M.TECH. CYBER SECURITY SYSTEMS AND NETWORKS

Amrita Center for Cyber Security Systems and Networks

This M.Tech programme aims to train the students in the cyber security discipline through a well designed combination of courseware and it s application on real-world scenarios. The programme has a strong emphasis on foundational course such mathematics for security application, advanced algorithms, networks etc., in addition to diverse subject core areas such as cryptography, operating systems and security, cloud security, security of cyber physical systems etc.

Students will be exposed to real-world problems, open-end problems and simulated real-life scenarios with active guidance from domain experts in this field. The programme will help the students to:

1. Comprehend the various security threats and vulnerabilities of the cyber world keeping in line with industrial trends.
2. Scale up to the demand from multiple industrial sectors on the cyber world to promote effective methods, practices and tools to counter the cyber crimes.
3. To be able to architect, design and implement fool-proof product line in the field of cyber security.

Ultimately this programme will yield next generation cyber security leaders who can be successfully employed in various sectors of industries, business firms, Government departments, financial bodies, educational institutions, etc, and these sectors generate huge demand for well-trained, professional people to be employed on cyber security front and they are always on the look-out for professionally trained people in the area of cyber security. |

CURRICULUM

First Semester

Course Code	Type	Course	L T P	Cr
16MA609	FC	Mathematical Foundations for Cyber Security Systems	4 0 0	4
16SN611	SC	Operating System and Security	3 0 1	4
16CS602	FC	Advanced Algorithms and Analysis	3 0 1	4
16SN601	FC	Advanced Computer Networks and Internet Architectures	3 0 1	4
16SN612	SC	Database and Web Application Security	3 0 0	3
16SN613	SC	Programming Concepts: Practical	0 0 1	1
16HU601	HU	Cultural Education*		P/F
			Credits	20

*Non-credit Course

Second Semester

Course Code	Type	Course	L T P	Cr
16SN614	SC	Principles of Cryptography	3 0 0	3
16SN602	FC	Cyber Forensics and Incident Response	3 0 1	4
16SN615	SC	Systems and Network Security - 1	3 0 1	4
16SN616	SC	Wireless Security	3-0-0	3
	E	Elective–I	3 0 0	3
16EN600	HU	Technical Writing*		P/F
			Credits	17

*Non-credit course

Third Semester

Course Code	Type	Course	L T P	Cr
	E	Elective –II	3-0-0	3
	E	Elective –III	3 0 0	3
16SN796	P	Live-in-Labs		P/F
16SN798	P	Dissertation		10
			Credits	16

Fourth Semester

Course Code	**Type**	**Course**	**L T P**	**Cr**
16SN799	P	Dissertation		12
			Credits	**12**

Total Credits: 65

List of Courses

Foundation Core

Course Code	Type	Course	L T P	Cr
16MA609	FC	Mathematical Foundations for Cyber Security Systems	4 0 0	4
16CS602	FC	Advanced Algorithms and Analysis	3 0 1	4
16SN601	FC	Advanced Computer Networks and Internet Architectures	3 0 1	4
16SN602	FC	Cyber Forensics and Incident Response	3 0 1	4

Subject Core

Course Code	Type	Course	L T P	Cr
16SN611	SC	Operating System and Security	3 0 1	4
16SN612	SC	Database and Web Application Security	3 0 0	3
16SN613	SC	Programming Concepts: Practical	0 0 1	1
16SN614	SC	Principles of Cryptography	3 0 0	3
16SN615	SC	Systems and Network Security -1	3 0 1	4
16SN616	SC	Wireless Security	3-0-0	3

Electives

Course Code	Course	L T P	Cr
	Elective-I		
16SN700	Distributed Systems and Security	3-0-0	3
16SN701	Security in the Cloud	3-0-0	3
16SN702	Formal Methods	3-0-0	3
	Elective-II		
16SN703	Security of Cyber Physical Systems	3-0-0	3
16SN704	Android Internal Security	2-0-1	3
16SN705	Principles of Machine Learning	3-0-0	3
16SN706	Systems and Network Security - 2	3-0-0	3
16SN707	Mobile Computing and Security	3-0-0	3
	Elective-III		
16SN708	Malware Analysis	2-0-1	3
16SN709	SCADA Network Security	3-0-0	3
16SN710	Software Protection	3-0-0	3
16SN711	Security of Internet of Things	3-0-0	3
16SN712	Digital Systems Security	3-0-0	3
16SN713	Binary Exploitation	2-0-1	3

Project Work

Course Code	Course	L T P	Cr
16SN798	Dissertation		10
16SN799	Dissertation		12

16MA609 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY SYSTEMS 4-0-0 4

Logic, Mathematical reasoning, Sets, Basics of counting, Relations.
Graph Theory: Euler graphs, Hamiltonian paths and circuits, planar graphs, trees, rooted and binary trees, distance and centres in a tree, fundamental circuits and cut sets, graph colorings and applications, chromatic number, chromatic partitioning, chromatic polynomial, matching, vector spaces of a graph.
Analytic Number Theory: Euclid's lemma, Euclidean algorithm, basic properties of congruences, residue classes and complete residue systems, Euler-Fermat theorem, Lagrange's theorem and its applications, Chinese remainder theorem, primitive roots.
Algebra: groups, cyclic groups, rings, fields, finite fields and their applications to cryptography.
Linear Algebra: vector spaces and subspaces, linear independence, basis and dimensions, linear transformations and applications.
Probability and Statistics: introduction to probability concepts, random variables, probability distributions (continuous and discrete), Bayesian approach to distributions, mean and variance of a distribution, joint probability distributions, theory of estimation,
Bayesian methods of estimation. Random Processes: general concepts, power spectrum, discrete-time processes, random walks and other applications, Markov chains,
transition probabilities.

TEXTBOOKS / REFERENCES:

1. R.P.Grimaldi, ”*Discrete and Combinatorial Mathematics*”, Fifth edition, Pearson Education, 2007.
2. K. H. Rosen, “*Discrete Mathematics and its applications*”, Seventh Edition, Tata MCGraw-Hill Publishing company limited, New Delhi, 2007.
3. H. Anton, “*Elementary Linear Algebra*”, John Wiley & Sons, 2010.
4. N. Deo, “*Graph theory with applications to Engineering and Computer Science”*, Prentice Hall of India, New Delhi, 1974.
5. T. M. Apostol, “*Introduction to Analytic Number Theory”*, Springer, 1976.
6. Douglas C. Montgomery and George C. Runger, “*Applied Statistics and Probability for Engineers”*, Third Edition, John Wiley & Sons Inc., 2003.
7. A. Papoulis and U. Pillai, Probability, “*Random Variables and Stochastic Processes”*, Fourth Edition, McGraw Hill, 2002.
8. Ronald E. Walpole, Raymond H Myres, Sharon.L.Myres and Kying Ye, “*Probability and Statistics for Engineers and Scientists”*, Seventh Edition, Pearson Education, 2002.

16SN611 OPERATING SYSTEM AND SECURITY 3-0-1- 4

Processes – Processes, Threads, Inter Process Communications (IPC) , Synchronization – Semaphores, Monitors, Scheduling, Classical IPC problems Case study – Process in Linux, User and Kernel threads Memory Management - Memory abstraction, Virtual memory, Page replacement algorithms, Design issues for paging system, Segmentation.
File Systems: Files, Directories, File System Management and Optimization.
Trusted Operating Systems, Assurance in Trusted Operating Systems, Virtualization Techniques. Introduction to OS Security – Secure operating system, Security goals, Trust model, Threat model Access Control Fundamentals – Protection system – Lampson's Access Matrix, Mandatory protection systems, Reference monitor.Verifiable security goals – Information flow, Denning's Lattice model, Bell-Lapadula model, Biba integrity model,

Covert channels. Introduction to Kernel exploitation - User space vs. Kernel space Attacks, Kernel Stack Vulnerabilities. Case study - Linux kernel, Android, Damn Vulnerable Linux (DVL)

TEXTBOOKS / REFERENCES:

1. Andrew S. Tanenbaum, “*Modern Operating Systems*”, Third Edition, Prentice Hall, 2007.
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, “*Operating System Concepts with Java*”, Eighth Edition, Wiley, 2008.
3. Trent Jaeger ,”Operating System Security”, Morgan and Claypool, 2008
4. Enrico Perla, Massimiliano Oldani, “*A Guide to Kernel Exploitation - Attacking the Core*”, Elsevier, Syngress, 2011
5. Charles P. Pfleeger , Shari Lawrence Pfleeger, “*Security in Computing*”, Fifth Edition Prentice Hall, 2015
6. Wolfgang Mauerer, “*Professional Linux Kernel Architecture*”, Wiley, 2008.
7. Daniel P. Bovet and Marco Cesati, “*Understanding the Linux Kernel*”, Third Edition, O'Reilly, 2006.
8. W. Richard Stevens, Stephen A. Rago, “*Advanced Programming in the Unix Environment*”, Third Edition, 2013

16CS602 ADVANCED ALGORITHMS AND ANALYSIS 3-0-1-4

Algorithm Analysis: Asymptotic Notation-Standard - Recurrences - Solution to Recurrences Divide and Conquer - Sorting, Matrix Multiplication and Binary Search. Dynamic Programming- Longest common sustring/subsequence - Matrix Chain Multiplication - 0-1 Knapsack problem - Coin Change problem. Greedy algorithms: Fractional knapsack, job scheduling, matroids. Graph Algorithms - Graph Traversal, Single- Source Shortest Paths, All pairs Shortest Paths, Depth First Search, Breadth First Search and their applications, Minimum Spanning Trees. Network Flow and Matching: Flow Algorithms - Maximum Flow – Cuts - Maximum Bipartite Matching -Graph partitioning via multi-commodity flow, Karger'r Min Cut Algorithm. Amortized Analysis - Aggregate Method - Accounting Method - Potential Method. String Matching Algorithms: KMP, Aho-Korasik algorithm, Z-algorithm. NP Completeness: Overview - Class P - Class NP - NP Hardness - NP Completeness - Cook Levine Theorem - Important NP Complete Problems - Reduction of standard NP Complete Problems (SAT, 3SAT, Clique, Vertex Cover, Set Cover, Hamiltonian Cycle). Approximation Algorithms: Approximation algorithms for known NP hard problems - Inapproximability - Analysis of Approximation Algorithms -

TEXT BOOKS/ REFERENCES:

1. Michael T Goodrich, Roberto Tamassia, “Algorithm Design: Foundations, Analysis and Internet Examples”, John Wiley and Sons, 2002
2. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, “Introduction to Algorithms”, Third Edition, The MIT Press, 2009
3. Sanjoy Dasgupta, Christos Papadimitriou and Umesh Vazirani, “Algorithms”, Tata McGraw-Hill, 2009
4. R. K. Ahuja, TL Magnanti, JB Orlin, “Network flows: Theory, Algorithms, and Applications”, Prentice Hall Englewood Cliffs, NJ, 1993
5. Rajeev Motwani and Prabhakar Raghavan, “Randomized Algorithms”, Cambridge

University Press, 1995.

16SN601 ADVANCED COMPUTER NETWORKS AND INTERNET ARCHITECTURES 3-0-1- 4

Review of Communication models and data transmission. Data link layer- Frames and Error detection, LAN technologies and network topology, Hardware addressing and Frame type identification, LAN wiring and interface hardware. Extending LANs. Introduction to Wireless Networks – Wireless LAN technology, Standards-Infrared LANs, Spread Spectrum – DSSS, FHSS, Narrow band. Bluetooth.

Network layer – Internet Addresses, ARP, RARP, IP, Routing algorithm – Interior and Exterior routing. ICMP, Classless and Subnet Address Extensions (CIDR), Internet Multicasting, NAT, VPN – Addressing and Routing, VPN with private address, Internet Security and Firewall design, Transport layer services and principles – Principles of congestion control. Socket Introduction-address structures-Value-Result Arguments, Byte Ordering function, Byte manipulation functions. Elementary TCP sockets. TCP Client/ Server Model of Interaction and examples. Denial-of-service (DOS) attacks. Impact of wireless technology on transport protocols. RIP, OSPF, BGP, MPLS

Software Defined Networking (SDN)Management issues in present network architecture,Key ideas and evolution of SDN, Examples of SDN controllers - OpenFlow, Ethane, Onix, SDN Programming, Mininet based OpenFlow emulator , Socket Level programming, RPC, High level networking using Java/Python, Application layer protocols – World Wide Web: HTTP – File transfer: FTP – Electronic Mail – DNS – SNMP. WAN Technologies, Next Generation Internet Architecture – Design requirements of future Internet architectures, CDN, NDN

TEXTBOOKS/ REFERENCES:

1. Andrew S. Tanenbaum, "*Computer Networks*", Fourth Edition, Pearson Education Asia, 2002.

2. Douglas E. Comer, "*Internetworking with TCP/IP Volume* – I", Fifth Edition, Prentice Hall, 2008.

3. W. Richard Stevens, Bill Fenner and Andrew M. Rudoff, "*Unix Network Programming, Vol.1: The Sockets Networking API*", Third Edition, Addison-Wesley Professional, 2003.

4. Behrouz A. Forouzan and Firouz Musharraf, "*Data Communications and Networking*", Fourth Edition, McGraw-Hill, 2007.

16SN612 DATABASE AND WEB APPLICATION SECURITY 3-0-0-3

Database security – Introduction includes threats, vulnerabilities and breaches,Basics of database design,DB security – concepts, approaches and challenges, types of access controls, Oracle VPD,Discretionary and Mandatory access control – Principles, applications and poly-instantiation,Database inference problem, types of inference attacks, distributed database, security levels, SQL-injection: types and advanced concepts.Security in relational data model, concurrency controls and locking,SQL extensions to security (oracle as an example), System R concepts, Context and control based access control,Hippocratic databases,Database watermarking,Database intrusion,Secure data outsourcing, Web application security,Basic principles and concepts,Authentication,Authorization,Browser security principles; XSS and CSRF, same origin policies,File security principles,Secure development and deployment methodologies,Web DB principles, OWASP – Top 10 - Detailed treatment,IoT security – OWASP Top 10 – Detailed treatment,Mobile device security – Introduction, attack vector and models, hardware centric security aspects, SMS / MMS vulnerabilities, software centric security aspects, mobile web browser security,Application security – Concepts, CIA Triad, Hexad, types of cyber attacks,Introduction to software development vulnerabilities, code analyzers – Static and dynamic analyzers,Security testing / Penetration testing – Principles and concepts, PT work flows and examples, blind tests, ethical hacking techniques, synthetic transactions, interface testing and fuzzing,SDLC phases and security mandates

TEXTBOOKS/ REFERENCES:

1.Michael Gertz and Sushil Jajodia, “*Handbook of Database Security— Applications and Trends*”, Springer, 2008.
2. Bryan and Vincent, “*Web Application Security, A Beginners Guide* ”,McGraw-Hill, 2011
3. Bhavani Thuraisingham, “*Database and Applications Security*”, Integrating Information Security and Data Management, Auerbach Publications, 2005.
4. Alfred Basta, Melissa Zgola, “*Database Security*”, Course Technology, 2012.

16SN613 PROGRAMMING CONCEPTS: PRACTICAL 0-0-1- 1

General Problem-Solving Concepts: Review of Concepts of Programming, Functions– Expressions and Equations –- Planning Solution: Communicating with the Computer-Organizing the Solution - Coding the Solution. Programming Structure: Structuring a Solution - Problem Solving with Logic Structure - Problem Solving with Decisions- Problem Solving with Loops
Higher level programming Concepts including Socket Level programming, RPC, High level networking using Java/Python.

TEXTBOOKS/ REFERENCES:

1. Maureen Sprankle and Jim Hubbar, “*Problem Solving and Programming Concepts*”, Ninth Edition, Prentice Hall, 2009.
2. R. G. Dromey, “*How to Solve it by Computers*”, Prentice Hall India, 2001.

16SN614 PRINCIPLES OF CRYPTOGRAPHY 3-0-0-3

Mathematics for cryptography (probability theory, complexity theory, number theory, algebra) Symmetric Key Cryptographic Systems - Caesar and affine ciphers,
mono-alphabetic substitutions, transposition, homophonic, Vigenère and
Beaufort ciphers, one-time pad, product/iterated/block ciphers, DES and AES.
Cryptanalysis of symmetric key ciphers - attack models, linear, differential and
other cryptanalysis techniques, meet-in-the-middle attack. Public (asymmetric) Key Cryptographic Systems (PKCS) - Concepts of PKCS, Diffie-Hellman key-exchange protocol, RSA, Rabin and El Gamal cryptosystems, primality testing, pollard rho factorization

(birthday paradox),man-in-the-middle attack. Stream Ciphers - synchronous and self-synchronizing stream ciphers,linear feedback shift registers, Berlekamp-Massey algorithm, algebraic attack.Digital Signatures - Rabin, Lamport, Matyas-Meyer, RSA, multiple RSA and ElGamal signatures, digital signature standard.

Hash Functions and MACs - Hash functions: the Merkle-Damgard construction, Message Authentication Codes (MACs). Boolean functions - discrete Fourier transform on Boolean functions, Parseval's relation, cryptographic criteria for Boolean functions,

nonlinearity, balancedness and resiliency, algebraic immunity, bent Booleanfunctions

TEXTBOOKS/REFERENCES:

1. William Stallings, "*Cryptography and Network Security*", Fifth Edition, Prentice Hall, 2011
2. Josef Pieprzyk, Thomas Hardjono and Jenifer Seberry , "*Fundamentals of Computer Security*", Springer, 2003.
3. Alfred J Menezes, Paul C Van Oorshot and Scott A. Vanstone, "*Handbook of Applied Cryptography*", CRC Press, 1996.
4. Claude Carlet, "*Boolean Functions for Cryptography and Error Correcting Codes"*, http://www.math.univ-paris13.
5. Stein William. "*Elementary number theory. Primes, congruences, and secrets. A Computational approach*", http://wstein.org/ent/
6. Neal Koblitz. "*A Course in Number Theory and Cryptography*", Springer-Verlag,1994

16SN602 CYBER FORENSICS AND INCIDENT RESPONSE 3-0-1- 4

Introduction to Cyber Forensic Investigation, Investigation Tools, Digital Evidence Collection, Evidence Preservation, E-Mail Chat Investigation, Data Recovery,Encryption and Decryption methods, Search and Seizure of Computers and devices, Recovering deleted evidences, Password Cracking, Hardware Forensics, Memory Forensics, Mobile Forensics, Network and communication Forensics, Security Standards, Assessing Threat Levels, Incident Response, Cyber Laws and Legal Frameworks, Operating System Attacks, Malware Analysis, Cloud forensics, Financial Frauds, Espionage and Investigations.

TEXTBOOKS/ REFERENCES:

1. Digital Evidence and Computer Crime: Forensic Science, Computers,and the Internet, Third Edition, Eoghan Casey, ISBN: 978-0-120374268-1
2. Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom Larry Daniel, Lars Daniel ISBN: 978-1-59749-643-8
3. Android Forensics: Investigation, Analysis and Mobile Security for Google Android, Andrew Hoog, ISBN: 978-1-59749-651-3

16SN615 SYSTEMS AND NETWORK SECURITY - 1 3-0-1-4

Introduction-Need for network security, Goals of Network Security Overview, Network Security Model, Types of Attack, Overview of Most Common Security Issues, Linux

Security Overview, Password Attack, Dictionary Attack - Thwarting dictionary attack, IPTables, Using iptables to thwart dictionary attack, Password Cracking - Hashing overview, Lookup tables, Introduction to Rainbow Table, Modern Linux Password Hashing Scheme Malware Primer - Viruses and Worms, Virus Infection Techniques, Classification of Viruses, Defenses, Case Study Morris Worm & Conficker worm, Application Vulnerabilities – Assembly Primer, ELF File Format, Smashing the Stack for Fun and Profit, Format String Attacks, Integer Overflow, Return to Libc Attacks, Heap Overflow, ROP Web Security-Overview of HTML & Javascript, DOM, Browser Security, Cookies, URLs, Secure HTTP, Session Hijacking, SSL/TLS For Secure Web Services – SSL Connection & SSL Session, SSL Connection State, SSL Session State, SSL Record Protocol, SSL Handshake Protocol, TOR Protocol for Anonymous Routing, Email Spam and Solutions. Ciphertext Attacks-Perfect Secrecy, Statistical Attack on Substitution Ciphers, One Time Pad, Vulnerabilities of Two time pad, WEP Attack, Overview of Private Key & Public Key Cryptography, PRG, Secure PRF, Overview of Stream & Block Cipher, Padding Oracle Attacks, Digital Signatures, Message Authentication Codes, HMAC, Authentication & Key Distribution – Needham Schroeder, Kerberos TCP/IP Vulnerabilities- TCP Overview - Connection Setup/Teardown, Packet Sniffing, Detecting Sniffers on your network, IP Spoofing, ARP Poisoning, UDP Hijacking, Fragmentation Attack- Ping of Death, Evasion & Denial of Service, UDP Hijacking, TCP Spoofing, TCP Hijacking - Mitnick attack, Joncheray attack, SYN Flood Attack, Denial of Service Attack, Port Scanning Techniques, ICMP- ICMP Attacks – ICMP Echo Attacks, Smurf Attacks, ICMP Redirect Attacks, DNS – DNS Zones, Zone Transfer, BIND, DNS Spoofing, DNS Cache Poisoning, IPSec – Introduction, Tunnel & Transfer Modes, IPSec Authentication Header, Encapsulating Security Header and Payload, IPSec Key Exchange, VPNs Firewalls – Packet-filtering, Stateless and Stateful, Intrusion Detection.

TEXT BOOKS/REFERENCES:

1. Charlie Kaufman, Radia Perlman and Mike Speciner, "*Network Security: PRIVATE Communication in a PUBLIC world*", Second Edition, Prentice Hall, 2002.
2. Neil Daswani, Christopher Kern, Anita Kesavan, "*Foundations of Security, What Every Programmer Needs to Know*",Apress, 2007
3. Eric Rescoria, "*SSL and TLS : Designing and Building Secure Systems*", Addison-Wesley Professional, 2000.
4. Jonathan Katz, Yahuda Lindell, "*Introduction to Modern Cryptography*", CRC Press,2014
5. Larry L.Peterson, Bruce S. Davie, "*Computer Networks: A Systems Approach*",*TBS,2011*
6. Jon Ericson, "*Hacking: The Art of Exploitation*", Second Edition, No Starch Press, 2008
7. Gary McGraw, John Viega, "*Building Secure Software*", Addison-Wesley Professional, 2001.

16SN616 WIRELESS SECURITY 3-0-0- 3

Wireless Standards Security: Vulnerabilities in existing Wireless networks, Bluetooth Security, 3G Security, Wifi Security. Trends and Upcoming Wireless Networks: Upcoming Wireless Networks, Trends and Security challenges in wireless networks. Trust Assumptions and Adversary models: Trust, Trust in Ubiquitous computing. Physical Layer Security: Jamming, Wiretapping, Physical Layer defenses. MAC Layer Security: Operating principles of IEEE 802.11, Detecting selfish behavior in hotspots, Selfish behavior in pure ad hoc networks, MAC layer defenses. Network Layer Security: Securing ad hoc network routing protocols, Secure routing in sensor networks, Network layer defenses. Privacy in Wireless Networks: Privacy in RFID Systems, Location privacy in vehicular networks, Privacy preserving routing in ad hoc networks. Game Theory: Normal Form Games, Strict Dominance, Weak Dominance, Iterated Dominance, Pure and Mixed Strategy Nash Equilibrium, Extensive Form Games, Backward Induction, Subgame Perfect Nash Equilibrium, Game Theory in Wireless Networks, Forwarder's dilemma, Joint Packet Forwarding game, Multiple Access Game and Jamming Game. Applications: RFID Security, Security for Wireless Sensor Networks, Security for Vehicular Networks.

TEXT BOOKS/REFERENCES:

1. Nicholos Lekkas, *"Wireless Security"*, McGraw-Hill, 2000.
2. Kaveh Pahlavan and Prashant Krishnamurthy, *"Principles of Wireless Networks"*, Prentice Hall, 2006.

16EN600 TECHNICAL WRITING P/F

(Non-credit Course)

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.)

TEXTBOOKS/REFERENCES:

1. H.L. Hirsch, *Essential Communication Strategies for Scientists, Engineers and Technology Professionals*, Second Edition, New York: IEEE Press, 2002.
2. P.V. Anderson, *Technical Communication: A Reader-Centered Approach,* Sixth Edition, Cengage Learning India Pvt. Ltd., New Delhi, 2008, (Reprint 2010).
3. W.Jr. Strunk and E.B.White, *The Elements of Style*, New York. Alliyan & Bacon, 1999.

16SN700 DISTRIBUTED SYSTEMS AND SECURITY 3-0-0-3

Introduction: Goals, challenges, types of distributed systems. Architectures: centralized, decentralized and hybrid architectures, interceptors, self-management in distributed systems, server clusters, code migration. Communication: RPC/RMI, message-oriented, stream-oriented multicast.

Naming: Flat naming, structured naming and attribute-based naming. Synchronization: Physical clock, logical clocks: Scalar and vector clocks, mutual exclusion, leader election. Consistency and replication: Data-centric and client-centric consistency models, replica management.

Fault tolerance: Process resilience, reliable unicast and multicast communication, distributed commit, check pointing and recovery. Security: Threats, policies, mechanisms, secure channels, access control and security management.

Case studies: Enterprise Java Beans, Globe distributed shared objects, NFS/DFS, Amoeba operating system, web server clusters.

TEXTBOOKS/ REFERENCES:

1. Andew S. Tanenbaum and Maarten van Steen, “*Distributed Systems: Principles and*

Paradigms", Second Edition, Pearson Prentice-Hall, 2007.

2. George Coulouris, Jean Dollimore and Tim Kindberg ," *Distributed Systems: Concepts and Design*", Fourth Edition, Addison-Wesley, 2005.

3. Vijay K. Garg, "*Elements of Distributed Computing*", John Wiley & Sons, 2002.

4. Ajay D. Kshemkalyani and Mukesh Singhal, "Distributed Computing: Principles, Algorithms, and Systems", Cambridge University Press,2011

16SN701 SECURITY IN THE CLOUD 3-0-0- 3

Introduction to cloud computing:- Evolution of cloud computing, Definition of cloud computing, NIST reference model, Service delivery model, Deployment models, Benefits and challenges of cloud adoption,Introduction to popular cloud platforms, Virtualization, Containers Security Introduction and Distributed Computation: - Concepts of security, Threats and Risk analysis, Attacks in cloud, STRIDE model, Infrastructure security, virtualization and container security, Distributed computation-benefits and challenges, mapreduce concept.Advanced Security Concepts:- Trustworthy cloud infrastructures, Differential privacy, Secure computations, High-availability and integrity layer for cloud storage, Homomorphic encryption, Malware and cloud, Cloud forensics.Cloud-centric regulatory compliance issues and mechanisms

TEXT BOOKS / REFERENCES:

1. Tim Mather, S. Kumaraswamy and S. Latif, "*Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*", O'Reilly Media, 2009
2. Ronald L. Krutz Russell Dean Vines "*Cloud Security: A Comprehensive Guide to Secure Cloud Computing*", Wiley ,2010
3. [Paper] Roy, Indrajit, et al. "*Airavat: Security and Privacy for MapReduce*." NSDI. Vol. 10. 2010.
4. [Paper] Bowers, Kevin D., Ari Juels, and Alina Oprea. "*HAIL: a high-availability and integrity layer for cloud storage*" Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009.
5. [Paper] Dean, Jeffrey, and Sanjay Ghemawat. "*MapReduce: simplified data processing on large clusters*" Communications of the ACM 51.1 (2008): 107-113.

16SN702 FORMAL METHODS 3-0-0-3

Background: Computability and Complexity

Decidability, Semi-decidability, Undecidability, Halting problem, Rice's theorem
Overview of complexity classes: P, NP, NP-completeness.
Propositional and First-Order Logic: Syntax, Semantics, Proof methods

Program Verification: Floyd-Hoare logic, Weakest Pre-conditions; Partial Correctness and Termination Structural induction and Fixed-point induction for recursive procedures

Z specification language: Fundamentals and abstract datatype specifications.
Data refinement in Z abstract data types: Forward and backward simulation, Concurrent Programs and Correctness Properties: Owick-Gries, Assume-Guarantee

Reactive Systems: Transformational vs Reactive systems, Temporal Logic: Linear (LTL) and Branching Time (CTL), Temporal specification of reactive systems: Safety, Liveness, Fairness, Buchi automata, LTL-to-Buchi automata, Properties: containment, emptiness

Model Checking: LTL and CTL model-checking. Analysis of model-checking algorithms Symbolic model checking; overview of state-space reduction methods, Case study and practical verification of properties

Process Algebra: CCS and Pi-calculus, Reductions and labelled transitions, Harmony lemma, Bisimulations

TEXT BOOKS / REFERENCES:

1. E.M. Clarke, O. Grumberg, and D. Peled "*Model Checking*", MIT Press, 2000.
2. Davide Sangiorgi and David Walker, "*Pi-calculus: The Theory of Mobile Processes*", Cambridge University Press,2001
3. Sanjeev Arora and Boaz Barak, "*Computational Complexity – A Modern Approach*", Cambridge University Press, 2009
4. Michael Huth and Mark Ryan, "*Logic in Computer Science*". Cambridge University Press, 2004.
5. J. Woodcock & J. Davies "*Using Z: Specification, Refinement and Proof*", Prentice Hall, 1994.

16SN703 SECURITY OF CYBER PHYSICAL SYSTEMS 3-0-0- 3

Security and vulnerability of cyber-physical infrastructure networks, game theory for infrastructure security, An analytical framework for cyber-physical networks, Mobile and wireless network security, Robust wireless infrastructure against jamming attacks, Security of Mobile Adhoc networks, Defending against indentity based Attacks in wireless networks, Security of sensor networks , Hardare & Security:Vulnerabilities & Solutions, Languages and Security: Safer software through Language and Compiler techniques, Cloud computing and data security, Event Awareness and System Monitoring for Cyber Physical Infrastructure, Pervasive Sensing and Monitoring for Situational Awareness, Managing and Securing Critical Infrastructure with Semantic Policy and Trust-Driven Approach, Policies, Acess Control and Formal Methods, Formal Analysis of Policy-Based Security Configuarations in Enterprise Networks, Security and Privacy in Smart Grid, Automotive Information Technology, Mobile Health-Care (m-health) systems, VoIP Telecommunication Networks.

TEXTBOOKS/ REFERENCES:

1. Sajal Das, Krishna Kant, and Nan Zhang, "*Securing Cyber-Physical Critical Infrastructure – Foundations & Challenges*", Morgan Kaufmann, 2012.

16SN704 ANDROID INTERNALS AND SECURITY 2-0-1- 3

Introduction - Android Framework, Dalvik Virtual Machine, Art Virtual Machine, Linux OS Review -Process, Program, File System, Partition, DAC, MAC -, Android Hardware Architecure Layer, IPC Mechanism in Android, Android OS Internals – Rooting an Android Device, Android's Init, Zygote, Binder Activity Manager, Package Manager, APK Components -Activity, Services, Broadcast Receivers, Content Providers, , Intent, Intent Receivers, Android Manifest Android Development- Development Tools, Application Runtime, Application Framework, Building an App, Linux Networking Refresher– Ports, Sockets, Java Networking, Linux/Android IP Tables, Android Virtual Devices – Emulator Networking, File Systems – ext4, vfat, yaffs2, AVD Networking – Connecting Android VD, Routing Table, NetCat, Network Devices with lo and eth, TCP/IP Networking Overview, Well known TCP/IP exploits on Android, Android Security – Android Permissions, Login Credentials, SE Android Reverse engineering of APKs – Tools, Analyses of Android malware, Bouncer, Privacy, Code Injection- ASLR, ROP-, Mitigation – Kernel Hardening, System Call Hardening-, Security enhancement of Android Framework. ASLR and ROP. Android Forensics. Future of body-hugging computing/networking devices

TEXT BOOKS/REFERENCES:

1. Nikolay Elenkov, "*An In-Depth Guide to Android's Security Architecture*",October 2014, 432 pp. ISBN: 978-1-59327-581-5
2. Karim Yaghmour, *"Embedded Android"*, O'Reilly Media, Inc., 2013, 412 pp; WSU Safari Books Online 9781449327958
3. Joseph Annuzzi, Jr., Lauren Darcey, Shane Conder, *"Introduction to Android Application Development: Android Essentials"*, Fourth Edition, Addison-Wesley Professional, 2013
4. Adapted Materials from Android development sites.

16SN705 PRINCIPLES OF MACHINE LEARNING 3-0-0- 3

Role of learning in intelligent behavior, Designing a learning system; learning from example; Concept learning, Bayesian decision theory, Bayesian Learning, Decision tree learning: Univariate Trees , Classification Trees , Regression Trees , Rule Extraction from Trees, Learning Rules from Data , linear discrimination, SVMs: linear SVMs, introduction to kernel methods, multilayer perceptrons, Local models, Competitive Learning, Incorporating Rule-Based Knowledge ,Computational Learning Theory, Instance based Learning, Learning sets of Rules, Analytical Learning, Boosting algorithms, Combining multiple learners, Reinforcement learning.

TEXTBOOKS/ REFERENCES:

1. Tom Michael, "*Machine Learning*", McGraw Hill, 1997.
2. E. Alpaydin, "*Introduction to Machine Learning*", PHI, 2005.
3. T. Hastie, R.T Ibshirani and J. Friedman, "*Machine Learning*", McGraw Hill 1997.
4. T. Hastie, R.T Ibshiran, and J. Friedman, "*The Elements of Statistical Learning*", Springer, 2001.
5. Y.N.Vapnik, "*The Nature of Statistical Learning Theory*", Springer, 1999.

16SN706 SYSTEMS AND NETWORK SECURITY -2 3-0-0-3

Application Security – Introduction – Overview of Attacks Against Applications, Attacking SUID Programs, Environment Attacks, Input Argument Attacks, File Access Attacks, Smashing the Stack for Fun and Profit, Format String Attacks, Assembly Primer, ELF File Format, PLT and GOT, Data and BSS Overflow,Array Overflow, Non-terminated String Overflow, Heap Overflow, Tools and Defenses

Network Security – Introduction – Overview of Network Attacks, Network Protection - IDS, Types of IDS's, Issues in Intrusion Detection, Challenges in Intrusion Detection, Taint Analysis, Network Based IDS, Problems in NIDS, Impact Analysis, TCP Overview - Connection Setup/Teardown, Packet Sniffing, Detecting Sniffers on your network, IP Spoofing, ARP Poisoning, UDP Hijacking, Fragmentation Attack- Ping of Death, Evasion & Denial of Service, UDP Hijacking, TCP Spoofing, TCP Hijacking - Mitnick attack, Joncheray attack, SYN Flood Attack, Denial of Service Attack, Port Scanning Techniques, ICMP, ICMP Attacks – ICMP Echo Attacks, Smurf Attacks, ICMP Redirect Attacks, WLAN, 802.11, Wireless Security Overview, Attacks Against Wireless Networks – Eavesdropping, WEP Attacks, Injection Attacks -, WEP Encryption, WEP Attacks, FMS Attack, Denial of Service, Man-in-the-Middle Attack, Protection Mechanisms and Tools, War Driving, Vulnerabilities in Internet Applications(SMTP, FTP, DNS, Remot Access), SPAM, DNS Zones, Zone Transfer, BIND, DNS Spoofing, DNS Cache Poisoning**,** IPSec – Introduction, Tunnel & Transfer Modes, IPSec Authentication Header, Encapsulating Security Header and Payload, IPSec Key Exchange, VPNs, FTP Protocol,Exploiting FTP, FTP Bounce

Web Security – HTTP Challenge Response Protocol, Web-based Authentication, Man-in-the-Middle Attacks, Cookies, Sessions, CGI, Active Server Pages (ASP), Servlets, Java Server Pages, PHP, Web Framework, Client-side Scripting , DOM and BOM, Javascript Security, Browser Security, AJAX, Web Attacks, SQL Injection, XSS, Authentication Attacks, Authorization Attacks, Command Injection Attacks, Server-Side Includes(SSI)

TEXT BOOKS/REFERENCES:

1. Charlie Kaufman, Radia Perlman and Mike Speciner, "*Network Security: PRIVATE Communication in a PUBLIC world*", Second Edition, Prentice Hall, 2002.
2. Eric Rescoria, "*SSL and TLS : Designing and Building Secure Systems*", Addison-Wesley Professional, 2000.
3. Jonathan Katz, Yahuda Lindell, Introduction to Modern Cryptography, CRC Press
4. Larry L.Peterson, Bruce S. Davie, Computer Networks: A Systems Approach
5. Jon Ericson, Hacking: The Art of Exploitation , Second Edition, No Starch Press, 2008

16SN707 MOBILE COMPUTING AND SECURITY 3-0-0- 3

Introduction to Mobile Computing: Mobile Compuing Models, Design and Implementation, Mobile Architecture, Service Discovery protocol, Mobile P2P systems, Mobile Networking; Security in Mobile Computing: Information flow tracking, Privacy, Application Security, Execution transparency; Situation Awareness: Situation Models, Modeling situation awareness, Modelling Context and User; Location awareness: Indoor localization – Radar, Horus, Outdoor localization – Global Positioning Satellite, Assisted Global Positioning Satellite; Context-Aware Computing: Context modeling, Ontological based approach, Context Reasoning, Context-aware systems, Middleware in Context Aware Computing, Context-aware security, Proactive Computing.

TEXTBOOK AND REFERENCES:

1. F. Adelstein, S.K.S. Gupta, G.G. Richard III and L. Schwiebert, “*Fundamentals of Mobile and Pervasive Computing”*, McGraw Hill, 2005, ISBN: 0-07-141237-9.

2. This will be a research paper based course. Students are expected to read, summarize and discuss assigned research papers in the field for each class.

16SN708 MALWARE ANALYSIS 2-0-1-3

Introduction to malware, Basic Static and Dynamic Analysis, Overview of Windows file format, PEView.exe, Patching Binaries , Disassembly(objdump, IDA Pro), Introduction to IDA, Introduction to Reverse Engineering, Extended Reverse Engineering using GDB and IDA, Advanced Dynamic Analysis - debugging tools and concepts, Malware Behavior - malicious activities and techniques, Analyzing Windows programs – WinAPI, Handles ,Networking , COM, Data Encoding, Malware Countermeasures , Covert Launching and Execution, Anti Analysis- Anti Disassembly, VM, Debugging -, Packers – packing and upacking, Intro to Kernel – Kernel basics, Windows Kernel API, Windows Drivers, Kernel Debugging - , Rootkit Techniques- Hooking, Patching, Kernel Object Manipulation , Rootkit Anti-forensics , Covert analysis

TEXT BOOKS / REFERENCES:

1.Michael Sikorski and Andrew Honig, “ *Practical Malware Analysis*”, No Starch Press,2012
2.Jamie Butler and Greg Hoglund, “*Rootkits: Subverting the Windows Kernel*”, Addison-Wesley, 2005
3.Dang, Gazet and Bachaalany, “*Practical Reverse Engineering*”,Wiley,2014
4. Reverend Bill Blunden, “*The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System*” Second Edition,Jones & Bartlett, 2012.

16SN709 SCADA NETWORK SECURITY 3-0-0-3

Introduction-Critical Infrastructure Control System Cybersecurity Background, Brief History of Critical Infrastructure and ICS, Overview of ICS Processes & Roles Types of ICS Systems, Fundamental principles and concepts of SCADA, DCS, PLCs, Field components, Real-Time Operating systems and Ladder Logic, Communications and OLE for Process Control (OPC), DCS vs. SCADA, IT & ICS Differences, ICS Lifecycle Challenges Physical Security, ICS Network Architecture, Network Models, Design Example, Industrial Control Systems (ICS) characteristics, threats and vulnerabilities, Introduction to PLC and role in automation, PLC components, Field devices connected to PLC,PLC Programming (LD , FBD),PLC - SCADA Communications, History of SCADA, Architecture, Components, Functions, SCADA Control and Next Generation SCADA Systems, Features - HMI, Data Historian, Visualization tools, SLD, Error detection, Alarms and Events - handling, logging, archiving, reports,Protocols - Modbus, DNP3, Profinet, IEC Variants (60870-5-101/4,61580), Ethernet/IP, BacNET, SCADA Protocols over Serial RS-485 and RS-232 and Ethernet TCP/IP communication, Industrial Wireless and IoT (802.11, 900 Mhz, GPRS and Zigbee),Inter- Master Station Communication-ICCP SCADA reliability, redundancy and Fault Tolerance.ICS/SCADA Security-Overview, ICS Attack Surface, Threats and Attack Routes, Risk Assessment, Components, Attacks on HMIs and UIs, Remote devices, Firmware, Attacks on Control servers, Network communications, Web attacks, Security Standards & Mitigation - NIST, ISA, NERC CIP, etc. Security Testing - Penetration testing approaches, programs, tools, Defending ICS servers and Workstations - Windows, Linux, Updates, Patching, Endpoint defenses, Log management, Databases and Historians, Defending ICS Networks and Devices - WAN,LAN Security Mechanisms, Intrusion Detection Systems, Firewalls, NAC, Enforcement Zone devices, DMZs, Unidirectional gateways, honeypots,ICS/SCADA Security-Advanced,Development and implementation of security controls for SCADA Systems, Introduction to tools, Building Domain Specific Models in process control and automation using SCADA - Power, HVAC, Storage, Pipeline etc.

TEXT BOOKS / REFERENCES:

1. Eric D. Knapp, “*Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*”, O'Reilly, 2014
2. Robert Radvanovsky and Jacob Brodsky, “*Handbook of SCADA/Control Systems Security”*, Second Edition, 2016
3. Jack Wiles and Ted Claypoole, “*Techno Security's Guide to Securing SCADA: A Comprehensive Handbook On Protecting The Critical Infrastructure*”, 2008

16SN710 SOFTWARE PROTECTION 3-0-0- 3

Introduction: Software Protection: What, why, how.

Setting up software analysis lab. State-of-the-art tools. Protocol for handling potentially malicious programs. Legal issues.

Offensive and Defensive strategies - Offense – Motivation, Methods of attacking software protection. Defense: Methods for hiding information, purpose, algorithms in software.

Program Analysis Static analysis: Control flow analysis, data flow analysis, dependence analysis.

Dynamic analysis: Debugging, tracing, profiling, emulation.

Static Code obfuscation - In-depth Semantics preserving obfuscating transformations, complicating control flow, opaque predicates, data encoding, breaking abstractions.

Obfuscation – Theoretical Bounds Various impossibility results.

Tamper roofing and Watermarking Definitions, Algorithms for Tamperproofing, Remote Tamperproofing.

Watermarking Definitions, Methods of Watermarking, Tamperprooging watermarks, Resilient watermarks, Stealth watermarks. Steganographic watermarks, Dynamic watermarking.
Software Similarity Analysis:- Alternate methos for defeating obfuscations. K-gram based analysis, API-Based analysis, Tree-based Analysis, Graph-Based analysis, Metrics-Based Analysis.

TEXTBOOKS/ REFERENCES:

1. Christian Collberg and Jasvir Nagra, "*Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection*," Addison-Wesley, 2010.

16SN711 SECURITY OF INTERNET OF THINGS 3-0-0-3

Fundamentals,Architecture of IoTs, IoT Security Requirements, IoT Privacy Preservation Issues, Attack Models - Attacks to Sensors in IoTs, Attacks to RFIDs in IoTs,Attacks to Network Functions in IoTs,Attacks to Back-end Systems,Security in Front-end Sensors and Equipment,Prevent Unauthorized Access to Sensor Data,M2M Security,RFID Security,Cyber-Physical Object Security,Hardware Security,Front-end System Privacy Protection,Networking Function Security-IoT Networking Protocols,Secure IoT Lower Layers,Secure IoT Higher Layers,Secure Communication Links in IoTs,Back-end Security-Secure Resource Management,Secure IoT Databases,Security Products-Existing Testbed on Security and Privacy of IoTs,Commercialized Products

TEXT BOOKS / REFERENCES:

1. Fei HU, "*Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*", CRC Press,2016
2. Russell, Brian and Drew Van Duren, "*Practical Internet of Things Security*", Packt Publishing, 2016.
3. Ollie Whitehouse, "*Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond*", NCC Group, 2014

16SN712 DIGITAL SYSTEMS SECURITY 3-0-0-3

Introduction to Hardware Description Languages (HDL) – Design of combinational logic and sequential elements in HDL – Register Files – FIFOs – LIFOs – SIPOs – Bidirectional Shift Register – Universal Shift Register – Barrel Shifter – Linear Feedback Shift Registers – Memory – RAM – Static RAM – Dynamic RAM – Booth Multiplier – Introduction to FSM and State Diagram – Vulnerabilities in Combinational and Sequential Logic – Finite State Machines – Trojan Attacks – Detection and Isolation – Side-channel Attacks - Emerging Hardware Security Topics – Digital Water Marking – Physically Unclonable Functions (PUFs) – Linear Feedback Shift Registers (LFSR) – Pseudo Random Pattern Generators (PRPG) – True Random Number Generators (TRNG) – Boundary scan – Attacks and Protection mechanisms – Logic Design of Crypto algorithms – Introduction to FPGA – Design and Synthesis of Security modules on FPGA.

TEXT BOOKS / REFERENCES:

1. Michael D. Ciletti, “*Advance Digital Design with Verilog HDL*”, Pearson Higher Education, 2011.
2. M. Tehranipoor and C. Wang, “*Introduction to Hardware Security and Trust”*, Springer, 2011.
3. Jim Plusquellic, “*Trojan Taxonomy*”, University of New Mexico, http://www.ece.unm.edu/~jimp/HOST.
4. Debdeep Mukhopadhyay, Rajat Subhra Chakraborty “*Hardware Security Design, Threats, and Safeguards*”, CRC press, 2015.

16SN713 BINARY EXPLOITATION 3-0-0-3

Overview – Memory Corruption Attacks, Defenses, ASLR, Bypassing Stack Cookies, DEP, ROP, SROP, Heap Overflow- heap structure, corruption, use after free, , C++ differences and concepts, Introduction to kernel exploitation, Kernel vulnerabilities, Kernel memory attacks, Windows kernel overview, Practical windows exploitation, Remote kernel exploitation Future -Fuzzing, Taint analysis, Dynamic instrumentation

TEXT BOOKS / REFERENCES:

1. Jon Ericson, “*Hacking: The Art of Exploitation”*, Second Edition, No Starch Press, 2008, ISBN 978-1593271442
2. Enrico Perla, Massimiliano Oldani, “*A Guide to Kernel Exploitation-Attacking the Core*”, First Edition, Elsevier, 2010
3.Chris Anley, John Heasman, Felix Linder, Gerardo Richarte, The Shellcoder’s Handbook : Discovering and Exploiting Security Holes, Second Edition, Addison-Wiley, ISBN 978-0470080238