## M.TECH. CYBER SECURITY SYSTEMS AND NETWORKS

### Amrita Centre 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 its 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 title | L-T-P | Credits |
|---|---|---|---|---|
| 18SN611 | SC | Essentials of Cyber Security | 0 0 3 | 3 |
| 18SN612 | SC | Operating System and Security | 3 0 1 | 4 |
| 18SN601 | FC | Practical Algorithms for Programmers | 1 0 3 | 4 |
| 18SN613 | SC | Network Security | 3 0 1 | 4 |
| | | Elective -I | | 3 |
| 18HU601 | HU | Amrita Values Program* | | P/F |
| 18HU602 | HU | Career Competency I* | | P/F |
| | | | Credits | 18 |

***** Non-credit Course

### Second semester

| Course code | Type | Course title | L-T-P | Credits |
|---|---|---|---|---|
| 18SN614 | SC | Cryptography and Applications | 4 0 0 | 4 |
| 18SN615 | SC | Systems Security | 3 0 1 | 4 |
| 18SN616 | SC | Cyber Forensics and Incident Response | 2 0 1 | 3 |
| | E | Elective II | | 3 |
| | E | Elective III | | 3 |
| 18HU603 | HU | Career Competency II | 0 0 2 | 1 |
| 18RM600 | SC | Research Methodology | 2 0 0 | 2 |
| 18SN797 | P | Live-in-Labs* | | P/F |
| | | | Credits | 20 |

***** Non-credit Course

### Third semester

| Course code | Type | Course title | L-T-P | Credits |
|---|---|---|---|---|
| | E | Elective IV | | 3 |
| | E | Elective V | | 3 |

| | | | | |
|---|---|---|---|---|
| 18SN798 | P | Dissertation | | 10 |
| | | | Credits | 16 |

**Fourth semester**

| Course code | Type | Course title | L-T-P | Credits |
|---|---|---|---|---|
| 18SN799 | P | Dissertation | | 10 |
| | | | Credits | 10 |

**Total credits: 64**

**List of courses**

**Foundation core**

| Course code | Type | Course title | L-T-P | Credits |
|---|---|---|---|---|
| 18SN601 | FC | Practical Algorithms for Programmers | 1 0 3 | 4 |

**Subject Core**

| Course code | Type | Course title | L-T-P | Credits |
|---|---|---|---|---|
| 18SN611 | SC | Essentials of Cybersecurity | 0 0 3 | 3 |
| 18SN612 | SC | Operating System and Security | 3 0 1 | 4 |
| 18SN613 | SC | Network Security | 3 0 1 | 4 |
| 18SN614 | SC | Cryptography and Applications | 3 0 0 | 3 |
| 18SN615 | SC | Systems Security | 3 0 1 | 4 |
| 18SN616 | SC | Cyber Forensics and Incident Response | 2 0 1 | 3 |

**Electives**

| Course code | Course title | L-T-P | Credits |
|---|---|---|---|
| 18MA612 | Mathematical Foundations for Cyber Security | 3 0 0 | 3 |
| 18SN701 | Distributed Systems and Security | 3 0 0 | 3 |

| | | | |
|---|---|---|---|
| 18SN702 | Security in the Cloud | 3 0 0 | 3 |
| 18SN703 | Formal Methods | 3 0 0 | 3 |
| 18SN704 | Security of Cyber Physical Systems | 3 0 0 | 3 |
| 18SN705 | Android Internal Security | 2 0 1 | 3 |
| 18SN706 | Advanced Network Security | 3 0 0 | 3 |
| 18SN707 | Mobile Computing and Security | 3 0 0 | 3 |
| 18SN708 | Malware Analysis | 2 0 1 | 3 |
| 18SN709 | SCADA Network Security | 3 0 0 | 3 |
| 18SN710 | Software Protection | 3 0 0 | 3 |
| 18SN711 | Security of Internet of Things | 1 0 2 | 3 |
| 18SN712 | Digital Systems Security | 3 0 0 | 3 |
| 18SN713 | Introduction to Software Reverse Engineering | 2 0 1 | 3 |
| 18SN714 | Wireless Security | 3 0 0 | 3 |
| 18SN715 | Database and Web Application Security | 3 0 0 | 3 |
| 18SN716 | Data Analytics for Security | 2 0 1 | 3 |
| 18SN717 | Blockchains and Cryptocurrencies | 2 0 1 | 3 |
| 18SN718 | Cybersecurity Governance | 3 0 0 | 3 |
| 18SN719 | Software Defined Networking and Security | 1-0-2 | 3 |

**Project Work**

| Course Code | Course title | L T P | Credits |
|---|---|---|---|
| 18SN798 | Dissertation | | 8 |
| 18SN799 | Dissertation | | 12 |

**18SN611 ESSENTIALS OF CYBERSECURITY 0-0-3-3**

Linux: Install Linux using a VM. Installing softwares in linux using apt, Using the shell, changing passwords, resetting password from GRUB, password protecting GRUB, installing mysql on docker, connecting to other linux machines using SSH, configuring passwordless login using SSH, verifying file integrity
IPtables: Configuring iptables, exercises using iptables (blocking a particular service, blocking a particular port, whitelisting, blocking IP from a certain country)
Cookie Stealing Lab: Locating cookies in file system, Install firebug plugin to export cookie and importing it in another machine, automating cookie stealing using python.
Secure Email using gpg: Setting up gpg keys, securing email using gpg
Openssl Lab: Encryption and decryption using openssl
Information Gathering: Enumerating Ports, SMB, SMTP, SNMP; Using Shodan.io to scan IoT devices; Vulnerability scanning using OpenVAS
Metasploit: Installing and setting up, MSF, Payloads, Exploiting using Metasploit
Password Cracking: Dictionary attack, Keyspace bruteforce, using online tools (Ncrack, Hydra), Password hash attacks
Capture the Flag exercises: Basic exercises in Crypto, Reverse Engineering, forensics and exploitation using InCTFj

**18SN612 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 8 Management - Memory abstraction, Virtual memory, Page replacement algorithms, Design issues for paging system, Segmentation. File Systems - Files, Directories, File System Management and Optimization. Virtualization Techniques. Introduction to OS Security. Linux Kernel Modules. Linux Security Modules, SELinux. Malwares. Introduction to Kernel exploitation - User space vs. Kernel space Attacks, Kernel Stack Vulnerabilities. Case study - Linux kernel

**TEXTBOOKS / REFERENCES:**

1. Andrew S. Tanenbaum, “Modern Operating Systems”, Third Edition, Prentice Hall, 2009.
2. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, “Operating System Concepts with Java”, Ninth Edition, Wiley, 2012.
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. Wolfgang Mauerer, “Professional Linux Kernel Architecture”, Wiley, 2008.
6. Daniel P. Bovet and Marco Cesati, “Understanding the Linux Kernel”, Third Edition,O'Reilly, 2006.
7. W. Richard Stevens, Stephen A. Rago, “Advanced Programming in the Unix Environment”, Third Edition, 2013

**18SN601 PRACTICAL ALGORITHMS FOR PROGRAMMERS 1-0-3-4**

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.

**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.


**18SN613 NETWORK SECURITY 3-0-1-4**

Introduction - Overview of computer networks and network security
Application layer - Overview of HTTP, FTP, SMTP and DNS and socket programming. Weaknesses, vulnerabilities and attacks against above protocols - hijacking, spoofing and DoS attacks. Attacks using above protocols: simple, amplified and distributed DoS attacks.
Application layer security - Goals, cryptography primitives and principles, TLS - Objectives, protocol, working and features, PGP: Overview, objective, working, features and limitations. Firewalls, Intrusion Detection Systems and Intrusion Prevention Systems. Future directions.
Transport layer - Introduction, objectives, unreliable data transfer and UDP, general principles of reliable data transfer, TCP: Overview, reliable data transfer, flow control, congestion control. Attacks against transport layer protocols: UDP flooding, TCP spoofing, TCP connection hijacking, TCP SYN flood.
Network layer – Addressing schemes(IPv4 and IPv6), Forwarding and routing in Internet, Routing algorithms, Routing protocols in Internet(OSPF, RIP and BGP), BGP security, ICMP, NAT, IPSec – Introduction, Tunnel and Transfer Modes, IPSec Authentication Header, Encapsulating Security Header and Payload, IPSec Key Exchange and VPNs.
Link layer - Introduction and services, Link layer addressing, Multiple Access Protocols, Ethernet, ARP, Attacks against and vulnerabilities in ARP.

**TEXTBOOKS/ REFERENCES:**


1. Andrew S. Tanenbaum, "*Computer Networks*", Fourth Edition, Pearson Education Asia, 2002.
2. William Stallings, "*Cryptography and Network Security*", Fifth Edition, Prentice Hall, 2011.

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.

**18SN614 CRYPTOGRAPHY AND APPLICATIONS 4-0-0-4**

Unit 1: Concepts of Number Theory: Number Theory, GCD, Euclidean algorithm, Extended Euclidean algorithm, prime numbers, congruence's, how to solve congruence equations, Chinese remainder theorem, residue classes and complete residue systems, Euler Fermat theorem, primitive roots.

Unit 2: Symmetric Key Cryptographic Systems: Caesar and affine ciphers, mono-alphabetic substitutions, transposition, homophonic, Vigenere and Beaufort ciphers, one-time pad, product/iterated/block ciphers, DES and AES. Heavy discussion is given to the security of these ciphers, not only are they studied in an algorithm sense but their attacks and defences are also discussed.

Unit 3: Cryptanalysis of symmetric keys- Attack Models, Linear, Differential and various others such as meet-in-the-middle attack.

PKCS- Concepts of PKCS, Diffie Hellman key-exchange protocol, RSA, Rabin and EL Gamal cryptosystems, primarily testing, pollard rho factorisation, man-in-the-middle attack.

Unit 4: Stream Ciphers- synchronous, self-synchronizing attack ciphers, linear feedback shift registers, Berlekamp-Massey algorithm, algebraic attacks. Digital Signatures- Rabin, Lamport, Matyas-Meyer, RSA, multiple RSA and ElGamal signatures, digital signature standard.

Unit 5: Hash Functions and MACs- Hash functions: the Merkle-Damgard construction, Message Authentication Codes, security of Hash functions, security weakness of MD4, MD5, SHA1,SHA2 and construction of SHA3, identification protocols, authenticated key exchange and SSL/TLS session setup, Zero knowledge protocols.

Unit 6: Basic elliptic curve cryptography: definition, mathematical formulation of them, elliptic curve cryptography and pairings, introduction to quantum computers and the future of cryptography.

**TEXTBOOKS/REFERENCES:**

1. William Stallings "Cryptography and Network Security" Fifth Edition, Prentice Hall, 2011
2. Alfred J Menzes, Paul C Van Oorshot and Scott A. Vanstone "Handbook of Applied Cryptography", CBC Press, 1996
3. Stein William. "Elementary number theory. Primes, congruence's, and secrets." A computational approach
4. Neal Koblitz "A course in Number Theory and Cryptography" Springer-Verlag 1994
5. Christof Paar, "Understanding Cryptography", Springer-Verlag-2010

**18SN615 SYSTEMS SECURITY 3-0-1-4**

Security Goals, Secure Design Principles, Authentication, Linux Password scheme, Password Security, Privilege Escalation Attacks, Assembly Primer, Shellcoding, ELF File Format, Memory Exploits – Buffer Overflow, Off by one overflow, Format String Attacks, Integer

Overflow, Return to Libc, Heap Overflow, Case Study of Local and Remote Attacks, Exploit Development with Metasploit, Web Security – HTML/DOM Refresher, JavaScript, Browser Security Model, Authentication and Session Management, Cookies, Same Origin Policy, Security Policy for Windows and Frames, Web Vulnerabilities - Cookie protocol problems, SQL Injection, XSS, CSRF, SSL/TLS Vulnerabilities, Session Hijacking, Guninski Attack, Defenses, Understanding Threats - Classification, Rootkits, Virus, Worm, Clickjacking, Phishing, Pharming, Exploit kits, Botnets, Defenses- ASLR, DEP, Stack Canaries, Secure Coding Techniques for C Programs, Trusted Execution Environment- Case Study on TrustZone, Security Vulnerability Tools , Static and Dynamic Analysis overview

**TEXT BOOKS/REFERENCES:**


1. Neil Daswani, Christopher Kern, Anita Kesavan, "*Foundations of Security, What Every Programmer*
2. *Needs to Know*",Apress, 2007
3. James C. Foster and Vincent T. Liu, "*Writing Security Tools and Exploits"*, Syngress Publishing
4. Gary McGraw, John Viega, "*Building Secure Software"*, Addison-Wesley Professional, 2001.
5. Jon Ericson, "*Hacking: The Art of Exploitation"*, Second Edition, No Starch Press, 2008, ISBN 978-1593271442
6. Chris Anley, John Heasman, Felix Linder, Gerardo Richarte, The Shellcoder's Handbook : Discovering and Exploiting Security Holes, Second Edition, Addison-Wiley, ISBN 978-0470080238


**18SN616 CYBER FORENSICS AND INCIDENT RESPONSE 2-0-1-3**

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 forGoogle Android, Andrew Hoog, ISBN: 978-1-59749-651-3


**18MA612 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY SYSTEMS 3-0-0-3**

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 forEngineers*", 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.


**18RM600 RESEARCH METHODOLOGY 2-0-0-2**

Unit I:

Meaning of Research, Types of Research, Research Process, Problem definition, Objectives of Research, Research Questions, Research design, Approaches to Research, Quantitative vs. Qualitative Approach, Understanding Theory, Building and Validating Theoretical Models, Exploratory vs. Confirmatory Research, Experimental vs Theoretical Research, Importance of reasoning in research.

Unit II:

Problem Formulation, Understanding Modeling & Simulation, Conducting Literature Review, Referencing, Information Sources, Information Retrieval, Role of libraries in

Information Retrieval, Tools for identifying literatures, Indexing and abstracting services, Citation indexes

Unit III:
Experimental Research: Cause effect relationship, Development of Hypothesis, Measurement Systems Analysis, Error Propagation, Validity of experiments, Statistical Design of Experiments, Field Experiments, Data/Variable Types & Classification, Data collection, Numerical and Graphical Data Analysis: Sampling, Observation, Surveys, Inferential Statistics, and Interpretation of Results

Unit IV:
Preparation of Dissertation and Research Papers, Tables and illustrations, Guidelines for writing the abstract, introduction, methodology, results and discussion, conclusion sections of a manuscript. References, Citation and listing system of documents

Unit V:
Intellectual property rights (IPR) - patents-copyrights-Trademarks-Industrial design geographical indication. Ethics of Research- Scientific Misconduct- Forms of Scientific Misconduct. Plagiarism, Unscientific practices in thesis work, Ethics in science

**TEXT BOOKS/ REFERENCES:**


1. Bordens, K. S. and Abbott, B. B., "Research Design and Methods – A Process Approach", 8th Edition, McGraw-Hill, 2011
2. C. R. Kothari, "Research Methodology – Methods and Techniques", 2nd Edition, New Age International Publishers
3. Davis, M., Davis K., and Dunagan M., "Scientific Papers and Presentations", 3rd Edition, Elsevier Inc.
4. Michael P. Marder," Research Methods for Science", Cambridge University Press, 2011
5. T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand, 2008
6. Robert P. Merges, Peter S. Menell, Mark A. Lemley, "Intellectual Property in New Technological Age". Aspen Law & Business; 6 edition July 2012


**18SN701 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, checkpointing 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. Andrew S. Tanenbaum and Maarten van Steen, "*Distributed Systems: Principles andParadigms*", 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


**18SN702 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 EnterprisePerspective on Risks and Compliance*", O'Reilly Media, 2009
2. Ronald L. Krutz Russell Dean Vines "*Cloud Security: A Comprehensive Guide to SecureCloud 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 andintegrity layer for cloud storage*" Proceedings of the 16th ACM conference on Computer andcommunications security. ACM, 2009.
5. [Paper] Dean, Jeffrey, and Sanjay Ghemawat. "*MapReduce: simplified data processing onlarge clusters*" Communications of the ACM 51.1 (2008): 107-113.


**18SN703 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 data type 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.


**18SN704 SECURITYOFCYBER PHYSICAL SYSTEMS 3-0-0-3**

Theoretical foundations - Security and vulnerability of cyber-physical infrastructure networks, Game theory for infrastructure security, Analytical framework for cyber-physical networks, Security for wireless mobile networks - Jamming attacks, Mobile adhoc networks (MANET), Identity based attacks, Security of sensor networks – Distributed access control, Physical attacks, detection of compromised nodes, Platform security – Hardware: Hardware supply chain, hardware support, Languages: Compiler techniques, Static analysis, Cloud computing and data security - Protecting data in outsourcing scenarios, Mobile cloud computing, Event Monitoring and Situation Awareness - Distributed network and system monitoring, Sensor event analysis, Pervasive sensing and monitoring for situational awareness, Policy issues in security management - Managing and securing critical infrastructure, policies, access control and formal methods, Formal analysis of policy-based security configurations in enterprise networks, Security in Real-World Systems - Security and privacy in the Smart Grid, Automotive Information Technology, Mobile Health-Care (m-health) systems, Internet infrastructure, Emergency vehicular networks, VoIP Telecommunication Networks.

**TEXTBOOKS/ REFERENCES:**


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


**18SN705 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 Architecture 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 IPTables, 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 AndroidApplication Development: Android Essentials"*, Fourth Edition, Addison-WesleyProfessional, 2013
4. Adapted Materials from Android development sites.


**18SN706 ADVANCED NETWORK SECURITY 3-0-0-3**

**Application Security –** Introduction – Overview of Attacks Against Applications, AttackingSUID 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: PRIVATECommunication 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


**18SN707 MOBILE COMPUTING AND SECURITY 3-0-0-3**

Introduction to Mobile Computing: Mobile Computing 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 Mobileand 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.


**18SN708 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

**TEXTBOOKS / 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 ofthe System*" Second Edition,Jones & Bartlett, 2012.

**18SN709 SCADA NETWORK SECURITY 3-0-0-3**

Introduction- History, Architecture, Components, Functions, Fundamental principles and concepts of SCADA, DCS, PLCs, Field components, Real-Time Operating systems and Ladder Logic, Communications and OLE for Process Control (OPC), ICS Lifecycle Challenges, Physical Security, Network Architecture, models and design examples PLC – Role in Automation, PLC-SCADA Communications, SCADA Protocols, Security – ICS Attack Surface, Threats and Attack Routes, Attacks on Control Servers, Network Communications and Web Attacks, Security Standards and Mititgation, Defending ICS networks, servers and devices – Firewalls, NAC, Enforcement Zone Devices, DMZ, Honepots, Case Studies of ICS

**TEXT BOOKS / REFERENCES:**

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

**18SN710 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, Tamperproofing watermarks, Resilient watermarks, Stealth watermarks. Steganographic watermarks, Dynamic watermarking. Software Similarity Analysis:- Alternate methods 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.

**18SN711 SECURITY OF INTERNET OF THINGS 1-0-2-3**

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


**18SN712 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.

**18SN713 INTRODUCTION TO SOFTWARE REVERSE ENGINEERING 2-0-1-3**

Introduction, ethical and legal aspects of reverse engineering, low level assembly programming, identify common techniques and approaches for basic reverse engineering, disassembler and debugger aided debugging, reverse engineering high level languages, identifying and defeating anti-disassembly techniques, anti-debugging techniques, anti-VM techniques and code obfuscation, introduction to techniques used by malware, analysing and reversing windows executables, reverse engineering higher level languages(Python, Java and .Net bytecode).

**TEXT BOOKS / REFERENCES:**


1. Bruce Dang, Alexandre Gazet, Elias Bachaalany and Sebastien Josse, Practical Reverse Engineering, First Edition, Wiley Publishers, 2014.
2. Eldad Eilam, Reversing: Secrets of Reverse Engineering, Wiley Publishers, 2005.
3. Chris Eagle, IDA Pro Book, Second Edition, No Starch Press, 2011.
4. Michael Sikorski and Andrew Honig, Practical Malware Analysis, First Edition, No Starch Press, 2012.


**18SN714 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.


**18SN715 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 andTrends*", 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.


**18SN716 DATA ANALYTICS FOR SECURITY 2-0-1-3**

Introduction: Introduction to Information Security, Introduction to Data Mining for Information Security

Network Intrusion Detection: Signature-based solutions (Snort, etc), Data-mining-based solutions (supervised and unsupervised); Deep Packet Inspection: Alert aggregation for web security, One-class Multi-classifier systems for packet payload modeling and network intrusion detection , Host Intrusion Detection: Analysis of shell command sequences, system call sequences, and audit trails, Introduction to Insider threats, Masquerader/Impersonator/Insider threat detection strategies, Web Security: Anomaly detection of web-based attacks using web server logs, Anomaly detection in web proxy logs Email: Spam detection, Phishing email detection, phishing website detection Social network security: Detecting compromised accounts, detecting social network spam, Authentication: Anomaly detection of Single Sign On (Kerberos, Active Directory), Detecting Pass-the-Hash and Pass-the-Ticket attacks, Behavioural Biometrics: Active authentication using behavioural and cognitive biometrics, Mouse dynamics analysis for active authentication, touch and swipe pattern analysis for mobile active authentication, Automated correlation: Attack trees, Building attack scenarios from individual alerts, Issues: Privacy issues, Adversarial machine learning: Overview of Multi-classifier systems (MCS), advantages of MCS in security analytics, security of machine learning, Other potential topics: Fraud detection, IoT/Infrastructure security, Mobile/Wireless security, Machine Learning for Security: Challenges in applying machine learning (ML) to security, guidelines for applying ML to security, Current and future trends in security

**TEXTBOOKS / REFERENCES:**

1) Daniel Barbara and Sushil Jajodia, "Applications of Data Mining in Computer Security", Vol. 6. Springer Science & Business Media, 2002
2) Marcus A. Maloof, "Machine Learning and Data Mining for Computer Security", Springer Science & Business Media, 2006
3) V Rao Vemuri, "Enhancing Computer Security with Smart Technology", Auerbach Publications, 2005
4) S. Stolfo, S. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair, S. Smith, "Insider Attack and Cyber Security: Beyond the Hacker", Vol. 39. Springer Science & Business Media, 2008
5) Dhruba K. Bhattacharyya, Jugal K. Kalita, "Network Anomaly Detection: A Machine Learning Perspective", Crc Press, 2013
6) Anoop Singhal, "Data Warehousing and Data Mining Techniques for Cyber Security", Vol. 31. Springer Science & Business Media, 2007
7) Markus Jakobsson and Zulfikar Ramzan, "Crimeware, Understanding New Attacks and Defenses", Addison-Wesley Professional, 2008

**18SN717 BLOCKCHAINS AND CRYPTOCURRENCIES 3-0-0-3**

Bitcoin Protocol and Consensus: A High Level Overview, Bitcoin and Blockchain History, Bitcoin Mechanics and Optimizations: A Technical Overview, Bitcoin IRL: Wallets, Mining, and More, Ethereum and; Smart Contracts: Enabling a Decentralized Future, Game Theory and Network Attacks: How to Destroy Bitcoin, Crypto economics and Proof-of- State, Distributed Systems and Alternative Consensus, Scaling Blockchain: Cryptocurrencies for the Masses, Enterprise Blockchain: Real-World Applications, Anonymity: Mixing and Altcoins, Conclusion: Future of Blockchains

**TEXTBOOKS / REFERENCES:**

1. Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder
2. Mastering Bitcoin by Andreas Antonopoulos

**18SN718 CYBERSECURITY GOVERNANCE 3-0-0 3**

Principles of cyber-security governance, Assessment of cyber security maturity, Theories of governance – introduction, Governance – definitions and typologies, Tools, methods and processes, Vulnerability management, Threat management, Endpoint management , Intrusion detection and prevention (IDPS), Security incident management, Security operations center (SOC) and related concepts, Measurement of governance: Metrics – concepts, Application security metrics, Network security metrics, Security incident metrics, Vulnerability metrics, Service level objectives / agreement (SLO / SLA), NIST metrics, Basics of security analytics, Threat intelligence and governance, Data driven security governance, Impact of cognitive security on security governance, Industry specific security compliance, Cyber security governance India and Other countries, NIST mandates for compliance, Security reporting basics, CISO – role and organization structure

**TEXTBOOKS / REFERENCES:**

1. Hayden, Lance. *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*. McGraw-Hill Education Group, 2010.
2. Jacobs, Jay, and Bob Rudis. *Data-driven security: analysis, visualization and dashboards*. John Wiley & Sons, 2014.

3. Collins, Michael. *Network Security Through Data Analysis: From Data to Action*. " O'Reilly Media, Inc.", 2017.
4. Jaquith, Andrew. *Security metrics: replacing fear, uncertainty, and doubt*. Pearson Education, 2007.
5. Cybersecurity, Critical Infrastructure. "Framework for Improving Critical Infrastructure Cybersecurity." *Framework* 1 (2014): 11.

**18SN719 SOFTWARE DEFINED NETWORKING AND SECURITY 1-0-2-3**

SDN Origins and Evolution, Centralized and Distributed Control and Data Planes, SDN APIs, Virtualization of Network Functions (VNF) and NFV, Open Virtual Networking (OVN), Open Network Operating Systems (ONOS), SDN ABSTRACTIONS- How SDN Works,The Openflow Protocol, Big picture and other protocols, Controller Platforms, SDN Software Stack(s),PROGRAMMINGSDN- Northbound Application Programming Interface, Current Languages and Tools, Composition of SDNs, Mininet Environment and Implementation, SDN APPLICATIONS IN SECURITY- Switching and Load Balancers, Firewall and Access Control, Use cases in Legacy Networks security, Security in modern networks – Cloud, Fog, IoT, 5G, SDN CHALLENGES- Characteristics of SDN Architecture, Scalability of Control and Data Planes, Security Analysis and Potential attacks, Solutions, Fault Tolerance Designs, Debugging and Trouble Shooting,SDN-EXTENSIONS, Data plane and Control plane programming, Open vSwitch, Software and Hardware based, Middleboxes, Click OS, SD-WAN, SD Multi-Clouds and Internet Exchange points structure.

**TEXTBOOKS / REFERENCES:**

1. Software Defined Networks: A Comprehensive Approach by Paul Goransson and Chuck Black, Morgan Kaufmann Publications, 2014
2. SDN: Software Defined Networks, An Authoritative Review of Network Programmability Technologies, By Thomas D. Nadeau, Ken Gray Publisher: O'Reilly Media, August 2013,
3. SDN and OpenFlow for Beginners by Vivek Tiwari, Sold by: Amazon Digital Services, Inc., ASIN:, 2013.
4. Network Innovation through OpenFlow and SDN: Principles and Design, Edited by Fei Hu, CRC Press, ISBN-10: 1466572094, 2014.
5. Software Defined Networking with OpenFlow By SiamakAzodolmolky, Packt Publishing, 2013
6. Feamster, Nick, Jennifer Rexford, and Ellen Zegura. "The road to SDN: an intellectual history of programmable networks." ACM SIGCOMM Computer Communication Review 44.2 (2014): 87-98.
7. Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." Proceedings of the IEEE 103.1 (2015): 14-76.
8. Nunes, Bruno AA, et al. "A survey of software-defined networking: Past, present, and future of programmable networks." Communications Surveys & Tutorials, IEEE 16.3 (2014): 1617-1634.
9. Lantz, Bob, Brandon Heller, and Nick McKeown. "A network in a laptop: rapid prototyping for software-defined networks." Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. ACM, 2010.

10. Monsanto, Christopher, et al. "Composing software defined networks." Presented as part of the 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13). 2013.
11. “Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud” - William Stallings.