - Protocols and Security	3 0 1	4
CY 612	Cryptography	3 0 1	4
CY 613	Concepts in System Security	3 0 1	4
CY 614	Cryptographic Protocols and Standards	3 0 1	4

Electives

Course Code	Course	L T P	Cr
	Elective I		
CY 701	Security in Mobile Networks	2 0 1	3
CY 702	Language-Based Security	2 0 1	3
CY 703	Network Security	2 0 1	3
	Elective II		
CY 704	Information Hiding	2 0 1	3
CY 705	Information Security and Risk Management	3 0 0	3
CY 706	HDL and Cryptographic Applications	2 0 1	3
	Elective III		
CY 707	Coding and Information Theory	3 0 1	4
CY 708	Security in Cloud Computing	3 0 1	4
	Elective IV		
CY 709	Formal Methods for Security	2 0 1	3
CY 710	Secure System Engineering	2 0 1	3
CY 711	Cyber Forensics	2 0 1	3

Project

Course Code	Courses	L T P	Cr
CY 799	Dissertation		22

MA 610 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY 4-0-0-4

Elementary Number Theory – Divisibility , Prime numbers; Algorithms for primality testing and Integer Factorisation; Arithmetic functions, Congruence, Quadratic Residues, Jacobians, Primitive roots.Algebraic Structures - Groups, Rings and Fields; Polynomials over Finite Field - Order of Polynomials, Minimal polynomials, Primitive polynomials. Extension Fields. Structure of Finite Fields, Algorithms for Discrete Logarithm, Arithmetic of Elliptic Curves, Bilinear maps. Matrices and Gaussian elimination, Determinants, Vector Spaces - Basis and Dimension, Eigen Values and Eigen vectors, Singular Value Decomposition, Solving nonlinear system of equations - XL algorithm and Grobner basis techniques. Normed Linear Space, Inner Product Space, Hilbert Space.Discrete and Continuous random variables, Expectation and Variance, Binomial, Poisson and Normal distributions, Cumulative distribution function, Joint probability distribution of functions of random variables, Expectations of sums of random variables, Covariance and variance of sums, Conditional expectation, Bayes' theorem.

TEXT BOOKS/REFERENCES:

1. R. Lidl and H. Niederreiter, *Finite Fields,* Second Edition, Cambridge University Press, 1997.
2. G.bStrang, *Introduction to Linear Algebra* , Fourth Edition, Wellesley-Cambridge Press, 2009.
3. S. M. Ross, *A First Course in Probability* , Eighth Edition, Pearson Education, 2009.
4. S.Y. Yan, *Number Theory for Computing* , Second Edition, Springer, Berlin, 2002.
5. A. Joux, *Algorithmic Cryptanalysis* , Chapman & Hall/CRC Cryptography and Series, 2009.

CY 602 DESIGN AND ANALYSIS OF ALGORITHMS 3-0-1-4

Basic techniques for designing and analyzing algorithms, dynamic programming, divide and conquer, balancing. Upper and lower bounds on time and space costs, worst case and expected cost measures, Disjoint set, graph algorithms, Persistent data structures, Polynomial complexity classes - P, NP, and co-NP; intractable problems, Randomized data structure, Search Trees and Skip Lists, Online Algorithms - *k*-Server Problem, Stable Marriage Algorithm. Approximation Algorithms - Greedy Approximation Algorithms, Weakly Polynomial-time Algorithms, 3/2-approximation for TSP, ILP relaxations. Fixed Parameter Algorithms - Parameterized Complexity, Kernelization, Treewidth. Parallel Algorithms – Pointer Jumping and Parallel prefix. Amortized analysis, Fast Multiplication Algorithms, Number Theoretic algorithms, Polynomial and Matrix calculations, Pseudo polynomial time algorithms, Random number generators. Heap - Binomial, Fibonacci. Randomized Hashing-Universal Hashing, Perfect Hashing.

TEXT BOOKS/REFERENCES:

1. T. Cormen, C. Leiserson, R. Rivest and C. Stein, *Introduction to Algorithms* , Third Edition, McGraw-Hill, 2009.
2. R. Motwani and P. Raghavan, *Randomized Algorithms* , Cambridge University Press, 1995.

3. J. J. McConnell, *Analysis of Algorithms*: *An Active Learning Approach*, Jones & Bartlett Publishers, 2001.
4. D. E. Knuth, *Art of Computer Programming, Volume 3, Sorting and Searching*, Second Edition, Addison-Wesley Professional, 1998.
5. S. Dasgupta, C. H. Papadimitriou and U. V. Vazirani, *Algorithms*, McGraw-Hill, 2008.

CY 603 PATTERN RECOGNITION AND MACHINE LEARNING 2-0-1-3

Gaussian Bayes classifiers, Bayesian networks, Naive Bayesian classifiers. Decision trees, information gain, Regression algorithms, Gaussian mixture models, *k*-means and hierarchical clustering, Hidden Markov models, Support Vector Machines, Reinforcement learning - Q-learning, Value function approximation. Minimum error rate classification, ROC curves, Discriminate functions and decision surface, Linearly separable case, Perception criterion function, Component analysis and discriminants, Expectation Maximization. Nonparametric Techniques - Parzen windows, Probabilistic Neural Networks, Metrics and Nearest Neighbor Classification, Multilayer Neural Networks, Back propagation as feature mapping, Stochastic search. Evolutionary Methods - Genetic Algorithms, Genetic programming. Ensembles - Bagging, Boosting, Stacking. Scalable Learning and Parallelization - Page Rank, Keyword Searching, Recursive queries, Iterative processing, Collaborative Filtering, Map Reduce algorithms, Hadoop.

TEXT BOOKS/REFERENCES:

1. T.R.Tibshirani and J. H. Friedman, *The Elements of Statistical Learning: Data Mining Inference and Prediction,* Second Edition, Springer, 2009.
2. T. Mitchell, *Machine Learning,* McGraw-Hill, New York, 1997.
3. J. Han and M. Kamber, *Data Mining: Concepts and Techniques,* Morgan Kaufmann, 2001.
4. R. O. Duda, P. E. Hart and D. G. Stork, *Pattern Classification ,* Second Edition, John Wiley & Sons Inc., 2003.
5. C. M. Bishop, *Pattern Recognition and Machine Learning* ,Springer,2006.

CY 604 SECURE CODING 3-0-1-4

Application Security and Secure Programming concepts. Secure Coding in C and C++ - Stack overflow, Strings, Integers, Arrays, File I/O, Race conditions, Signal handling. Recommended Practice - Secure Coding in Java and Web Applications. Anatomy of attacks - Data Breach, Threat modeling, Cross Site Scripting (XSS) vulnerabilities, Injection flaws (SQL, process, path,etc), Buffer overflows, Resource leaks and resource lifetime management, Threat modeling and Security design review, Software Assurance and Testing-Software Assurance overview, Testing threat categories, Assessing Risk, Secure Testing Methodologies - Attacking Dependencies, Attacking through the User Interface, Attacking Design, Attacking Implementation, Software engineering practices for development of high assurance code, Model Checking, Static Analysis techniques for analyzing software.

TEXTBOOKS / REFERENCES:

1. R. C. Seaford, *Secure Coding in C and C++,* Addison-Wesley Professional, 2005.
2. J. A. Whittaker and H. H. Thompson, *How to Break Software Security,* Addison Wesley, 2003.
3. J.C. Mitchell and Krzysztof Apt, *Concepts in Programming Languages,* Cambridge University Press, 2001.

CY 611 INTERNETWORKING - PROTOCOLS AND SECURITY 3-0-1-4

Network services and applications: DNS, HTTP, SMTP, peer-to-peer systems, Network transport architectures, TCP, UDP, ICMP, TCP congestion control, Routing and forwarding, intra-domain and inter-domain routing algorithms, Link layers and local area networks: Ethernet, Wi-Fi, and mobility, Multimedia communications and quality of service, Network measurement, inference, and management, Network experimentation and performance analysis. Security: ARP attacks and ARP poisoning, DNS attacks, SYN flood attacks and its mitigation, UDP ping-pong and fraggle attacks, TCP port scanning and reflection attacks.

TEXT BOOKS/REFERENCES:

1. J. F. Kurose and K. W. Ross, *Computer Networking - A Top Down Approach,* Fifth Edition, Addison-Wesley, 2010.
2. L. Peterson and B. Davie, *Computer Networks: A Systems Approach,* Fifth Edition, Elsevier Inc., 2011.
3. W. R. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols,* Addison-Wesley, 1994.

CY 612 CRYPTOGRAPHY 3-0-1-4

One way and trapdoor functions: Strong, weak and non uniform One-way functions, Trapdoor functions, Discrete Logarithm functions, RSA functions, squaring trapdoor function by Rabin, Hard core predicate of one way function: set of trapdoor predicates based on quadratic residue and RSA assumption. Pseudo random bit generators & Pseudo random functions: provably secure pseudorandom generators, existence of pseudo random generators; pseudo random functions and permutations (PRFs and PRPs), PRP under chosen plaintext attack and chosen ciphertext attack, usage of PRFs and PRPs in shared random function model and in modeling block ciphers. Construction of PRF, applications of PRFs: cryptographically strong hashing, private-key encryption Symmetric encryption schemes: Block ciphers and modes of operation, stream ciphers, information theoretic security, indistinguishability under chosen plaintext and chosen ciphertext attack. Public-key encryption: RSA, Rabin, Knapsack cryptosystems and ECC; polynomial indistinguishability, semantic security; probabilistic public key encryption. Message authentication & Digital signatures: XOR schemes, designing MACs using PRFs, CBC MAC and its security, universal hash based MACs, MACing with Cryptographic hash functions, Authenticated encryption; trapdoor function model, Generic signature schemes, RSA, ElGamal and Rabin's signature schemes, probabilistic signatures, signature scheme based on Claw-free trapdoor permutations, blind signatures, threshold signature schemes.

TEXT BOOKS/REFERENCES:

1. A. J. Menezes, P.C.V.Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography ,* CRC Press, 1996.

2. O. Goldreich, *Foundations of Cryptography: Volume 1,* Cambridge University Press, 2001.
3. O.Goldreich, *Foundations of Cryptography: Volume 2, Basic Applications,* Cambridge University Press, 2004.
4. J. Katz and Y. Lindell, *Introduction to Modern Cryptography,* Chapman & Hall/CRC, 2007.
5. J. H . Silverman, *The Arithmetic of Elliptic Curves* , Vol. 106. Dordrecht: Springer, 2009.

CY 613 CONCEPTS IN SYSTEM SECURITY 3-0-1-4

Transaction recovery and concurrency control in database systems.Access control mechanisms in general computing systems- Lampson's access control matrix. Mandatory access control, Authentication mechanisms in databases, DAC in databases- Griffiths and Wade, MAC mechanisms in databases-SeaView. RBAC in databases, Auditing in databases, Statistical inferencing in databases, Private information retrieval viewed as a database access problem. Privacy in data publishing, Virtual Private Databases, Hadoop security. Security and protection in operating systems - access control, auditing, trusted computing base with reference to Multics and the commercial Operating Systems such as UNIX/Linux, MacOS and Windows 8. Malware analysis and protection - rootkits and their defenses, polymorphic malware, malware capture and analysis such as honeypots.Virtualization techniques for security.Mobile Operating Systems security especially in Android and iOS.

TEXT BOOKS/REFERENCES:

1. M. Gertz and S. Jajodia, *Handbook of Database Security—Applications and Trends* , Springer, 2008.
2. C. J. Date, *An Introduction to Database Systems* , Pearson, Part IV, 2004.
3. T. Jaeger, *Operating System Security,* Volume 1 of Synthesis Lectures on Information Security, Privacy and Trust, Morgan & Claypool Publishers,2008.
4. W. Mauerer, *Professional Linux Kernel Architecture,* John Wiley and Sons, New York, , 2008.
5. M. J. Jipping, *Smartphone Operating System Concepts With Symbian OS* , John Wiley and Sons Ltd., 2007.

CY 614 CRYPTOGRAPHIC PROTOCOLS AND STANDARDS 3-0-1-4

Goals for authentication and Key Establishment, Formal Verification of Protocols, Complexity Theoretic Proofs of Security. Protocols Using Shared Key Cryptography – Entity Authentication Protocols, Server-Less Key Establishment, Server-Based Key Establishment, Zero Knowledge interactive proofs. 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. Protocols not based on Diffie Hellman. 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, Secret Sharing based Protocols. Pairing based cryptographic protocol- ID based encryption schemes, Boneh and Franklin's Scheme, Shamir's encryption and signature schemes, Okamoto's scheme, Gunther's scheme, Girault's scheme. Homomorphic encryption.

TEXT BOOKS/REFERENCES:

1. C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment,* Springer, 2010.
2. A. Das and C.E. Veni Madhavan, *Public-key Cryptography, Theory and Practice ,* Pearson Education, 2009.
3. L. Dong and K. Chen, *Cryptographic Protocol: Security Analysis Based on Trusted Freshness* , Springer, 2012.
4. J. Pieprzyk, T. Hardjono and J. Seberry, *Fundamentals of Computer Security*, Springer, 2003.

EN 600 TECHNICAL WRITING P/F

Technical terms- Definitions- extended definitions- grammar checks- error detection- punctuation- spelling and number rules - tone and style- pre-writing techniques - Online and offline library resources- citing references – plagiarism - Graphical representation - documentation styles- instruction manuals- information brochures- research papers, proposals – reports (dissertation, project reports etc.) - Oral presentations.

TEXTBOOKS/REFERENCES:

1. H. L. Hirish , *Essential Communication Strategies for Scientists, Engineers and Technology Professionals*. Second Edition. New York: IEEE press, 2002.
2. P. V. Anderson, *Technical Communication: A Reader-Centred Approach*, VI Edition, Cengage Learning India Pvt. Ltd., New Delhi, Reprint 2010.
3. W. Strunk Jr. and E. B.White, *The Elements of Style*, New York. Alliyan & Bacon, 1999.

CY 701 SECURITY IN MOBILE NETWORKS 2-0-1-3

Transmission Fundamentals, Antennas and Wave Propagation. Cellular Wireless networks, Third Generation Systems, 4G Long Term Evolution, Signal Encoding Techniques , Spread Spectrum, Coding and Error Control, Multiple Access in Wireless Systems. Satellite Networks, Wireless System Operations and Standards, Wi-Max and 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. Threats to Wireless networks, ESM, ECM and ECCM, Proliferation of devices and technologies, Practical aspects, Wireless availability, Privacy Challenges, Risks – Denial of Service, Insertion Attacks, Interception and monitoring wireless traffic, Misconfiguration, Wireless Attacks, Surveillance, War Driving, Client-to-Client Hacking, Rogue Access Points, Jamming and Denial of Service. Authentication**,** Encryption/Decryption in GSM, Securing the WLAN, WEP, RC4 , 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.

TEXT BOOKS/REFERENCES:

1. K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks,* Prentice –Hall, 2006.
2. C. Peikari and S. Fogie, *Maximum Wireless Security,* Sams, 2002.
3. H. Imai, M. G. Rahman and K.Kobara, *Wireless Communications Security,* Universal Personal Communications of Artech House, 2006.
4. W. Stallings , *Wireless Communications and Networks* , Second Edition, Pearson Education Ltd, 2009.
5. J. Edney and W. A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i* , Addison-Wesley Professional, 2003.

CY 702 LANGUAGE-BASED SECURITY 2-0-1-3

Types of programming language, Functional programming, Lists and Hoare logic, Constructive logic and type theory, Inductive definitions and proof techniques for informal and formal proof, The Coq proof assistant. Denotational Semantics and Operational semantics, Semantics of simple imperative language. Type systems - Introduction to the lambda-calculus, Formalizing the lambda-calculus, Simply typed lambda calculus and type checking, Simple extensions, derived forms, Type safety. Object oriented Programming-Semantics Subtyping, Metatheory of Subtyping, Recursive types, Metatheory of recursive types, Polymorphism, ADTs, Dependently typed programming.

TEXT BOOKS/REFERENCES:

1. B.C. Pierce, C. Casinghino, M. Greenberg, V. Sjöberg and B. Yorgey, *Software Foundations,* Online book, University of Pennsylvania 2010.
2. B. C. Pierce, *Types and Programming Languages,* The MIT Press, 2002.

CY 703 NETWORK SECURITY 2-0-1-3

Techniques for network intrusion detection: signature-based and anomaly-based detection, Snort, Firewalls-packet filters and stateful firewalls, application-aware firewalls, proxies, NAT, Virtual Private Networks-tunneling, IPSEC VPNs, L2TP, PPP, PPTP, denial of service (DoS) and distributed denial-of-service (DDoS) attacks, detection and reaction, worm and virus propagation, tracing the source of attacks, traffic analysis, techniques for hiding the source or destination of network traffic, secure routing protocols, protocol scrubbing and advanced techniques for reacting to network attacks. HTTP authentication, SSL/TLS, Kerberos, secure DNS, Email spam and its solutions, broadcast security, secure multicasting.

TEXT BOOKS/REFERENCES:

1. E.Rescorla, *SSL and TLS: Designing and Building Secure Systems,* Addison-Wesley Professional, 2000.
2. T. H. Ptacek and T. N. Newsham, *Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection,* Secure Networks, Inc., 1998.
3. P. Paul, *The Practical Intrusion Detection Handbook* , Third Edition, Prentice-Hall, Englewood Cliffs, 2001.
4. C. Kaufman, R. Perlman and M. Speciner, *Network Security: PRIVATE Communication in a PUBLIC World,* Second Edition, Prentice Hall PTR, 2002.

5. W. Stallings, *Network Security Essentials: Applications and Standards,* Fourth Edition, Pearson Prentice Hall, 2010.

CY 704 INFORMATION HIDING 2-0-1-3

Digitized image and its properties, Noise in images, Data structures for image analysis - Traditional and Hierarchical image data structures. Level of image data representation, Image pre-processing, Pixel brightness transformations, Geometric transformations, Image smoothing, Edge detectors, Zero crossings of the second derivative, Canny edge detection, Edges in multi-spectral images, Adaptive neighbourhood pre-processing, Image restoration. Transforms – Discrete Cosine Transform, Mellin, Fourier Transform, DWT. Multimedia systems – Video and Audio. Compression techniques, Digital Media, Encoding – JPEG , DCT, MPEG, MPEG system layer. Multimedia Standards, Editing-Compressed Domain Editing. Models of Watermarking – Communication Based Models, Geometric Models of Watermarking. Modeling Watermark Detection by Correlation, Watermarking with Side Information, Practical Dirty-Paper Codes, Robust Watermarking. Steganography, Practical Steganography Methods, Minimizing the Embedding Impact. Steganalysis: Statistical and Feature based Steganalysis.

TEXT BOOKS/REFERENCES:

1. I. J. Cox, M. L. Miller, J. A. Bloom , J. Fridrich and T.Kalker, *Digital Watermarking and Steganography ,* Second Edition, The Morgan Kaufmann Series in Multimedia Information and Systems, 2002.
2. D. A. Milovanovic, Z. S. Bojkovic and K. R. Rao, *Multimedia Communication System: Techniques, Standards, and Networks,* Prentice Hall, 2002.
3. K. R. Castleman, *Digital Image Processing ,* Prentice Hall, 1996.
4. R. C. Gonzalez and R. E. Woods, *Digital Image Processing ,* Third Edition, Prentice Hall, 2011.
5. J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications ,* First Edition. Cambridge University Press, 2010.

CY 705 INFORMATION SECURITY AND RISK MANAGEMENT 3-0-0-3

Information Risk Management ,Relationships among different security components - threat agent, vulnerability, risk, asset, exposure and safeguards. Governance models such as COSO and CobiT, ISO 27000 series of standards for setting up security programs, risk analysis and management, policies, standards, baselines, guidelines and procedures as applied to Security Management program, Information strategy objectives, 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. Business Continuity and Disaster Recovery- Business Continuity Management 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.

TEXT BOOKS / REFERENCES:

1. A. Calder and S. G. Watkins, *Information Security Risk Management for ISO27001 /ISO27002,* IT Governance Ltd, 2010.
2. S. Snedaker, *Business Continuity and Disaster Recovery Planning for IT Professionals ,* Elsevier Science & Technology Books, 2007.
3. H. F. Tipton and M. Krause, *Information Security Management Handbook,* Volume 1, Sixth Edition, Auerbach Publications, 2003.

CY 706 HDL AND CRYPTOGRAPHIC APPLICATIONS 2-0-1-3

Introduction to Verilog: structure, constructs, and conventions; Modeling at Gate level, Data flow level, Behavior level, and switch level. Design, simulation, and synthesis of digital circuits, modules, and systems. Functions, tasks, User defined primitives, Compiler directives. Queues, PLAs, and FSMs. FPGAs – blocks inside, their features and use. IDE and its use. FPGA based design realizations. Design of finite field arithmetic operations. Representative designs with AES, ECC and Hash Algorithms.

TEXT BOOKS/REFERENCES:

1. T. R. Padmanabhan and B. Bala Tripura Sundari, *Design through VERILOG HDL,* IEEE Press, John Wiley, 2003.
2. M. C. Cileti, *Advanced Digital Design with VERILOG HDL,* Prentice Hall, 2002.
3. S. Brown and Z. Vranesic, *Fundamentals of Digital Logic with VERILOG Design,* Tata McGraw Hill, 2002.
4. F. Riodrigues-Henriquez, N. Saqib, A. Diaz-Perez and C. Koc, *Cryptographic Algorithms on Reconfigurable Hardware,* Springer, 2007.
5. C. K. Koc , *Cryptographic Engineering ,* Springer, 2008.

CY 707 CODING AND INFORMATION THEORY 3-0-1-4

Information, Entropy, Source coding- Huffman, Lempel-Ziv and arithmetic codes, Image Coding – Rate distortion theory, Optimum Quantizer Design, JPEG Standard for lossless and lossy compression; Discrete memoryless channel, Mutual information, Linear block codes, Error detection and correction, Hamming codes, Reed Muller codes, Golay codes, Cyclic codes, Binary BCH codes, Reed Solomon codes, Decoding algorithms, Trellis representation of codes, Convolution codes and its applications, Viterbi algorithm and decoding, Concatenated codes - single and multilevel codes, decoding.

TEXT BOOKS/REFERENCES:

1. S. Lin and D. J. Costello, *Error Control Coding – Fundamentals and Applications,* Second Edition, Pearson Education Inc., NJ., USA, 2004
2. S. Lin and D. J. Costello, *Error Control Coding,* Second Edition, Prentice Hall, 1983.
3. R. 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.

CY 708 SECURITY IN CLOUD COMPUTING 3-0-1-4

The historical path to cloud computing. The trade-offs and differences among cloud offerings such as SaaS, PaaS and IaaS. Key-value stores and their trade-offs against transactional SQL stores. Implementations of classic key-value stores such as BigTable & Dynamo. The use of consensus in distributed systems and its implementation in Paxos and Raft. MapReduce and other parallel processing frameworks. Server and network virtualization. Security in the cloud---infrastructure and data. Significant hands-on project experience with a chosen cloud computing framework.

TEXT BOOKS/REFERENCES:

1. T. Mather, S. Kumaraswamy, S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly Series, 2009.
2. T. Erl, R. Puttini, Z. Mahmood, *Cloud Computing: Concepts, Technology & Architecture,* Prentice Hall, 2013.
3. The Google file system. In Proceedings of the nineteenth ACM symposium on Operating systems principles (SOSP '03). ACM, New York, NY, USA, 29-43.
4. MapReduce: simplified data processing on large clusters. Commun. ACM 51, 1, 107-113, 2008.
5. Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW '09). ACM, New York, NY, USA, 85-90, 2009.

CY 709 FORMAL METHODS FOR SECURITY 2-0-1-3

Formal Methods – propositional and predicate logic, and theorem-proving; fixed-points and their role in program analysis and model-checking; verification of sequential programs using weakest preconditions and inductive methods, and verification concurrent and reactive programs/systems using model-checking and propositional temporal logic (CTL and LTL); application of static and dynamic program analysis and model-checking for detecting common security vulnerabilities in programs and communication protocols; information flow and taint analysis for security of web applications; pi-calculus for formal modelling of mobile systems and their security. SPIN, PVS, and Isabelle tools.

TEXT BOOKS/REFERENCES:

1. M. Ruth and M. Ryan, *Logic in Computer Science - Modelling and Reasoning about Systems*, Cambridge University Press, 2004 .
2. E. C. Clarke, et al, *Model Checking*, MIT Press, 1999.
3. G. Bella, *Formal Correctness of Security Protocols*, Springer, 2009.
4. S. Jha, et al, *Analysis Techniques for Information Security*, Morgan and Claypool Publishers, 2010.
5. J. W. Lloyd and J.Lloyd, *Logic and Learning: Knowledge Representation, Computation and Learning in Higher-order Logic*, Springer Berlin Heidelberg, 2003.

CY 710 SECURE SYSTEMS ENGINEERING 2-0-1-3

Information flow and vulnerability model to build security into life cycle phase of software (and hardware) components. Threat and vulnerability analysis into architecture and design process, access-controlled and clean environment to build software, target environment hardening and secure application deployment. Introduction to hardware security – Physical and side channel attacks and its countermeasures, tamper resistance. Secure operational processes - roles and access policies for development. Practical aspects of cryptography - usable crypto algorithms and key life cycle management, mobile computing. Balancing security and usability – developing authentication mechanisms, secure browsing, social media and data sharing. Counter-measures for possible social engineering attacks in design. Secure interactive design. Usable PKI. Privacy issues in Human Computer Interaction. Security Economics: Risk assessment and selection of appropriate countermeasures with cost-benefit trade-offs.

TEXT BOOKS/REFERENCES:

1. M. Tehranipoor, C. Wang, *Introduction to Hardware Security and Trust* , Springer, 2011
2. S. Garfinkel and L.F. Cranor, *Security and Usability: Designing Secure Systems That People Can Use* , O'Reilly, 2008.
3. C. W. Axelrod, *Engineering Safe and Secure Software Systems*, Artech House, 2013.
4. Selected Papers and Class notes

CY 711 CYBER FORENSICS 2-0-1-3

Framework for Digital Forensic Evidence Collection and Processing, Fundamentals of Host Forensics for Microsoft Windows - Kernel and Device driver architecture, registry, auditing and security architecture. File system handling - Reconstruction of files and directory structures on the FAT and NTFS . Fundamentals of Host Forensics for UNIX derivatives - Linux operating system, Kernel and Device drives architecture, Security and audit mechanisms, file system and pseudo file systems, the reconstruction of file and directory structures using UFS and Ext2/3fs as exemplars. Forensic Analysis of Database Systems, Database Tampering, Forensic analysis of Database Components, table storage, transaction log, indexes, Forensic recovery for table storage. Network Forensics, investigating logs, network traffic and web attacks, Mobile Device and Wireless Forensics, Anti-Forensics, Steganography and Image file Forensics, Email investigation, Investigating Copiers, IVR, Video Surveillance, RFID and Vehicular tracking (GPS) devices, Case studies and Tools.

TEXT BOOKS/REFERENCES:

1. E. P. Dorothy, *Real Digital Forensics for Handheld Devices* , Auerback Publications, 2013.
2. J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*, Syngress Publishing, 2012.
3. E. Casey, *Handbook of Digital Forensics and Investigation*, Academic Press, 2010
4. C. H. Malin, E. Casey and J. M. Aquilina, *Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides*, Syngress, 2012
5. J. Wiles and A.Reyes, *The Best Damn Cybercrime and Digital Forensics Book Period*, Syngress, 2007.